PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C
	Application Number	
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 — Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	David		WYATT	

Residence Information (Select One) ● US Residency Non US Residency Active US Military Service

City	State/Province	Country of Residence
San Jose	CA	US

Mailing Address of Inventor:

Address 1	1314 Vanna Ct
Address 2	

City	State/Province	Postal Code	Country
San Jose	CA	95131	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. — Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	136197		
Email Address	officeaction@mhbpatents.com	Add Email	Remove Email

Application Information:

Title of the Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE		
Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	7	**Suggested Figure for Publication (if any)**	7

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C
	Application Number	
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	136197		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status: Patented — Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
	Continuation of	17075637	2020-10-20	11176538	2021-11-16

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C
	Application Number	
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
17075637	Continuation of	16459150	2019-07-01	10810579	2020-10-20
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16459150	Continuation of	15701261	2017-09-11	10339520	2019-07-02
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15701261	Continuation of	14981757	2015-12-28	9760884	2017-09-12
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14981757	Continuation of	14680979	2015-04-07	9224083	2015-12-29
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14680979	Division of	14217261	2014-03-17	9022286	2015-05-05
Prior Application Status	Expired				Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
14217261	Claims benefit of provisional	61794891	2013-03-15		

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C
	Application Number	
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C
	Application Number	
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C
	Application Number	
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	Virtual Electric Inc.		
Mailing Address Information For Applicant:			
Address 1	1314 Vanna Ct		
Address 2			
City	San Jose	**State/Province**	CA
Country	US	Postal Code	95131
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C
	Application Number	
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Anthony C. Murabito/			Date (YYYY-MM-DD)	2021-11-16
First Name	Anthony	Last Name	Murabito	Registration Number	35295

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C
	Application Number	
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

RELATED APPLICATIONS

[0001] This is a Continuation application of co-pending, commonly-owned U.S. Patent Application Serial No. 17/075,637, now U.S. Patent 11,176,538, filed 10/20/2020, which in turn was in turn a Continuation application of co-pending, commonly-owned U.S. Patent Application Serial No. 16/459,150, now U.S. Patent 10,810,579, filed July 1, 2019, which in turn was a Continuation application of co-pending, commonly-owned U.S. patent application Ser. No. 15/701,261, now U.S. Pat. No. 10,339,520, filed Sep. 11, 2017, which in turn was a Continuation application U.S. patent application Ser. No. 14/981,757, filed Dec. 28, 2015, now U.S. Pat. No. 9,760,884, which in turn was a continuation of U.S. patent application Ser. No. 14/680,979, filed Apr. 7, 2015, now U.S. Pat. No. 9,224,083, which in turn was a Division of U.S. patent application Ser. No. 14/217,261, filed Mar. 17, 2014, now U.S. Pat. No. 9,022,286, which in turn claims priority from Provisional Application 61/794,891, filed Mar. 15, 2013, each of which are hereby incorporated herein in their entirety by reference.

FIELD OF THE INVENTION

[0002] Embodiments according to the present disclosure generally relate to electronic or smart payment devices and, more specifically, to more secure, smart multi-function smart tokenizing electronic payment devices and transaction processing thereof.

IPR2025-01150
Apple EX1071 Page 10

BACKGROUND OF THE INVENTION

[0003] There are several different types of credit cards available in the marketplace at present. A first type of credit card is a conventional, standard piece of plastic with a magnetic strip, which is readily available and in wide commercial use. The advantage of this first type of credit card is that a large portion of the infrastructure for credit card transactions is built around this type of card, and consequently such a card works in a wide array of vendors' credit card machines, automated teller machines (ATMs), and other devices that support the present credit card and banking infrastructure.

[0004] Another type of credit card device employs the use of a smart integrated circuit chip. These types of credit cards have a built-in microprocessor with cryptographic capabilities. These microprocessors operate in a similar manner to a cell phone having a chip comprising a cryptographic processor. Such a smart card device requires contact with a reader in order to be read and to perform a transaction. The reader provides the manner in which a facility interacts with the built-in processor on the card, e.g., for purposes of performing verification on the authenticity of the card or for making a direct deposit on the card. These credit card devices also comprise a magnetic strip such that they are compatible with standard plastic credit card readers in wide use.

[0005] A different type of credit card device in circulation employs radio frequency identification ("RFID"). These cards essentially have a low-power RF antenna built into the card, and when the cardholder passes the antenna in front of a reader comprising an

IPR2025-01150
Apple EX1071 Page 11

RF field, enough power is generated to enable the processor to interact wirelessly with the receiving device.

[0006] A concern with each of these types of credit cards presently available in the marketplace is that they can all be, in various ways, susceptible to theft and/or compromise. Therefore, these types of credit cards have security limitations. Further, cards employing smart integrated circuit chips and RF technology are not in wide use at present because they are incompatible with existing credit card infrastructure, which still predominantly supports conventional plastic credit cards.

SUMMARY OF THE INVENTION

[0007] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

[0008] An embodiment includes a multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card. An apparatus is described to allow said device to emulate behavior of a credit card when used in electronic credit card readers. Additionally, methods are described to allow user control of said device for the purpose of authorizing or controlling use of said device in the application of credit, debit and cash transactions, including cryptocurrency and device-to-device transactions. Methods are also described for generating a limited-duration payment number when performing a transaction for the purpose of creating a limited-use payment number, which is limited in scope of use to a predetermined number of authorized transactions. Furthermore, said device may interact with other similar devices in proximity for the purpose of funds or credit/debit transfers.

[0009] More specifically, an aspect of the present disclosure provides an apparatus comprising: a thin card shaped sized body; a memory operative to store a plurality of identification data; a processor coupled to the memory; a user interface for selecting a

select identification data of said plurality of identification data; a magnetic card reader detection unit for determining if the body is adjacent to a standard magnetic card reader; and an inductor assembly coupled to the processor and integrated into the body, the inductor assembly under processor control for generating a magnetic field of alternating polarity responsive to the body being detected as adjacent to a standard magnetic card reader, the magnetic field generated in a region substantially encompassing the standard magnetic card reader, wherein the magnetic field encodes said select identification data, and wherein the magnetic field is operable to be read by a magnetic read head of the standard magnetic card reader.

[0010] According to another aspect of the present disclosure, a multi-function electronic device comprises: a near-field communication (NFC) unit; a touch sensor array; a display; a motion rate detection array; a memory, storing a user data and a currency amount; and a processor operatively coupled to the NFC unit, the touch sensor array, the display, the motion rate detection array, and the memory; and wherein the processor initiates a device-to-device transaction between two devices by a detected proximity of a first device and a second device and an input of information by a first user via said touch sensor array, and wherein the device-to-device transaction comprises an exchange of stored currency and said user data between the first device and the second device via the NFC unit.

[0011] According to yet another aspect of the present disclosure, a method of performing a transaction comprises: receiving an input signal at a multi-function electronic device from a user enabling operation of a near-field communication (NFC)

unit of the device; receiving an indication of an amount of currency for a transaction; generating at said device a limited-duration payment number; and transmitting said limited-duration payment number from said device to a recipient of the transaction.

IPR2025-01150
Apple EX1071 Page 15

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Embodiments of the present disclosure are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements.

[0013] Figure 1 is an illustration depicting an exemplary interaction between a device and a standard magnetic card reader, according to an embodiment of the present disclosure.

[0014] Figures 2A-2B are block diagrams illustrating data flow between the magnetic coils on the device and the microprocessor on the device according to an embodiment of the present disclosure.

[0015] Figure 2C depicts an exemplary process of selecting an account from a plurality of stored accounts according to an embodiment of the present disclosure.

[0016] Figure 3 is a flowchart illustrating an exemplary process of generating a magnetic field with an alternating polarity according to an embodiment of the present disclosure.

[0017] Figures 4A-4B illustrate a user interacting with a touch sensor of a device, according to an embodiment of the present disclosure.

[0018] Figure 5 is an illustration of a device connected with a computing system and operating according to an embodiment of the present disclosure.

[0019] Figure 6 is an illustration of two devices performing a transaction according to an embodiment of the present disclosure.

[0020] Figure 7 depicts an exemplary process according to an embodiment of the present disclosure.

IPR2025-01150
Apple EX1071 Page 17

DETAILED DESCRIPTION OF THE INVENTION

[0021] Reference will now be made in detail to the various embodiments of the present disclosure, examples of which are illustrated in the accompanying drawings. While described in conjunction with these embodiments, it will be understood that they are not intended to limit the disclosure to these embodiments. On the contrary, the disclosure is intended to cover alternatives, modifications and equivalents, which may be included within the spirit and scope of the disclosure as defined by the appended claims. Furthermore, in the following detailed description of the present disclosure, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. However, it will be understood that the present disclosure may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the present disclosure.

[0022] Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits that can be performed on computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer generated step, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities.

IPR2025-01150
Apple EX1071 Page 18

Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in a computer system. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[0023] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present claimed subject matter, discussions utilizing terms such as "storing," "creating," "protecting," "receiving," "encrypting," "decrypting," "destroying," or the like, refer to the action and processes of a computer system or integrated circuit, or similar electronic computing device, including an embedded system, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

ENCODING VIA AN ALTERNATING POLARITY OF A MAGNETIC FIELD

[0024] In one embodiment of the present disclosure, a smart multi-function electronic device comprises a dynamic magnetic region (strip) incorporating a main inductor assembly from which programmed magnetic field data symbols are dynamically generated. In one embodiment the inductor assembly may be a planar coil formed within the material that embodies the multi-function electronic device. An advantage of

using a planar coil is that it can dynamically produce a magnetic field in such a manner as to emulate the interaction between a traditional magnetic strip and a conventional card reader. As the magnetic strip of a conventional card is passed through a magnetic reader head, stripes of alternating magnetic polarity embedded in the strip induce a magnetic field of alternating polarity at the reader head. The pattern formed by the alternating polarity of the magnetic field encodes information, which when transformed by a transducer to a current signal in the magnetic reader head, provides user information for a transaction.

[0025] Embodiments of the present disclosure provide a multi-function electronic device able to generate a programmed magnetic field, wherein data is encoded and represented by an alternating polarity of the generated magnetic field. In a similar manner to a conventional plastic card, the magnetic field produced by the planar coil is able to be read by a pickup (or "transducer") and to thereby transmit information to the magnetic card reader. Figure 1 illustrates a payment transaction 100 performed between a multi-function electronic device 101 and a conventional magnetic reader 150. The multi-function electronic device 101 generates a magnetic field of alternating polarity 120 to be read by the conventional magnetic card reader 150, according to an embodiment of the present disclosure. The multi-function electronic device 101 is moved at a rate 130 relative to a magnetic reader head 155 of conventional magnetic card reader 150. The magnetic field 120 extends with sufficient distance and intensity from 101 so as to be read by magnetic head reader 155. The magnetic head reader 155 responds to the magnetic field 120 by producing a current in the conventional fashion,

which is then interpreted as encoded information by the magnetic reader 150. Therefore the magnetic field of alternating polarity 120 produced by the multi-function electronic device 101 has a substantially identical encoding effect as a traditional magnetic strip.

[0026] A characteristic of encoding information in a conventional magnetic card strip is that binary information is encoded by the pattern of alternating magnetic polarity formed by ferromagnetic stripes embedded on the magnetic strip. As the conventional magnetic card strip has a standardized format, the encoding of information is provided at a specified data density (bits per inch), according to which conventional magnetic readers are designed for interpretation of encoded data. In order to most ably emulate a conventional card interaction with a conventional magnetic reader the multi-function electronic device 101 of the present disclosure is provided with a means of determining a substantially optimal rate for alternating the polarity of the generated magnetic field 120 in order to produce data at a rate which is able to be readily received and correctly interpreted by the conventional magnetic reader 150. Embodiments of the present disclosure provide several means of determining the relative movement rate 130 between the multi-function electronic device 101 and the magnetic reader head 155. These features, as well as other characteristics of the multi-function electronic device of the present disclosure, can be better appreciated by a description of the internal components and functions of multi-function electronic device 101.

[0027] Figures 2A and 2B depict exemplary embodiments of a smart multi-function electronic device, in a block diagram view. The components of the block diagram are illustrated according to functional connections, and their locations should not be

construed as being limited to the respective locations as depicted in Figures 2A-2B. In Figure 2A, multi-function electronic device 201a is shown in a block diagram view. Multi-function electronic device 201a comprises a processor 205 and a memory unit 207, the processor 205 operatively coupled to the components of multi-function electronic device 201a. The memory 207 comprises a plurality of accounts 209, which may be credit card accounts, banking accounts, merchant accounts, online accounts, cryptocurrency accounts, and combinations thereof. A motion detection module 210 is coupled to the processor unit 205 and to a set of motion detection units, which comprise a rate detection assembly 225, an optical sensor array 230, and a set of accelerometers 235. The magnetic field is generated via a planar coil 220, which is controlled by the processor unit 205 via a coil interface 215. The rate at which the magnetic field changes polarity to encode the user data depends on the rate of relative movement detected by the rate detector. The multi-function electronic device 201a further comprises a real-time clock 240, a touch-sensor array 245, and a display 250, each operatively coupled to the processor unit 205. A user input may be made via the touch sensor array 245, which may comprise a touch screen panel, a keypad, or a combination thereof. The display 250 is able to display an alphanumeric sequence, as well as graphical icons (such as a logo for a bank, or other images). Further, an optional backup power source 255 is depicted.

[0028] In one embodiment, the processor unit 205 is connected to the planar coil 220 and the motion detection units, via the motion detection module 210. The processor unit 205 is responsible for determining the appropriate rate with which to output data from the planar coil 220, wherein output data is encoded using alternating polarity of a

generated magnetic field. The rate of the alternating polarity of the magnetic field is generated in accordance with the detected movement speed with which the card is swiped through the reader, in order for the reader to receive the encoded data at the appropriate rate. Magnetic card readers, which are designed to read conventional cards, are constructed to read data at specified input rates that correspond with the data density present in conventional magnetic card strips. The magnetic data symbols generated by the planar coil 220 are produced to align with the rate at which data is being read by the magnetic card reader. Accordingly, it is irrelevant if the multi-function electronic device 201a of the present disclosure is being swiped quickly or slowly, the planar coil 220 is controlled by the processor unit 205 to produce data at a substantially optimized rate, where the rate of data production is dependent on the rate at which the multi-function electronic device 201a is detected to be passing across the magnetic reader head.

[0029] Figure 2B depicts a multi-function electronic device 201b according to an embodiment of the present disclosure. Device 201b comprises a processor 205 and a memory unit 207, the processor 205 operatively coupled to the components of multi-function electronic device 201b. The memory 207 comprises a plurality of accounts 209, which may be credit card accounts, banking accounts, merchant accounts, online accounts, cryptocurrency accounts, and combinations thereof. A motion detection module 210 is coupled to the processor unit 205 and to a set of motion detection units, which comprise a rate detection assembly 225, an optical sensor array 230, and a set of accelerometers 235. Additionally, a galvanic sensor 275 is coupled to processor unit 205.

IPR2025-01150
Apple EX1071 Page 23

The magnetic field is generated via a planar coil 220, which is controlled by the processor unit 205 via a coil interface 215. The rate at which the magnetic field changes polarity to encode the user data depends on the rate of relative movement detected by the rate detector. The multi-function electronic device 201b further comprises a real-time clock 240, a touch-sensor array 245, and a display 250, each operatively coupled to the processor unit 205. A user input may be made via the touch sensor array 245, which may comprise a touch screen panel, a keypad, or a combination thereof. The display 250 is able to display an alphanumeric sequence, as well as graphical icons (such as a logo for a bank, or other images). Further, an optional backup power source 255 is depicted. Multi-function electronic device 201b further comprises a near-field communication (NFC) unit 260, as well as a radio frequency identification (RFID) unit 265, both of which are operatively coupled to the processor unit 205. In one embodiment the NFC and RFID may share the planar coil for use as a radio frequency antenna, through the coil interface 215. In one embodiment one or both the NFC and the RFID may have antennae dedicated to that individual sub-system. A universal serial bus (USB) connector 270 is coupled to the processor unit 205. The functionality of the components with regard to exemplary uses of multi-function electronic devices 201a and 201b is described in greater detail in the following description.

[0030] A further aspect of the present disclosure provides a single multi-function electronic device that can be used for multiple banks or financial institutions. For example, instead of carrying a separate payment card for each account of a variety of payment card companies, a customer need only to carry a single device according to

embodiments of the present disclosure. The capability of the multi-function electronic device to generate a multitude of payment numbers provides the ability of the multi-function electronic device to be associated with multiple accounts. Furthermore, inputs at the touch sensor array on the multi-function electronic device can be used to select the appropriate bank or credit provider account stored in the memory unit of the multi-function electronic device.

[0031] Figure 2C depicts a process of selecting an account from a plurality of stored accounts in order to perform a transaction with the selected account, according to an embodiment of the present disclosure. The process 280 begins at step 282, where a plurality of accounts stored by the multi-function electronic device memory is displayed. The plurality of accounts 209 are stored by memory 207, and are displayed using display 250. A user indicates an account selected from the plurality of accounts at step 284. The selection is able to be made by keypad or touch sensor array 245, and an indication of the selected account can be displayed via display 250. At step 286 the multi-function electronic device is configured according to account information associated with the selected account, which may include an account number, an expiration date, and other user information associated with the account (e.g. a username, PIN, password, email address, etc.). At step 288 the planar coil of the multi-function electronic device is encoded with a limited-duration payment number that is associated with the selected account. The limited-duration payment number is able to be generated according to the selected account, a timestamp, a transaction amount, an indicated merchant, user key or

secrets, on-card unique hardware secrets, payment authority key or secrets, user input from the card interface, and other information associated with the transaction.

MOVEMENT RATE FEEDBACK

[0032] The relative movement rate of multi-function electronic device 201a is detected by one or more of the set of motion detection units, comprising the rate detection assembly 225, the optical sensor array 230, and the set of accelerometers 235. Each of the motion detection units detects the motion of the device 201a in a distinct manner. The rate detection assembly 225, which is positioned alongside (but independent of) the planar coil 220, is able to detect the location of a magnetic head reader as the rate detection assembly 220 is being passed through the card reader. The reader module of a conventional card reader comprises a metal head having a small gap at the tip of the head. A pickup armature resides in this gap, such that as the metal head passes over a card strip, an electric field is induced in the head reader pickup circuit. In one embodiment the rate detection assembly 225 is constructed of an array of auxiliary inductor coils and magnetic pickup coils. As the metal head of the card reader assembly passes over the arrangement of auxiliary inductor coils and magnetic pickup coils of the rate detection assembly 225, a disturbance in the magnetic field flowing between the two is induced, generating a change in current and producing a detected movement signal. The change in current is detected by the motion detection module 210, and is used to determine the rate of motion of the card reader head passing across the surface of the multi-function electronic device 201a (and therefore along the planar coil 220).

IPR2025-01150
Apple EX1071 Page 26

[0033] The optical sensor array 230 is also operable to detect a movement rate of the multi-function electronic device 201a with respect to a conventional magnetic card reader. The optical sensor array 230 is disposed nearby the planar coil 220, in order to accurately detect a movement rate in the region of the planar coil 220. In an embodiment, the optical sensor array 230 is a thin strip parallel to, and extending along, the length of the planar coil 220. The optical sensor array 230 determines a location of a minimum of received light, which corresponds to the region of a surface in nearest proximity to the optical sensor array 230. The magnetic reader head of a conventional magnetic card reader extends furthest from the surface of the card reader, and therefore the detected minimum in received light at the optical sensor array 230 corresponds with the location of the reader head. By tracking over time the position of this minimum received light along the optical sensor array, a detected movement rate may be found.

[0034] The set of accelerometers 235 are also operable to detect a movement rate of the multi-function electronic device 201a. The set of accelerometers 235 are positioned in the multi-function electronic device 201a in order to effectively measure the position and acceleration of the multi-function electronic device 201a. In an embodiment, the set of accelerometers comprises groups of accelerometers, each group having one or more accelerometers disposed at orthogonal planes to each other, and each group capable of generating signals that allow for determination of the orientation, motion and acceleration of the multi-function electronic device 201a.

[0035] The detected movement signal is received by the motion detection module 210. The detected movement signal is generated by any one of the set of motion detection

units, or any combination of motion detection units of the set. For example, the movement detection signal is able to be generated by the combination of the rate detection assembly 225 and the optical sensor array 230. In an embodiment, the movement detection module 210 is able to determine the movement rate of the multi-function electronic device 201a from the detected movement signals, and transmits the determined movement rate, and orientation to the processor unit 205. In an embodiment, the motion detection module 210 sends the detected movement signal to the processor unit 205, and the processor unit 205 determines the relative movement rate.

[0036] In one embodiment, the generation of the magnetic field by the planar coil 220 at a specified rate of alternating polarity is accomplished according to the following description. One or more of the motion detection units in the set of motion detection units (rate detection assembly 225, optical sensor array 230, and set of accelerometers 235) detect a movement rate of the multi-function electronic device 201a with respect to a magnetic card reader, and signal the motion detection module 210. The movement rate is provided to the processor unit 205, which determines the appropriate rate for alternating the polarity of the magnetic field generated by the planar coil 220. The processor unit 205 outputs instructions or data to the coil interface 215 at the determined rate, which in an embodiment is a digital-to-analog converter (a DAC) and acts to translate the signal from digital to analog in order to drive the planar coil 220 and produce the magnetic field. The instructions from the processor unit 205 are comprise binary code, which are output through a shift register to the coil interface 215.

IPR2025-01150
Apple EX1071 Page 28

The shift register outputs data at a rate proportional to the determined movement rate of the multi-function electronic device 201a – thus, a higher determined multi-function electronic device 201a movement rate has a corresponding higher output rate at the shift register, leading to a higher rate of alternating polarity at the generated magnetic field (i.e., encoded data symbols output more quickly). Conversely, a lower movement rate of multi-function electronic device 201a leads the processor unit 205 to control the shift register to output data at a lower rate, and consequently the rate of alternating polarity in the generated magnetic field is lower.

[0037] Figure 3 illustrates an exemplary process 300 for determining the rate to alternate the polarity of the generated magnetic field of the multi-function electronic device, according to an embodiment of the present disclosure. At step 301 the process determines if a standard magnetic card reader is detected to be in proximity with the multi-function electronic device. If NO, the step repeats. If YES, the process moves to step 303. At step 303 a detection of a movement rate at which the body of the multi-function electronic device is moving relative to the standard magnetic card reader is made. The process continues at step 305, wherein a magnetic field is generated by an inductor assembly comprised by the multi-function electronic device, the magnetic field having a target rate of alternating polarity that is based on the detected movement rate from step 303. The process then repeats at step 301, determining if a standard magnetic card reader is (or remains) in proximity to the multi-function electronic device. In this manner, while a standard magnetic card reader is detected to be in proximity to the multi-function electronic device, the movement rate of the multi-function electronic

device is determined and the polarity and orientation of the generated magnetic field is alternated at the appropriate rate, to recreate the data as described above, at the correct rate, in order to clock out the data to be conveyed to the magnetic strip reader, at a rate matching the action of an ordinary magnetic strip card through same the magnetic card reader.

SECURITY

[0038] Security is an area of concern for payment card holders, as the small form factor makes theft quite easy, and additionally there are many ways for a malicious third-party to record the account number of a payment card in order to later make fraudulent transactions on the account. Embodiments of the present disclosure address security concerns of a payment card owner on several fronts.

[0039] In one aspect, security of the multi-function electronic device is enhanced by providing a means of locking the multi-function electronic device in order to prevent use, until such time that a valid user input is entered. Embodiments of the present disclosure provide a multi-function electronic device having a region for receiving human input, e.g., touch sensors which are able to be formed by contacts that a user can press (e.g., the touch sensor array 245 of Figures 2A-2B). Figures 4A-4B illustrate a user interacting with a multi-function electronic device 401 via a keypad or touch sensor array 445. In Figure 4A, the multi-function electronic device 401 is in a locked state. A display 450 is able to display a message to the user, for instance, the message "device locked" or "enter password," or question prompts which guide the user to respond with answers through the key-pad or the touch sensor, to certain preset questions, that

confirm personal knowledge known only to the associated user. The touch sensor array 445 enables user interaction with the multi-function electronic device 401. An exemplary use of the touch sensor array 445 is an input of a currency amount to be used in a transaction. The touch sensor array 445 is able to include buttons, or a touch-sensitive pad, or a combination of the two. Other embodiments of the touch sensor array 445 allowing a user to input data to the multi-function electronic device 401 are consistent with the spirit and scope of the present disclosure.

[0040] In order to unlock the multi-function electronic device 401 and enable a transaction or other usage, the user inputs data via the touch sensor array 445. Figure 4B illustrates the user inputting a password via a gesture 470, which operates to unlock the multi-function electronic device 401. The display 450b is able to display a message indicating the multi-function electronic device 401 is unlocked and ready for use, for instance, display 450b may display the message "unlocked," or it may display an account number associated with the multi-function electronic device 401.

[0041] Embodiments of the present disclosure provide additional functionality for the touch sensor array 445. For example, there may be touch contact terminals that a user can press to wake up the multi-function electronic device 401, to cause the battery to supply power, or to place the multi-function electronic device 401 in a power reduction mode when it is not being used. In an embodiment, if any number other than the correct password is entered multiple times, or if there is an attempted usage of the multi-function electronic device 401 without entering in a password, an automatic phone call may be triggered to the appropriate fraud protection authorities.

[0042] In one embodiment of the present disclosure, the display 450 is a thin-film liquid crystal display ("LCD"). The display 450 is able to have multiple uses. In one embodiment, the display 450 can be used to cue the user for a security question upon input of an improper password. Or if fraud protection services need to contact a customer, they can verify the customer's identity by transmitting a security question to the display 450 of user's multi-function electronic device 401, to which the user would need to respond correctly using the input buttons of touch sensor 445 on the card.

LIMITED-DURATION PAYMENT NUMBER

[0043] A further security feature of the multi-function electronic device provided in the present disclosure is the capability of producing a limited-duration payment number for performing transactions using accounts of the card. The multi-function electronic device comprises a real-time clock that is able to produce a cryptographically protected timestamp for each interaction. The power source is able to activate the processor unit such that a unique number may be generated by the multi-function electronic device and verified by the payment authority according to the timestamp and the transmitted user information. The limited-duration payment number is able to be produced at the time the multi-function electronic device is performing a transaction, and is able to be generated according to the user's private information, a bank information, information regarding the facility performing the transaction, and the time of day. The limited-duration payment number is able to be limited to only one transaction, a finite number of transactions, or may be limited to a specified period of time – e.g., 2 minutes, 10 minutes, 3 hours – after which time that particular limited-duration number would

become invalid. As detailed above, if an expired limited-duration payment number is attempted to be used for a transaction, the transaction is denied and an automatic notification is able to be made to a payment authority in order to notify the user and to prevent transactions on the account. The transaction count is able to be determined through the action of passing the card through magnetic reader, and the process of transmitting the payment number to the card reader.

[0044] In one embodiment, the number on the front of the card is able to be a full or partial number. In an embodiment, the number displayed on the multi-function electronic device is a static number, but the number transmitted during a transaction is a limited-duration payment number as described above. The number displayed on the multi-function electronic device may not necessarily be a static number. For example, the first four and last four digits of the payment number are able to be fixed, while the remaining eight digits can be dynamically generated. As the device is read by the machine, part or all of the number may be dynamically produced at the time the device is read. As described above, the dynamic part of the limited-duration payment number generated may be based on the user's private information, the user's bank information, the time of day or the facility that is reading the card. Further, the expiration date of the multi-function electronic device can also be dynamically generated.

[0045] Effectively, embodiments of the present disclosure provide a multi-function electronic device that has no fixed number, as illustrated in Figure 11, and therefore the account cannot be compromised. Only the number generated at the instant of the multi-function electronic device transaction matters. Accordingly, unauthorized use of the

multi-function electronic device is highly unlikely, because a transaction cannot be conducted with an expired limited-duration payment number, or only the static portion of the payment number. In one embodiment of the present disclosure, sufficient dynamically generated numbers are provided for on the multi-function electronic device such that a unique payment number can be generated for each transaction. In this embodiment, the multi-function electronic device of the present disclosure effectively acts as a unique per-transaction payment device.

[0046] With reference to Figure 2A, 2B, in one embodiment, the process steps enabling a card transaction are as follows. A multi-function electronic device (e.g., multi-function electronic device 201b) is connected to a computer system (e.g. computer system 590, Figure 5), via any of the connection means available to the multi-function electronic device (USB 270, NFC 260, and RFID 265). User data and other essential information, such as account information, are downloaded to the multi-function electronic device. For example, for an account designed for online transactions, user account information will likely include an account email and an account password. The account may be for example a bank account, a credit account, a merchant account, an online transaction account, or a cryptocurrency. In one embodiment a currency amount is also downloaded, which is made accessible to the multi-function electronic device 201b for transactions. In an alternative embodiment, rather than a currency amount being downloaded to the multi-function electronic device 201b, the user account information (e.g., username and password) is stored such that a subsequent authorized multi-function electronic device 201b transaction is automatically pre-authorized to deduct (or

credit) the entered transaction amount at a stored account. In an embodiment, a user uses the touch sensor array 245 of the multi-function electronic device 201b in order to input the user information, including the amount of currency to be stored. The information entered by the user is able to include an account source of a transaction (e.g., bank account, credit account, merchant account, ATM, online payment service, or a cryptocurrency), as well as a type of transaction to be made (e.g., as a debit card, as a credit card, or as a user account). In another embodiment, the information is entered using the computing system to which the multi-function electronic device 201b is connected.

[0047] Transactions may be authenticated on the specified account by entry of the username and password for the account during the transaction, using the touch sensor array 245. In an embodiment, a password for an account is represented by a user input (such as a gesture, a swipe, and/or an unlock keycode) which is entered on multi-function electronic device 201b during a transaction for account authentication. According to an embodiment of the present disclosure, a user that has "primed" the multi-function electronic device 201b for a transaction has already performed a security authentication on the card, and therefore a subsequent card transaction is able to be pre-authorized to perform the transaction without further user authentication steps. The priming action can be a tap of the multi-function electronic device 201b detected by accelerometers 235, or a gesture, swipe, or a key input received by touch sensor array 245.

[0048]

[0049] A transaction is able to be communicated using the planar coil 220. In one embodiment, when the transaction is a payment transaction, a limited-duration payment number is generated. A user inputs an amount for the transaction using the touch sensor array 245, and the limited-duration payment number is generated to correspond with the entered amount. The binary data corresponding to this limited-duration payment number is sent from the processor unit 205 to the coil interface 215, where it is converted to an analog signal in order to drive the planar coil 220 to generate a magnetic field having an alternating polarity corresponding to the encoded data of the limited-duration payment number.

ONLINE TRANSACTIONS

[0050] Figure 5 displays the multi-function electronic device 501 in connection with a computing device 590. In one embodiment, the multi-function electronic device 501 is able to be used to make online purchases. In one embodiment, the multi-function electronic device 501 is equipped with a means 570 for communicating with the USB port on a computer or other device in order to make online purchases. In one embodiment the multi-function electronic device 501 may have an area cut out, such that contact terminals corresponding to a USB cable connector are contained within, enabling connection of a USB cable (e.g., a micro-USB connection). When performing online transactions, the multi-function electronic device 501 can uniquely generate a limited-duration payment number (as described above) for online purchases. The multi-function electronic device 501 receives a user input indicating that a transaction is imminent, and an authorization. The user input is able to comprise a gesture, a swipe, a

key input sequence, and combinations thereof. The limited-duration payment number is able to be displayed on the front display of the multi-function electronic device 501. In one embodiment, the multi-function electronic device 501 is able to use RFID 265 or near field communication NFC 260 technology in order to connect to a personal computer 590. This enables a per-transaction, limited-use payment number, enhancing the security of the payment account by substantially negating the possibility of a theft of the payment number used to perform the transaction leading to account compromise. See also, for example, Figure 10.

[0051] According to an embodiment, the transaction is able to include information regarding a user account, such as an email address of the user, and upon reconnection of multi-function electronic device 201b to a computer system (for instance, computer system 590), the transaction information stored on multi-function electronic device 201b could be "replayed" by the computer system in order to finalize the transaction.

[0052] In one embodiment, a means of limiting an available credit amount are provided. According to the download process described above, the multi-function electronic device is able to have a total credit available. The multi-function electronic device is able to reference the total credit available in subsequent transactions, and will provide limited-duration payment numbers corresponding to amounts up to, but not exceeding, the remaining credit available to the multi-function electronic device. An attempt to perform a transaction having an amount exceeding the remaining credit available will not result in a valid limited-duration payment number, and therefore an authenticated transaction cannot proceed. In general, the multi-function electronic

device will only successfully generate a limited-duration payment number if the proper conditions for a transaction are determined to be present. The proper conditions for a transaction comprise a correct identification having been made by the user (via a gesture, swipe, and/or key input) and an amount for the transaction indicated to be less than the total credit available to the account indicated for the transaction.

DEVICE-TO-DEVICE TRANSACTIONS

[0053] In addition to transactions performed using conventional magnetic card readers (such as at point-of-sale locations, banks, and automated teller machines (ATMs)) and via cable connection with a computing device, transactions performed wirelessly between a device and a device (e.g., card-to-card, card-to-computer device having a reader dongle, card-to-ATM) are provided according to embodiments of the present disclosure. See, for example, Figures 8 and 10. For simplicity, the following describes a device-to-device transaction, but it will be understood that card-to-device transactions are similarly provided.

[0054] Figure 6 illustrates a device-to-device transaction according to one embodiment. A first multi-function electronic device 601a comprises a display 650a, and is in contact with a second multi-function electronic device 601b. A contact interaction between the devices is indicated by interaction 680. In one embodiment, the contact interaction is a tapping of a device 601a against another device 601b. In another embodiment, an optical sensor array at one or both of the devices detects interaction 680. In another embodiment, interaction 680 indicates a swipe of a device 601a across another device 601b. In one embodiment a user input through the key-pad initiates and

enables a transaction from first device to second device. In one embodiment the presence of second device in preparation for device-to-device transaction is confirmed through "polling", the process of which involves transmission of data between devices, and confirmed receipt of transmitted data by response received from second device received at first device, including information confirming receipt of the information, by second device.

[0055] The planar coil comprised by each of multi-function electronic device 601a and multi-function electronic device 601b is able to be a means of transferring information for a transaction, e.g., such as an antenna. Once either, or both, of multi-function electronic device 601a and multi-function electronic device 601b detect interaction 680, a transaction is able to be completed via generation of a magnetic field at one card and reception of the magnetic field (i.e., reading) at the other card. In this manner, the device (e.g., multi-function electronic device 601a) receiving the transaction information operates its planar coil in an antenna mode. This enables multi-function electronic device 601a and multi-function electronic device 601b to authentically perform a transaction, and to transfer a currency between multi-function electronic device 601a and multi-function electronic device 601b. As described above, in an embodiment the transaction is able to use a limited-duration payment number to encode the transaction.

[0056] In an embodiment, a set of accelerometers is used to detect the beginning of the transaction, for instance, a transaction performed by a swipe of multi-function electronic device 601a across multi-function electronic device 601b. Further, the set of accelerometers can detect a "priming" action for a multi-function electronic device, i.e.,

an indication for a multi-function electronic device that a transaction is imminent. The priming action can be a tap of the multi-function electronic device 601a, or tapping the multi-function electronic device 601a against the multi-function electronic device 601b. In one embodiment, a touch sensor array is able to be used for the priming action.

[0057] In an embodiment of a device-to-device transaction, one device (e.g. 601a, the device of the user having a currency debit) generates the limited-duration payment number, which is transmitted via the device's planar coil. The multi-function electronic device of the recipient (e.g., 601b, the card of the user receiving a currency credit) receives the encoded data via the planar coil, acting as an antenna, and the coil interface is able to convert the received signal into a digital signal understood by the processor to be the limited-duration payment number, identifying both the correct account and the amount of the transaction.

[0058] In one embodiment, the multi-function electronic device 201b stores cryptocurrency information in processor unit 205. The cryptocurrency information stored is able to include a plurality of cryptocurrency addresses, a plurality of private keys, and a plurality of public keys. The multi-function electronic device 201b is able to perform a transaction, as described above, using a cryptocurrency as the specified account. In one embodiment, the multi-function electronic device 201b is able to hash a portion of the transaction, using the processor unit 205 and the real-time clock 240 along with user information pertinent to the cryptocurrency account and the transaction. A subsequent connection of the device 201b to a computing device provides a means of connecting to the cryptocurrency servers and finalizing the transaction. Further, the

multi-function electronic device 201b is able to sign a cryptocurrency transaction by, for instance, receiving a prompt at the display 250 to input a dynamic PIN specific to the transaction, which is able to be entered by touch sensor array 245.

[0059] In a device-to-device cryptocurrency exchange, a record of the transaction can be made according to the following. A first device (e.g. 601a) making a deduction with an amount indicated via touch sensor array 245 is able to generate a record of the transaction and store the record in the device memory, while a second device (e.g. 601b) receiving the cryptocurrency is able to generate a confirmation of the received transaction amount. In one embodiment, the amount indicated is provided by the receiving device 601b. The hashed record of the transaction contains the unique information of each user, along with the transaction amount. The success or failure of the transaction is able to be displayed on the respective displays of devices 601a and 601b.

ACCOUNT THEFT AND UNINTENDED USE PREVENTION

[0060] A security concern for conventional credit cards utilizing wireless communication means is the ability of a thief to access and/or copy user information through un-detected interaction with the wireless communication means. Sensitive and confidential information can be gleaned via, for example, "listening-in" on an RFID interaction between a credit card and a contactless reader, recording the characteristics of the interaction, and replicating certain characteristics to fake an authorized transaction. While to a great extent security concerns are addressed by the usage of limited-duration payment numbers and other security features provided for by the

device of the present disclosure and previously described, a further security feature regarding the wireless communication means of the multi-function electronic device is described herein.

[0061] In one embodiment, wireless communication means of the multi-function electronic device 201b are in a powered-down, or disabled, state prior to receiving an authenticated activation signal from a user. Upon receiving the activation signal, the communication means (e.g., NFC 260, RFID 265, and planar coil 220) are activated, enabling the multi-function electronic device 201b to conduct a transaction. The activation signal can originate from one (or a combination) of the set of motion detection units (rate detection 225, optical sensor array 230, and accelerometers 235), the touch sensor array 245, and the galvanic sensor 275. The galvanic sensor 275 is operable to detect a contact of human skin, via a current produced at the sensor 275 upon such contact. See also, for example, Figure 8. In an embodiment the galvanic sensor 275 is comprised of metallic contacts disposed on opposite sides of, and isolated by, the body of multi-function electronic device 201b. In one embodiment, the current produced by user contact with the galvanic sensor 275 contacts is sufficient to provide small amounts of energy in order to power components of the card. For example, energy produced is able to power the processor unit 205 and the RFID 265. In one embodiment the galvanic sensor 275 further comprises two conducting surfaces separated by a junction, and the galvanic sensor 275 is configured as a thermoelectric generator (e.g., via the Peltier effect, the Seebeck effect, or a combination). For example, heat applied at one surface of the multi-function electronic device 201b may lead to differential heating between the

opposing, separated conducting surfaces of the galvanic sensor 275, generating an electric current and powering a subset of, or all of, the components of multi-function electronic device 201b (e.g., the processor unit 205, the NFC 260, and the RFID 265).

[0062] In an embodiment, the communication means are activated only so long as the activation signal continues to be detected. In another embodiment, the communication means are activated for a specified amount of time following detection of the activation signal. For example, if using the multi-function electronic device 201b in an ATM (or other device) preventing continuous human contact, the activation signal is able to be a swipe, gesture, or key input sequence entered via the touch sensor array 245, which activates the device for a specified duration (for instance, one minute). In an embodiment the detection of motion through accelerometer input indicates activation by a valid user. In one embodiment the specific motion detected through accelerometer input corresponding with a specific user action, such as a "flick", "swipe", "spin", "wave", "tap," may be used to initiate activation, wherein the motion is not normally generated at idle and during periods of inactivity. For example the motion not being generated accidentally while the device is stored in a user's wallet, carried while the user is actively moving, or is being handed from user to a clerk at a point of transaction. In one embodiment the specific motion, or sequence of motions, may be associated with a user, and stored on the device memory, such that performing the correct sequence when prompted can confirm the possession of the device by the known owner, thus initiating activation and enabling usage.

IPR2025-01150
Apple EX1071 Page 43

[0063] Figure 7 depicts a process of selectively enabling the communication capability of the multi-function electronic device according to an embodiment of the present disclosure. The process 700 begins at step 701, where an input signal is received at the multi-function electronic device from a user. The input signal is able to be generated by any one, or combination, of a plurality of input means, where the input means comprise: a swipe gesture received at a touch sensor array; a key press sequence; an accelerometer sensor indication of multi-function electronic device motion; and a galvanic sensor indication that the device is in a user grasp. The input received from the user enables operation of a near-field communication (NFC) unit of the multi-function electronic device. In one embodiment, the NFC unit is disabled prior to receiving the input signal. In one embodiment, an RFID communication unit is disabled prior to receiving the input signal, and is activated by the input signal. In one embodiment, the planar coil is disabled prior to receiving the input signal, and is activated by the input signal.

[0064] The multi-function electronic device, following enablement of the NFC unit, receives an indication of an amount of currency for a transaction at step 703. At step 705, the multi-function electronic device generates a limited-duration payment number, which at step 707 is transmitted to a recipient of the transaction. In one embodiment, the limited-duration payment number has a limited recurrence, and is limited in scope of use to a predetermined number of authorized transactions.

[0065] In the foregoing description of process 700, the ordering of the process steps is exemplary and should not be construed as limiting. Alternative ordering of the process

steps is consistent with the present disclosure, as conceived by one skilled in the relevant art.

[0066] In one embodiment of the present invention, a credit card comprises a dynamic magnetic strip incorporating a main inductor assembly from which magnetic field data symbols are dynamically generated. In one embodiment the inductor assembly may be a planar coil formed within the plastic that the credit card is composed with. The advantage of using a planar coil is that it can produce the same magnetic field interaction that a traditional magnetic strip on a conventional credit card can produce when it is passed through a reader. Similar to a traditional plastic credit card, the planar coil can also produce a magnetic field that can be read by a pickup (or "transducer"). The pickup produces electric current in the coil that, in turn, produces a magnetic field that is read by the pickup. Accordingly, the planar coil can be read in the same way as the magnetic strip on a traditional plastic credit card. The magnetic field produced by the planar coil would behave identically to a traditional magnetic strip.

[0067] In one embodiment, alongside the main planar coil, auxiliary rate detection assembly independent of the main inductor assembly would be provided to assist with the alignment of the production of data from the loop as it is being passed over the head of the credit card reader. The reader module of a traditional credit card reader comprises a metal head with a small gap on the tip of the head. This gap is where the pickup armature resides, so that when the metal head passes over the credit card strip, an electric field is induced in the head reader pickup circuit. In one embodiment the auxiliary rate detection assembly is constructed of an array of auxiliary inductor coils

and magnetic pickup coils, alongside the main coil. As the metal head of the card reader assembly passes over the arrangement of auxiliary coils and pickup circuits, a disturbance in the magnetic field flowing between the two generates a electrical current change that is detected by a rate detection circuit so as to detect the rate of motion of the card reader head passing across the surface of the card and therefore along the main induction assembly. The purpose of this is to allow the determination of the rate or production of magnetic data symbols in the main inductor assembly to align with the rate at which data is being read by the reader, according to the data density of standard card magnetic strips. Accordingly, it is irrelevant if the credit card of the present invention is being swiped fast or slow, the main inductor assembly produces data at just the right rate depending on the rate at which the card is detected it is being passed over the reader's head.

[0068] In one embodiment, a microprocessor is connected to the main coil and the alignment pickups. The microprocessor is responsible for producing the data from the coil at the appropriate rate in accordance with the speed with which the card is swiped through the reader. As shown in Figure 1, the auxiliary coil detects the rate at which the credit card is being swiped. The microprocessor then uses this information to produce the data from the main planar coil at the appropriate rate for the credit card reader.

[0069] In addition, the credit card of the present invention comprises a real time clock that can produce a cryptographically worthy timestamp for each interaction and a battery back up that can be used to power up the microprocessor. Further, the card can

comprise additional human inputs, e.g., touch sensors which can be formed by contacts that a user can press. For example, there can be contacts that a user can press to wake up the card, to cause the battery to supply power, or to put the card to sleep when it is not being used. There can also be additional inputs to key in customer specific information. For example, there can be inputs to key in a password or any other kind of unique identifier. If any other number besides the password is entered multiple times, or if there is attempted usage of the card without entering in a password, an automatic phone call may be triggered to the appropriate fraud protection authorities.

[0070] In one embodiment, the number on the front of the card can be a full or partial number. The number may not have to necessarily be a static number. For example, the first four and last four digits of the card number can be fixed while the remaining eight can be dynamically generated. As the credit card is read by the machine, part or all of the number may be dynamically produced at the time the card is read. The dynamic part of the number generated may be based on the user's private information, the user's bank information, the time of day or the facility that is reading the card. Further, the expiration date of the card can also be dynamically generated. Effectively, a credit card can be created that has no fixed number and therefore cannot be stolen. Only the number generated at the instant the card is being used matters. Accordingly, unauthorized use of the card is nearly impossible because no transaction can be conducted with only the partial static part of the payment number. In one embodiment of the present invention, enough dynamically generated numbers are provided for on the credit card such that a unique payment number can be generated for each transaction.

IPR2025-01150
Apple EX1071 Page 47

In this embodiment, the credit card of the present invention effectively acts as a unique per transaction credit card.

[0071] In embodiments of the present invention comprising dynamically created payment numbers, a single credit card can be used for multiple banks. For example, instead of carrying a separate credit card for all the different credit card companies, a customer would only need to carry a single card and one of the inputs on the front of the card can be used to select the appropriate bank or credit provider.

[0072] In one embodiment of the present invention, a thin film liquid crystal display ("LCD") can be fitted on the card so the credit card can have a display screen. The display can have multiple uses. In one embodiment, the display can be used to ask the user a security question if an improper password is entered. Or if the fraud protection services need to contact a customer, they can verify the customer's identity by transmitting a security question to the user's credit card screen to which the user would then need to respond correctly using the input buttons on the card.

[0073] In one embodiment, the credit card of the present invention could also be used to make online purchases. In this embodiment, the card could use RFID or near field technology so that it can connect to a personal computer and be used to uniquely generate a payment number for online purchases. The number could also, in one embodiment, be displayed on the front LCD of the card. In one embodiment, the card may also be equipped with a means for communicating with the USB port on the computer in connection with making the online purchases.

TABLE 1

1. An apparatus for conducting credit transactions comprising:

a device with the similar dimensions and thickness to a standard credit card

an inductor assembly integrated into said device capable of generating a programmed magnetic field at a location on the device where it will come into proximity to a standard credit card magnetic-strip reader

the inductor assembly being operable to be read by a magnetic pickup of an electronic credit card reader;

at least one auxiliary rate detection units adjacent to said inductor assembly, wherein said at least one auxiliary detection unit is operable to detect a rate at which said device, including said inductor assembly, is passed through said electronic credit card reader; and

a microprocessor operatively coupled to said inductor assembly and said at least one detection unit, wherein said microprocessor is operable to simulate magnetic-strip data fields using the inductor assembly, at a rate determined from said auxiliary detection units.

2. A method of Claim 1, wherein the inductor assembly is a planar coil which is a looped inductor with dimension roughly equal to, and along the axis of, the standard credit-card magnetic strip

3. A method of Claim 1, wherein said detection assembly consists of a plurality of

motion rate detection units, which may comprise inductor coils and companion magnetic-field pickup coils, each of which is able to detect the proximity of metallic objects, such as magnetic-strip reader heads, passing through the magnetic field created by said inductor and detected by said pickup coil.

4. A method of Claim 1, wherein said device may incorporate a plurality of touch sensors arranged along the surface of said device which may;

allow user input of information,

allow introducing a transaction specific identifier,

to confirm/deny transaction information,

to operate in sequence, or with a gesture across said sensor for the purpose lock/unlock or control access for transactions

5. A method of Claim 4, wherein said device contains a real-time clock or counter unit which generates a sequential parameter when the card is read by said credit card reader, and which along with certain user information, transaction identifiers, user secrets, payment authority secrets is combined to generate a limited-use payment number, which has a limited recurrence, is limited in scope of use to a predetermined number of authorized transactions

6. A method of Claim 5, wherein the time, sequence, user, payment authority and other information is similarly combined by credit card processing facility to generate

a payment number for comparison to the number transmitted by the credit card reader, for the purposes of authenticating said number is from a recognized card used in a user-authorized transaction

7. A method of Claim 1, wherein said device incorporates a display allowing payment number, time, passcodes, sequence codes, amounts and other credit card transaction information to be displayed for user, merchant, bank or credit card authority

8. An Apparatus for conducting credit transactions comprising,
wherein the edge of said device contains a connector for connection to standard computing devices such as a USB interface.

[0074] The foregoing description, for purpose of explanation, has been described with reference to specific embodiments. However, the illustrative discussions above are not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the invention and its practical applications, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as may be suited to the particular use contemplated.

[0075] Embodiments according to the invention are thus described. While the present disclosure has been described in particular embodiments, it should be appreciated that

the invention should not be construed as limited by such embodiments, but rather construed according to the below claims.

IPR2025-01150
Apple EX1071 Page 52

CLAIMS:

What is claimed is:

1. A method of performing a transaction, the method comprising:

receiving an input at an electronic device,

wherein the input corresponds to a priming operation of the electronic device by an identified user, and,

wherein the electronic device comprises:

a processor;

a touch-screen display coupled to the processor; and

a near field communications (NFC) interface coupled to the processor;

receiving a request for a transaction payment at said electronic device via at least one the set consisting of: the NFC interface, the touch-screen display;

displaying, on the touch-screen display, information reflecting the request for the transaction payment, and

images of:

a card issuer payment card method selection,

including at least a 4-digit partial number of a card issuer supplied account number of the card issuer payment card,

a card issuer card logo, and

other iconography of the card issuer payment card;

generating, by the processor, a limited-use payment information, and

using said limited-use payment information in place of said card issuer supplied payment information;

transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface; and

visually conveying a status of said transaction via a user-interface displayed on said touch-screen display.

2. The method of claim 1, wherein the generating limited-use payment information comprises dynamically generating a cryptogram number for a use by the electronic device in place of a card validation value, associated with said card issuer payment card.

3. The method of claim 1, further comprising wirelessly receiving a static device account number from a card issuing authority, in response to a user-entry of a user's card issuer payment card information.

4. The method of claim 2, further comprising wirelessly receiving a static device account number from a card issuing authority, in response to a user-entry of a user's card issuer payment card information.

5. The method of claim 4, wherein the wirelessly received static device account number is for use in place of a user-entered card issuer payment card information, in a device payment transaction by an authorized device user.

IPR2025-01150
Apple EX1071 Page 54

6. The method of claim 5, wherein the limited-use payment information comprises combining the dynamic cryptogram number and the static device account number.

7. The method of claim 2, wherein the dynamically generated cryptogram number is based in part on a per-transaction sequential parameter originating from within the electronic device.

8. The method of claim 7, further comprising wirelessly receiving a static device account number from a card issuing authority, in response to a user-entry of a user's card issuer payment card information.

9. The method of claim 8, wherein the wirelessly received static device account number is for use in place of a user-entered card issuer information, in a device payment transaction by an authorized device user.

10. The method of claim 9, wherein the limited-use payment information comprises combining the dynamic cryptogram number and the static device account number.

11. A system comprising:

an electronic device responsive to a priming operation from an authorized device user;

wherein the priming operation comprises a user input to the device enabling a payment transaction by the device;

wherein the electronic device comprises:

a processor;

at least one user input means, coupled to the at least one processor for receiving the user input;

a near field communications (NFC) interface coupled to the processor and operable to receive a request for a transaction payment; and,

a touch-screen display coupled to the processor, and

operable to display information reflecting the request for a payment transaction and information reflecting at least one payment option of at least one card issuer payment card;

wherein the electronic device is operable to dynamically generate a limited-use payment number based on a payment transaction sequential parameter originating from within the device;

wherein the electronic device is operable to store device-secret information; and,

wherein the electronic device is operable to transmit limited-use payment information comprising a combination of said dynamically generated limited-use payment number and said device-secret information, to an NFC recipient via said NFC interface in connection with the request for a payment transaction; and,

wherein the touch-screen display is operable to visually convey a status of said payment transaction

wherein the touch-screen display is operable to visually convey that the payment transaction is approved only when at least the following conditions are met: the device transacted limited-use payment number matches a payment number similarly generated by a payment card processing authority, the payment transaction sequential

parameter matches a transaction sequential parameter similarly generated by a payment card processing authority, and when the device-secret information matches a device-secret information stored within the payment card processing authority.

12. The system of claim 11, wherein the secret information from a payment card processing authority comprises a static device account number.

13. The system of claim 12, wherein said static device account number is specific to the electronic device.

14. The system of claim 13, wherein the payment card processing authority recognizes said use of said static device account number, as being from a recognized device in a user-authorized transaction, when payment card processing authority generated limited-use payment number based at least in part on a transaction sequential parameter similarly generated by a payment card processing authority, matches in comparison with said transacted limited-use payment information.

IPR2025-01150
Apple EX1071 Page 57

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

ABSTRACT

An embodiment includes a multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card. An apparatus is described to allow the device to emulate behavior of a credit card when used in electronic credit card readers. Additionally, methods are described to allow user control of the device for the purpose of authorizing or controlling use of the device in the application of credit, debit and cash transactions, including cryptocurrency and device-to-device transactions. Methods are also described for generating a limited-duration payment number when performing a transaction for the purpose of creating a limited-use payment number, which is limited in scope of use to a predetermined number of authorized transactions. Furthermore the device may interact with other similar devices in proximity for the purpose of funds or credit/debit transfers.

IPR2025-01150
Apple EX1071 Page 58

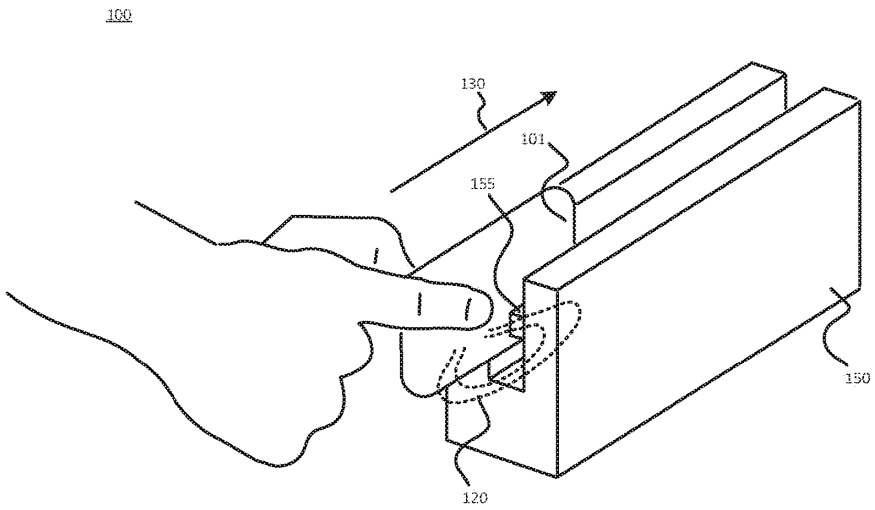


FIG. 1

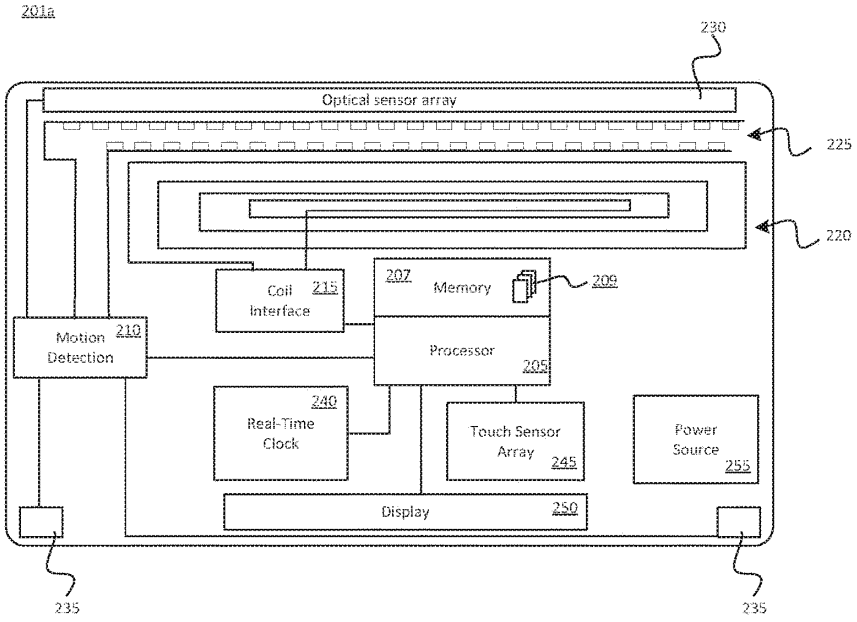

201a
230
Optical sensor array
225
220
Coil Interface 215
207 Memory
209
Motion Detection 210
Processor 205
240 Real-Time Clock
Touch Sensor Array 245
Power Source 255
Display 250
235
235

FIG. 2A

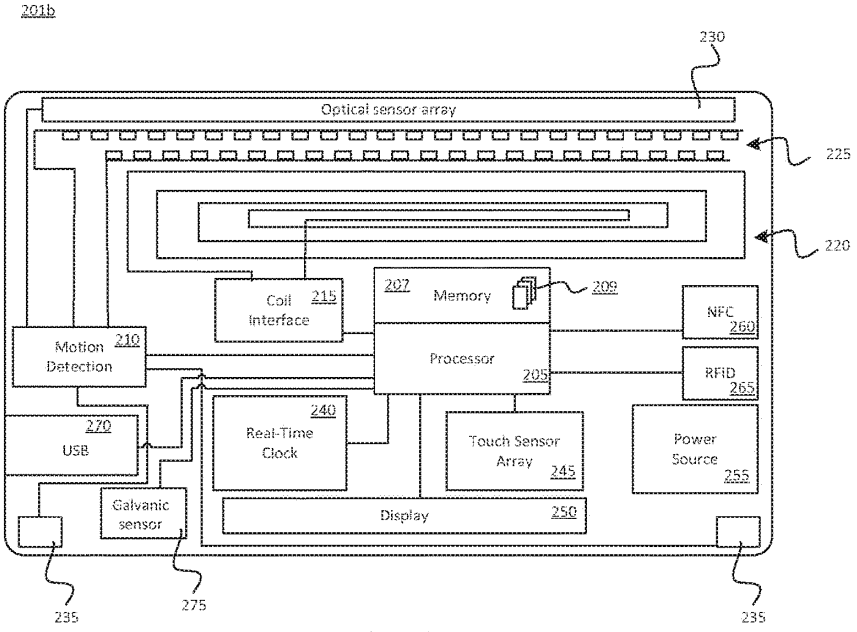

201b
230
Optical sensor array
225
220
Coil Interface 215
207 Memory
209
NFC 260
Motion Detection 210
Processor 205
RFID 265
240 Real-Time Clock
270 USB
Touch Sensor Array 245
Power Source 255
Galvanic sensor
Display 250
235
275
235

FIG. 2B

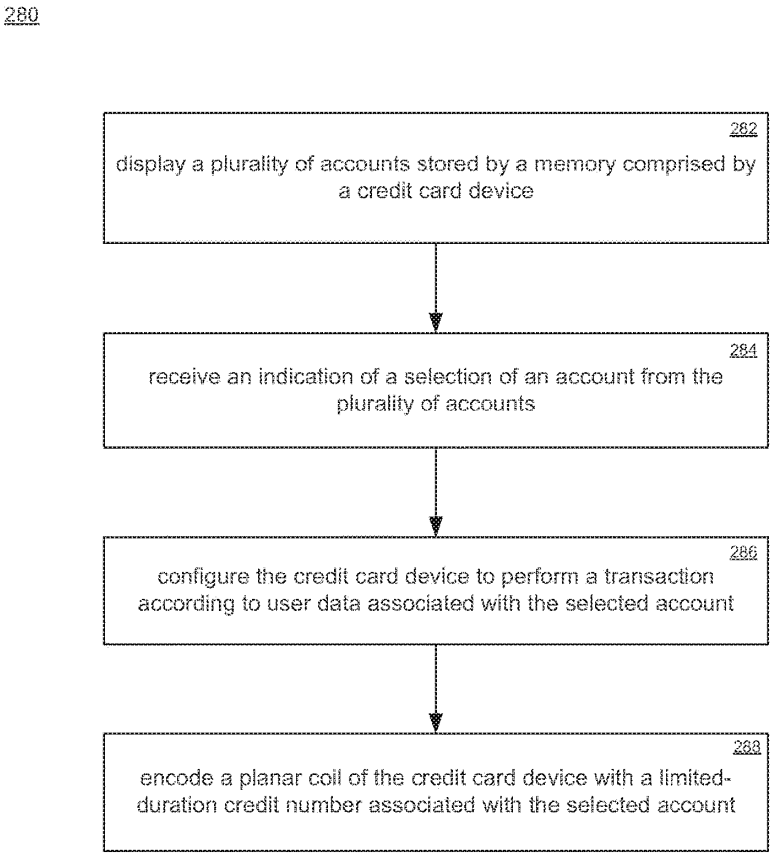

280
282
display a plurality of accounts stored by a memory comprised by a credit card device
284
receive an indication of a selection of an account from the plurality of accounts
286
configure the credit card device to perform a transaction according to user data associated with the selected account
288
encode a planar coil of the credit card device with a limited-duration credit number associated with the selected account

FIG. 2C

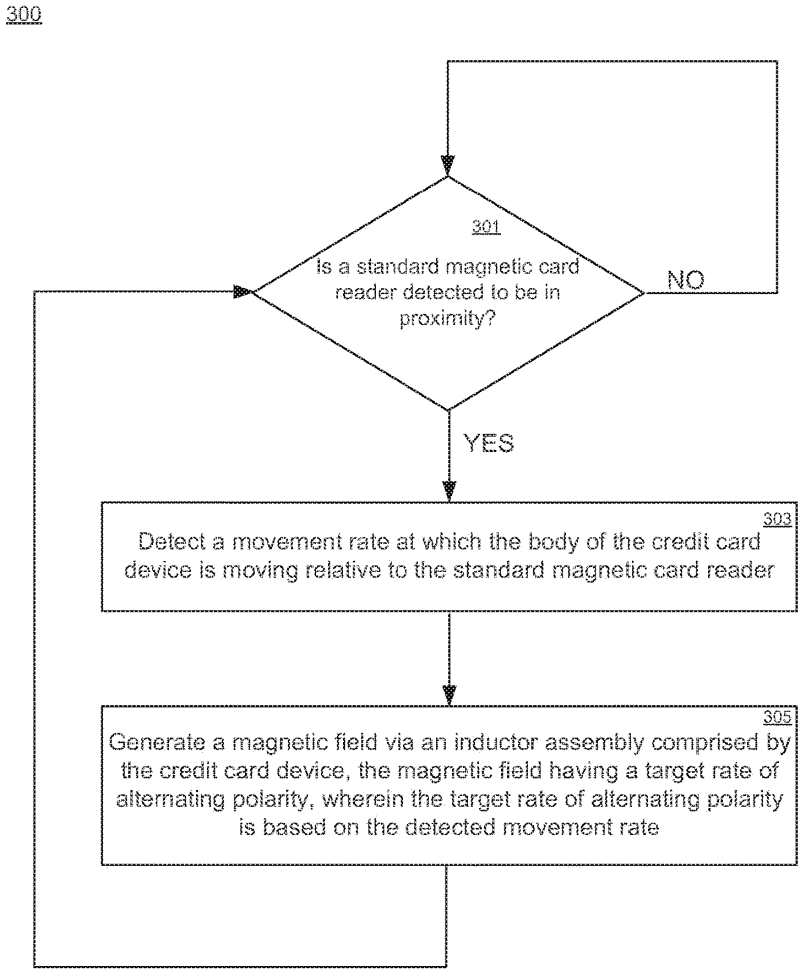

300
301
Is a standard magnetic card reader detected to be in proximity?
NO
YES
303
Detect a movement rate at which the body of the credit card device is moving relative to the standard magnetic card reader
305
Generate a magnetic field via an inductor assembly comprised by the credit card device, the magnetic field having a target rate of alternating polarity, wherein the target rate of alternating polarity is based on the detected movement rate

FIG. 3

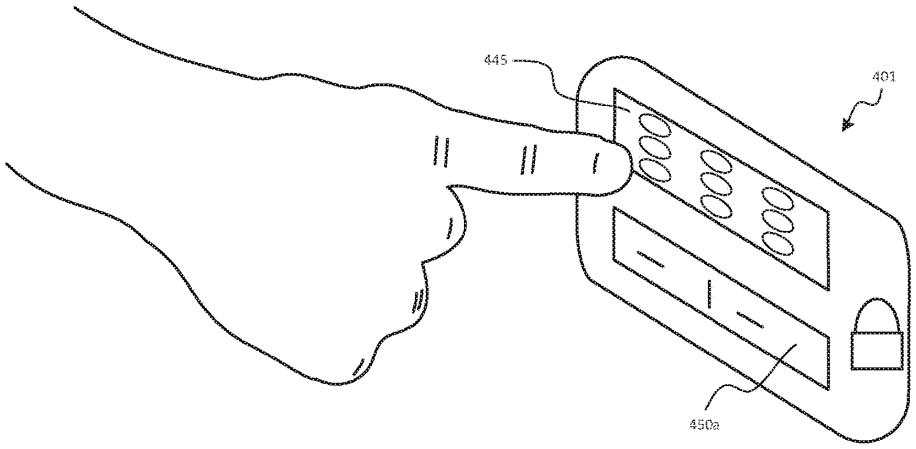


FIG. 4A

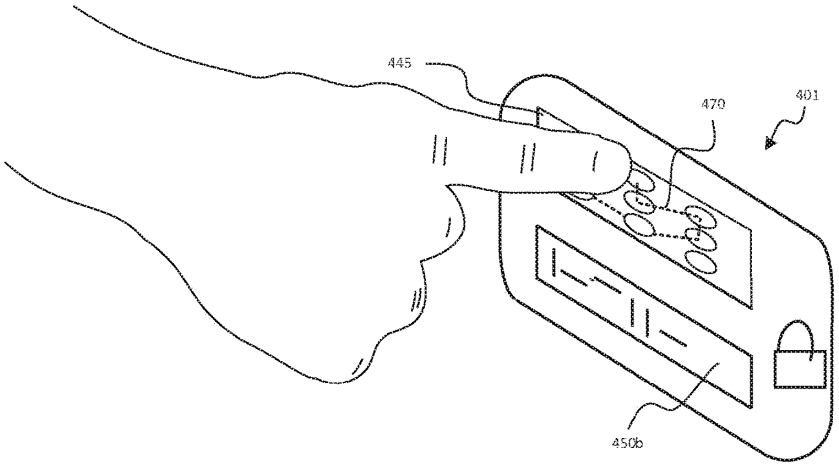


FIG. 4B

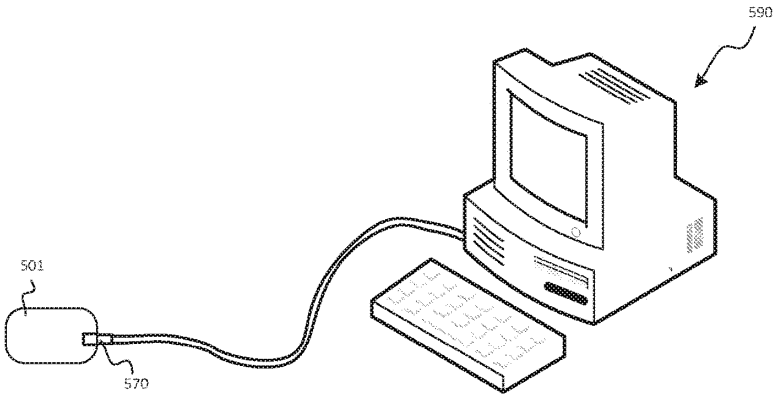


FIG. 5

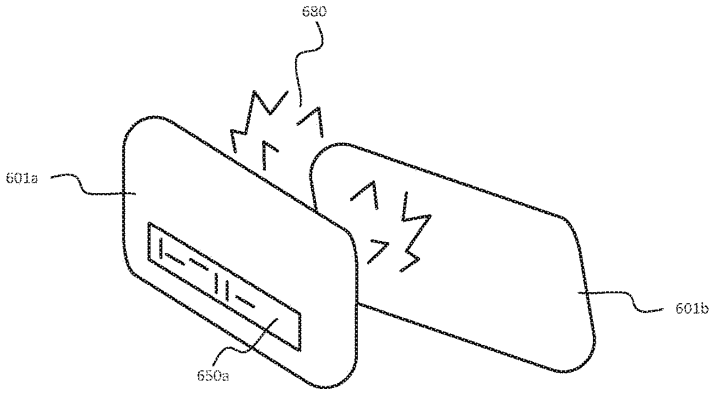


FIG. 6

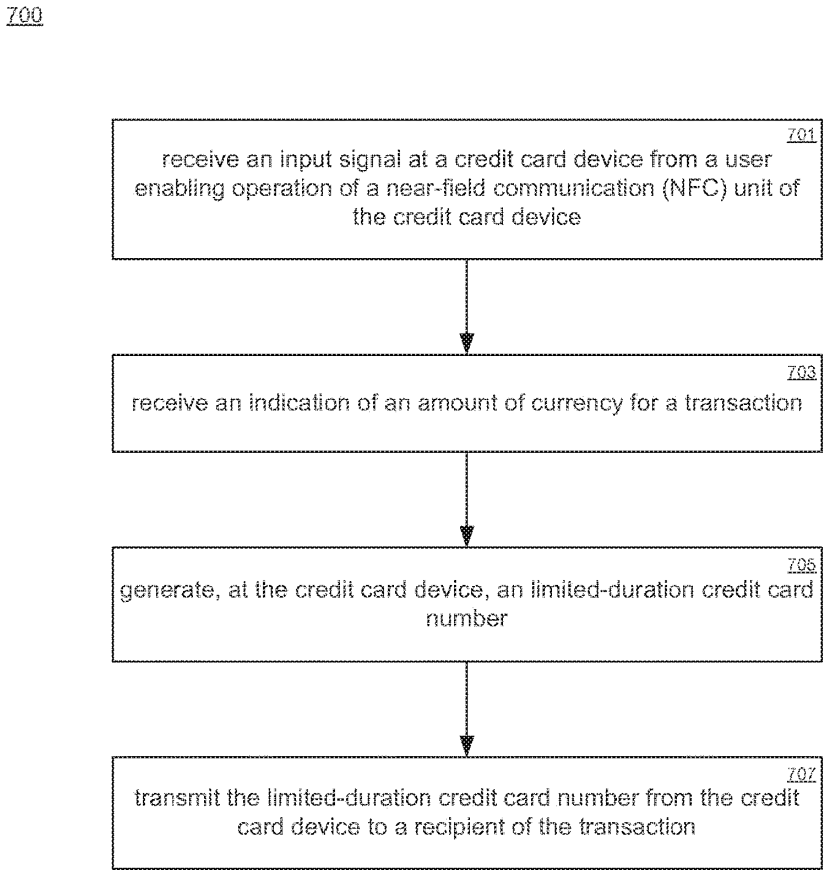

700
701
receive an input signal at a credit card device from a user enabling operation of a near-field communication (NFC) unit of the credit card device
703
receive an indication of an amount of currency for a transaction
705
generate, at the credit card device, an limited-duration credit card number
707
transmit the limited-duration credit card number from the credit card device to a recipient of the transaction

FIG. 7

WYAT-0002.US

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	MULTI-FUNCTIONAL CREDIT CARD TYPE PORTABLE ELECTRONIC DEVICE

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: David WYATT Date (Optional): 3/17/14

Signature: D. A. Wyatt

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	44299149
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Anthony C. Murabito/Missy Isaac
Filer Authorized By:	Anthony C. Murabito
Attorney Docket Number:	WYAT-0002USD1C1C1C1C1C
Receipt Date:	16-NOV-2021
Filing Date:	
Time Stamp:	19:38:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	WYAT-0002USD1C1C1C1C1C_ADS_11-16-2021.pdf	1793710 62b4a63f295cdc1f5a0f24a9ecfb06d0ff3629a5	no	9

Warnings:

Information:					
2		WYAT-0002USD1C1C1C1C1C_CON_APP_11-16-2021.pdf	250438 c81e978a673b02a2cc3aeeac8703501af1efc9ac	yes	49
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	43	
	Claims		44	48	
	Abstract		49	49	
Warnings:					
Information:					
3	Drawings-only black and white line drawings	WYAT-0002USD1C1C1C1C1C_FIGURES_11-16-2021.pdf	228170 c221514b3dda9b2eb45b3f19858633199bee3641	no	7
Warnings:					
Information:					
4	Oath or Declaration filed	WYAT-0002USD1C1C1C_DEC_FROM_PARENT_10-20-2020.pdf	69977 049fb9a8b7b25d07cfa88c9c27b06162a61c06e0	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	2342295		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 17/528,073

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	14 minus 20 =	*	x 50 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*	x 240 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	830		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2876	0.00	WYAT-0002.USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

FILING RECEIPT

OC000000130108239

Date Mailed: 12/01/2021

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

David WYATT, San Jose, CA;

Applicant(s)

Virtual Electric Inc., San Jose, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

IPR2025-01150
Apple EX1071 Page 70

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: To Be Determined - pending completion of Missing Parts
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01150
Apple EX1071 Page 73

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C

CONFIRMATION NO. 4809

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

FORMALITIES LETTER

OC000000130108240

Date Mailed: 12/01/2021

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **80** basic filing fee.
- $ **80** surcharge.
- $ **350** search fee.
- $ **400** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **910** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ldvan/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C

CONFIRMATION NO. 4809

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

FORMALITIES LETTER

OC000000130108240

Date Mailed: 12/01/2021

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **80** basic filing fee.
- $ **80** surcharge.
- $ **350** search fee.
- $ **400** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **910** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ldvan/

IPR2025-01150
Apple EX1071 Page 77

Electronic Patent Application Fee Transmittal

Application Number:	17528073
Filing Date:	16-Nov-2021
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Filer:	Anthony C. Murabito/Mina Oliveri
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	80	80
UTILITY SEARCH FEE	2111	1	350	350
UTILITY EXAMINATION FEE	2311	1	400	400
Pages:				
Claims:				
Miscellaneous-Filing:				
LATE FILING FEE FOR OATH OR DECLARATION	2051	1	80	80
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with $0 paid	2252	1	320	320
Miscellaneous:				
		Total in USD ($)		**1230**

Electronic Acknowledgement Receipt	
EFS ID:	45256596
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Anthony C. Murabito/Mina Oliveri
Filer Authorized By:	Anthony C. Murabito
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Receipt Date:	17-MAR-2022
Filing Date:	16-NOV-2021
Time Stamp:	18:01:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	EFT
Payment was successfully received in RAM	$1230
RAM confirmation Number	E20223GI01353793
Deposit Account	504160
Authorized User	Mina Oliveri
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.19 (Document supply fees)	

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	notice.pdf	71700 d75fd13af1fcf453d256bbf8830d5497825ed4fc	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	49236 6086a42e2680174242ef1816e5270c4d0841152c9	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	120936		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	TBD
Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9818104		2017-11-14	KATZER; ET AL.	
	2	9105020		2015-08-11	RONCA; ET AL	
	3	8571937		2013-10-29	ROSE; ET AL	
	4	11100431		2021-08-24	MULLEN; ET AL	
	5	10037524		2018-07-31	ROYYURU; ET AL	
	6	8690055		2014-04-08	ANDERSON; ET AL	
	7	7100821		2006-09-05	RASTI	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	TBD
	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020153424		2002-10-24	LI	
	2	20110276416		2011-11-10	MULLEN, et al.	
	3	20150317632		2015-11-05	PARK, et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2012154915	WO	A1	2012-11-15	DYNAMICS INC		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	TBD
	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	TBD
	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Anthony C. Murabito/	Date (YYYY-MM-DD)	2022-03-17
Name/Print	Anthony C. Murabito	Registration Number	35295

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2012 (15.11.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/154915 A1

(51) International Patent Classification:
G06Q 40/02 (2012.01)

(21) International Application Number:
PCT/US2012/037237

(22) International Filing Date:
10 May 2012 (10.05.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/484,588	10 May 2011 (10.05.2011)	US
61/484,566	10 May 2011 (10.05.2011)	US
61/484,576	10 May 2011 (10.05.2011)	US
61/484,547	10 May 2011 (10.05.2011)	US

(71) Applicant *(for all designated States except US)*: **DYNAM¬ ICS INC.** [US/US]; 493 Nixon Road, Cheswick, PA 15024 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MULLEN, Jeffrey, D.** [US/US]; 731 South Negley Avenue, Apartment #2, Pittsburgh, PA 15232 (US). **RIGATTI, Christopher, J.** [US/US]; 321 Jacksonia Street, Pittsburgh, PA 15212 (US). **WALLACE, Michael, T.** [US/US]; 202 North Trailwood Road, Payson, AZ 15024 (US).

(74) Agent: **WALLACE, Michael, T.**; 493 Nixon Road, Cheswick, PA 15024 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(H))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: SYSTEMS, DEVICES, AND METHODS FOR MOBILE PAYMENT ACCEPTANCE, MOBILE AUTHORIZATIONS, MOBILE WALLETS, AND CONTACTLESS COMMUNICATION MECHANISMS

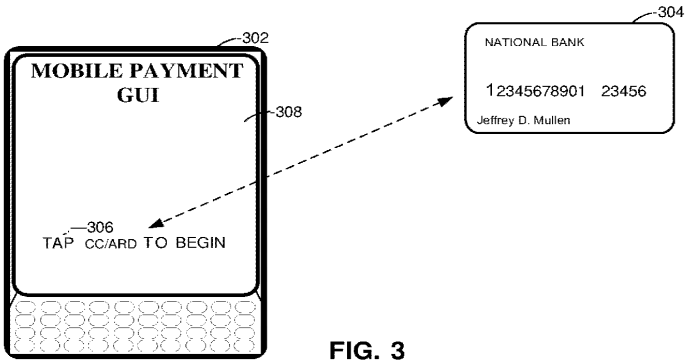


FIG. 3

(57) Abstract: A mobile device may provide payment acceptance and/or payment authorization for purchases, payments and/or money transfers by accepting payment information from a powered, or a non-powered, card using a contactless communication channel formed between the card and the mobile device. The payment information may be communicated by the mobile device to network entities that may be used to settle/authorize such purchase, payment and/or money transfer transactions. Physical cards may be presented to a mobile device to establish a contactless communication channel between the physical card and the mobile device. Information communicated by the physical card may be received, stored, and used by the mobile device to generate a mobile wallet of virtual cards.

WO 2012/154915 A1

IPR2025-01150
Apple EX1071 Page 87

SYSTEMS, DEVICES, AND METHODS FOR MOBILE PAYMENT ACCEPTANCE, MOBILE AUTHORIZATIONS, MOBILE WALLETS, AND CONTACTLESS COMMUNICATION MECHANISMS

Background of the Invention

[0001] This invention relates to mobile devices and related systems.

Summary of the Invention

[0002] A mobile device is provided that may be used as a point-of-sale terminal. A contactless communication channel may, for example, be formed between the mobile device and a payment card to communicate payment information from the payment card to the mobile device. The mobile device may, for example, use the communicated payment information to complete a purchase transaction that may be initiated by the mobile device. Accordingly, for example, no payment information need reside on the mobile terminal to complete a payment transaction. Instead, an application may be remotely activated, or a user of a mobile device may activate an application on the mobile device, that allows the mobile device to accept payment

information directly from a payment card before and/or during a payment transaction.

[0003] A mobile device may, for example, provide a browsing activity where goods and/or services may be located for purchase on a website (e.g., an Amazon or eBay website). An application may, for example, be executed on a mobile device that may communicate with a checkout application running on a website. Payment information may be exchanged directly from a user's payment card to the checkout application using the user's mobile device. In so doing, for example, a mobile device may be used as a contactless payment acceptance terminal.

[0004] A user may be provided an option of storing payment information associated with a payment card within a memory of the mobile device. Accordingly, for example, a mobile device may store payment information associated with one or more payment accounts. In so doing, for example, a mobile device may store multiple payment accounts that may be recalled from a memory of the mobile device at the user's request to complete a payment transaction.

[0005] A mobile device may detect the presence of a card that is brought within a communication distance of a contactless interface of the mobile device. For example, a card having RFID capability may communicate with an RFID device of a mobile device when the card comes within a distance (e.g., up to 2 inches) of the mobile device. Accordingly, for example, a card type (e.g., a powered card or a non-powered card) may be identified by the mobile device.

[0006] A non-powered card may, for example, communicate one, two, and/or three tracks of magnetic

stripe data to a mobile device via a contactless interface of the mobile device. Accordingly, a processor of a mobile device may identify an account type (e.g., credit or debit) that may be associated with the non-powered card by inspection of magnetic stripe data (e.g., account number) received from the non-powered card.

[0007] A powered card may, for example, communicate information (e.g., information within discretionary data fields) to a contactless interface of a mobile device. In so doing, for example, the additional information may be analyzed by a processor of the mobile device to determine that a detected card is a powered card having increased capability. Accordingly, for example, a user of a powered card may select a feature (e.g., pay with credit) on the powered card and a processor of a mobile device may detect that such a feature is selected based upon an analysis of information (e.g., discretionary data) received from the powered card.

[0008] A mobile device may validate a payment card. For example, a mobile device may request entry of a PIN after a payment card is presented to the mobile device and payment information is communicated to the mobile device by the payment card. Once entered, a mobile device may, for example, access a server associated with the payment card's issuing entity to validate the PIN. Alternately, for example, a processor of a mobile device may compare the PIN entry against local memory contents of the mobile device to validate the entered PIN.

[0009] As per another example, a mobile device may validate a payment card by requiring that the physical

payment card be present during a payment transaction. Accordingly, for example, a mobile device may require that a physical payment card be tapped against the mobile device so that a contactless communication channel may be formed between the payment card and the mobile device to verify the identity of the payment card. Accordingly, for example, identifying information communicated by the payment card to the mobile device may be compared against information previously stored within a memory of the mobile device that may be associated with the payment card.

[0010] One or more payment cards may, for example, be presented to a mobile device to complete a purchase transaction. Accordingly, for example, split-payment options may be offered by a mobile device. In so doing, for example, a first payment card may be tapped against a mobile device and accepted by the mobile device as a first form of partial payment, a second payment card may be tapped against a mobile device and accepted by the mobile device as a second form of partial payment, and so on. A mobile device may, for example, allow a user to select an amount for each partial payment and may settle each partial payment amount with each respective issuer of each payment card presented for partial payment.

[0011] A mobile device may provide checkout options to a user. For example, a mobile device may allow a user to associate purchase categories (e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile device so that the user may prepare a more detailed accounting of his or her expenditures. As per another example, a rewards card may be tapped against a mobile device so that rewards card

information may be credited with purchases transacted by the mobile device.

[0012] A mobile device may provide receipt delivery options to a user. For example, a mobile device may allow a user to select one of many receipt delivery options (e.g., text messaging, email or autonomous delivery to accounting software executed by a processor of the mobile device) . Other receipt options may be provided by a mobile device in a graphical format (e.g., a barcode) so that proof-of-purchase may be verified by a reader (e.g., a barcode reader) .

[0013] Money transfers may, for example, be transacted by a mobile device. One or more payment accounts (e.g., a car account or a utility account) may be selected by a user of a mobile device to receive a payment transacted by the mobile device. Payment information may be recalled from memory and/or entered by a user of the mobile device and then communicated to network entities by the mobile device to complete payment transactions.

[0014] Person to person transfers may, for example, be transacted by a mobile device. A user of a mobile device may, for example, tap a payment card against the mobile device to communicate source account information to the mobile device where funds are to be withdrawn. A person receiving a transfer of funds may, for example, tap his or her payment card against a device (e.g., a mobile device) to communicate target account information where funds are to be deposited. A mobile device may, for example, gather source and target account information and communicate such information to network entities to complete the funds transfer transaction .

[0015] A mobile device may, for example, provide a scanning capability (e.g., via a camera) to scan images (e.g., barcodes) that may be analyzed by a processor of the mobile device. Accordingly, for example, a mobile device may be used to scan product information from a product tag (e.g., a barcode) to select an item for purchase. As items are selected for purchase, scanned information is processed and displayed by the mobile device to produce a summary of items that may be selected for purchase. The mobile device may, for example, collect payment information from a payment card via a contactless communication channel and then use the payment information to complete a purchase transaction for the items scanned by the mobile device.

[0016] A mobile device may access electronic billing information via one or more communication capabilities of the mobile device. A merchant (e.g., a restaurant) may provide access to an electronic tab generated by the merchant (e.g., a bill generated by a restaurant for a dinner for two). Items billed by the merchant may be accessed by a user of a mobile device and displayed by the mobile device to produce a summary of items billed. The mobile device may, for example, collect payment information from a payment card via a contactless communication channel and then use the payment information to complete a purchase transaction for the billed items.

[0017] Any mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may be a point-of-sale terminal. Accordingly, for example, a mobile device may accept payment information from any payment card, communicate such payment

information via a network, complete a settlement process with network entities (e.g., an issuer or a payment server) on such a network, and provide results (e.g., an electronic receipt) of the completed purchase transaction to a user of the mobile device.

[0018] A mobile device may include a contactless communication device. Accordingly, for example, a mobile device may communicate with any card having contactless communication capability. For example, a card (e.g., a non-powered card) may include a near-field communication device (e.g., an RFID tag) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. In so doing, for example, a non-powered card may communicate one, two, and/or three tracks of magnetic stripe information to a mobile device before and/or during a purchase transaction conducted by the mobile device.

[0019] A card (e.g., a powered card) may include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device. A powered card may, for example, include a battery, a processor, memory, and a manual input interface (e.g., one or more buttons) that may allow a user of the powered card to programmably communicate information to a mobile device. For example, a powered payment card may include a feature associated with a button that allows a user to, for example, pay with credit or pay with debit. Accordingly, for example, a powered payment card may communicate such a payment selection within discretionary data fields of one or more tracks of magnetic stripe data.

[0020] A powered card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the powered card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device and processed by a processor of the mobile device as data communicated by the powered card.

[0021] A powered card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the powered card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a powered card as data communicated by a mobile device.

[0022] A powered card may, for example, include a light source (e.g., an LED) to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the powered card. A powered card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the powered card through a contactless communication channel. A mobile

device may, for example, include sound emission capabilities that may be detected by a microphone of a powered card as data communicated by the mobile device through a contactless communication channel.

[0023] A user may communicate information directly from a card to a memory location of a mobile device via a contactless communication channel between the card and the mobile device. Accordingly, for example, a mobile device may store information (e.g., payment information) associated with one or more cards (e.g., one or more payment cards) that have been presented within a proximity to the mobile device. In so doing, for example, a mobile device may be a mobile wallet having multiple accounts (e.g., payment, identification, and travel accounts) stored within a memory of the mobile wallet where each account may be recalled from a memory of the mobile wallet at the user's request to perform a function (e.g., to complete a payment transaction) .

[0024] A mobile device may detect the presence of a card that is brought within a communication distance of a contactless interface of the mobile device. A card may, for example, provide RFID capability that may communicate with an RFID device of a mobile device when the card comes within a communication distance of the mobile device. Accordingly, for example, a card type may be identified by the mobile device and information associated with the card type may be communicated from the card to the mobile device. Information received by the mobile device from the card may be autonomously categorized by the mobile device in accordance with a card type and the information may be stored and

displayed to a user in accordance with the categorization .

[0025] A card (e.g., a non-powered payment card) may, for example, communicate one, two, and/or three tracks of magnetic stripe data to a mobile device via a contactless interface. Accordingly, for example, a processor of a mobile device may identify a card type (e.g., a payment card) by analyzing the magnetic stripe data received from the card. A processor of a mobile device may, for example, determine an account type (e.g., credit or debit) that may be associated with the non-powered payment card by inspection of magnetic stripe data (e.g., account number) received from the non-powered card.

[0026] A powered card may, for example, communicate information to a contactless interface of a mobile device. In so doing, for example, additional information (e.g., information presented in discretionary data) may be identified by a processor of the mobile device to determine that a detected card is a powered card having increased capability. Accordingly, for example, a user of a powered card may select a feature (e.g., pay with credit) on the powered card and a processor of a mobile device may detect that such a feature is selected based upon an analysis of the information received from the powered card.

[0027] A mobile device may, for example, validate a payment card. For example, a mobile device may request entry of a PIN after a payment card is presented to the mobile device. Once a PIN is entered, a mobile device may, for example, access a server associated with the issuing entity to validate the PIN. A processor of a mobile device may, for example, compare the PIN entry

against memory contents of the mobile device to locally validate the entered PIN.

[0028] Data received from a card may, for example, be encrypted. Accordingly, for example, data received from a card may be stored in an encrypted state and decrypted upon receipt of a decryption key. A decryption key may, for example, be received from a sponsoring entity of the card (e.g., a card issuer's server) . Decrypted data may, for example, be destroyed such that each usage of encrypted data may require a decryption key prior to usage. Alternately, for example, decrypted data may be stored within a protected memory of the mobile device and kept for future use.

[0029] A user of a mobile device may, for example, extract physical, or real, cards (e.g., payment, identification, travel, and rewards cards) from the user's physical wallet or purse and may convert each physical card into a virtual equivalent card that resides electronically within the mobile device. Accordingly, for example, each physical card (e.g., a powered card or a non-powered card) may be brought within a proximate, or touching, relationship with a mobile device to create a contactless communication channel. Card information (e.g., cardholder data, card data, and card configuration data) may, for example, be communicated by the card to the mobile device via such a contactless communication channel. In so doing, for example, a virtual card may be created within the mobile device that is both visibly and functionally equivalent to its physical counterpart.

[0030] A non-powered card may, for example, be virtually rendered onto a display of a mobile device in

a manner that resembles its physical counterpart. Card and cardholder information may, for example, be communicated by the non-powered card to the mobile device and rendered onto a virtual card that may be displayed by a processor of the mobile device. Accordingly, for example, the functionality of the physical card (e.g., a non-powered payment card) may be imparted to the virtual card by the mobile device when the mobile device communicates information (e.g., payment information) that may be associated with the non-powered payment card. As per one example, a mobile device may communicate payment information associated with a virtual card that may be displayed on a GUI of the mobile device when the mobile device is brought within a communication distance of a merchant terminal to complete a purchase transaction (e.g., an RFID device of the mobile device may communicate with an RFID device of a merchant terminal to exchange payment information between the mobile device and the merchant terminal to complete the purchase transaction) . As per another example, a mobile device may communicate payment information associated with a virtual card when the mobile device accesses a network entity (e.g., a payment server) via a wireless network (e.g., a cellular network or a Wi-Fi hotspot) to complete a purchase transaction using the communicated payment information .

[0031] A powered card may, for example, be virtually rendered onto a display of a mobile device in a manner that resembles its physical counterpart. A powered card may, for example, be virtually rendered onto a display of a mobile device in a manner that provides user interface functionality that may be associated

with the physical counterpart. A powered card may, for example, communicate configuration information (e.g., button placement and associated functionality, display placement and associated functionality and input/output functionality) to a processor of a mobile device and the processor may render such a configuration onto a virtual card such that the configuration of the virtual card provides substantially identical functionality as compared to its physical counterpart.

[0032] As per one example, a powered card (e.g., a powered payment card) may include one or more buttons that when activated determine a method of payment to be used to complete a transaction (e.g., pressing one button may invoke a credit payment transaction while pressing another button may invoke a debit payment transaction) . Accordingly, for example, a virtual card may be rendered onto a display of a mobile device that includes the same functionality, such that when one virtual button is touched on the virtual card, a credit payment message is communicated by the mobile device and when another virtual button is touched on the virtual card, a debit payment message is communicated by the mobile device.

[0033] As per another example, a powered card may be programmed for a particular feature by pressing a button on the powered card associated with that feature. Accordingly, for example, a powered card may communicate information associated with a selected feature to a mobile device and a processor of the mobile device may render a virtual card on a GUI of the mobile device in accordance with the selected feature. In so doing, for example, a powered card may be selected as a powered payment card with a debit feature

and the selected feature may be communicated to a mobile device (e.g., the debit feature may be communicated to a mobile device within a discretionary data field of a magnetic stripe message). The resulting virtual payment card rendered onto a display of the mobile device may, for example, provide a virtual payment card having a fixed payment feature (e.g., a fixed debit payment feature).

[0034] A mobile device may, for example, challenge a user of the mobile device to enter a password (e.g., a PIN) that may be associated with a card. A mobile device may, for example, require a password before a virtual card may be created and stored within the mobile device. A mobile device may, for example, allow a virtual card to be created and stored within a mobile device, but may challenge a user of the mobile device to enter a password associated with the virtual card before it can be recalled from a memory of the mobile device and used (e.g., used to complete a purchase transaction).

[0035] A user may, for example, participate in the personalization of a virtual card that may be stored within a memory of a mobile device. A mobile device may, for example, store various logos (e.g., issuer logos, network brand logos, and merchant logos) within a memory of the mobile device and may allow a user of the mobile device to use a GUI of the mobile device to personalize an appearance of a virtual card with such logos. Accordingly, for example, a user may perform drag-and-drop operations, alphanumeric entry operations, and any other operation to personalize an appearance of a virtual card stored within a memory of the mobile device.

[0036] A processor of a mobile device may, for example, organize two or more virtual cards for display on a GUI of the mobile device. A mobile device may, for example, keep track of a number of usages of one or more virtual cards and may sort such virtual cards within a list of displayed virtual cards so that a user may easily access his or her most used virtual card from a top of the displayed list. A mobile device may, for example, track a location of a user of the mobile device and organize a list of virtual cards in accordance with such a location. Accordingly, for example, a user may be shopping within a general merchandise store (e.g., Target), a processor of the user's mobile device may track the user's position to the Target store and the processor of the user's mobile device may display a virtual card (e.g., a Target gift card) at the top of a displayed list of virtual cards based upon the user's location. In so doing, for example, a virtual card most pertinent to the user's location may be sorted to the top of a displayed list of virtual cards for easy and convenient access by the user .

[0037] A user may, for example, select one virtual card from a list of virtual cards presented by a GUI of a mobile device and may perform one of many operations on the selected virtual card. A user may, for example, conduct a purchase transaction using a virtual payment card selected from a list of virtual cards. Accordingly, for example, a user may place a mobile device within a vicinity of a merchant terminal and may communicate payment information associated with a selected payment card to the merchant terminal. As per another example, payment information associated with a

selected virtual card may be communicated to a network entity (e.g., a payment server or an issuer's server) by the mobile device to complete a purchase transaction .

[0038] A mobile device may, for example, receive an electronic receipt for the purchase transaction either via a communication channel established between the mobile device and the merchant terminal or via other communication channels (e.g., text messaging or email exchange with a network entity such as a payment server) . A user may, for example, view documents (e.g., receipts or bank statements) that may be associated with a virtual card. Accordingly, for example, a mobile device may collect and store documents associated with a virtual payment card and may display the associated documents upon request from the user. A GUI of a mobile device may, for example, allow a user to annotate documents that may be associated with a virtual card (e.g., a user may make a note that may be electronically attached to an electronic receipt that may be associated with a virtual payment card) .

[0039] Other cards (e.g., other virtual cards) may be associated with a selected virtual card and those associations may be viewed from a GUI of the mobile device. For example, a payment card may be associated with a rewards card, such that in response to a request from a user of a mobile device, a processor of the mobile device may display the associations to the payment card and may use the associated virtual cards in support of a purchase transaction (e.g., the associated rewards card may be used during a payment transaction conducted with the selected virtual payment

card so that the rewards account may accrue rewards points for the purchase transaction) .

[0040] A mobile device may, for example, allow a user of the mobile device to cancel an account that may be associated with a virtual card stored within the mobile device. Accordingly, for example, a virtual payment card may be stored within a mobile device and may be associated with a payment account that is administered by an issuing entity of the payment account. A mobile device may, for example, communicate with such an issuing entity to cancel a payment account that may be associated with a virtual payment card stored within the mobile device. A mobile device may, for example, negotiate with other issuing entities to determine when new payment card offers may be available and to allow a user of the mobile device to accept such payment card offers. Once accepted, a user of a mobile device may conduct other transactions with the newly accepted payment card offers (e.g., account balance (s) associated with existing virtual cards may be transferred to the newly accepted payment card via a request made by the mobile device and an issuing server) .

[0041] Any mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may be a mobile wallet. Accordingly, for example, a mobile device may accept payment and other information from any payment card, store and display such information as a virtual card on a GUI of the mobile device, communicate such payment information via a wired and/or a wireless network, complete a settlement process with network entities (e.g., an

issuer or a payment server) on such a network, and provide results (e.g., an electronic receipt) of the completed purchase transaction to a display of the mobile device.

[0042] A mobile device may include a contactless communication device. Accordingly, for example, a mobile device may communicate with any card having contactless communication capability. For example, a card (e.g., a non-powered card) may include a near-field communication device (e.g., an RFID tag) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. In so doing, for example, a non-powered card may communicate one, two, and/or three tracks of magnetic stripe information to a mobile device before and/or during a purchase transaction conducted by the mobile device.

[0043] A card (e.g., a powered card) may include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device. A powered card may, for example, include a battery, a processor, memory, and a manual input interface (e.g., one or more buttons) that may allow a user of the powered card to programmably communicate information to a mobile device. For example, a powered payment card may include a feature associated with a button that allows a user to, for example, pay with credit or pay with debit. Accordingly, for example, a powered payment card may communicate such a payment selection within discretionary data fields of one or more tracks of magnetic stripe data.

[0044] A powered card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the powered card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device and processed by a processor of the mobile device as data communicated by the powered card.

[0045] A powered card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the powered card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a powered card as data communicated by a mobile device.

[0046] A powered card may, for example, include a light source (e.g., an LED) to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the powered card. A powered card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the powered card through a contactless communication channel. A mobile

device may, for example, include sound emission capabilities that may be detected by a microphone of a powered card as data communicated by the mobile device through a contactless communication channel.

[0047] A mobile device may be used as an authorization terminal to conduct transactions (e.g., purchase transactions) using the mobile device. Purchase transactions may, for example, be completed by a mobile device using payment information stored within a memory of the mobile device. In order to conduct a purchase transaction, a processor of a mobile device may, for example, first require security credentials to authorize a purchase transaction. Security credentials may, for example, be any type of information that may be communicated to a mobile device by a contactless device using a contactless communication channel (e.g., an RFID communication channel) .

[0048] Security credentials may, for example, be payment information that may be communicated to a processor of a mobile device by a payment card (e.g., a powered or a non-powered payment card) . Accordingly, for example, if payment information communicated to a processor of a mobile device by a physical payment card matches payment information previously stored within a memory of the mobile device, the mobile device may authorize the purchase transaction.

[0049] As per an example, a mobile device may receive payment information (e.g., a payment account number and an expiration date) from a payment card via a contactless communication channel and may store such payment information within a memory of the mobile device for future use. Prior to conducting a requested purchase transaction, a processor of a mobile device

may first require that a physical payment card be used to authorize the purchase transaction. Accordingly, for example, the same physical payment card that was used to originally communicate payment information to a processor of the mobile device may be required to once again communicate payment information in order to authorize the purchase transaction. Upon verification that the newly communicated payment information matches at least a portion of payment information contained within a memory of the mobile device, the mobile device may authorize the payment transaction.

[0050] A powered card may, for example, communicate security credentials that may contain a dynamic security code and other information (e.g., at least a portion of a payment account number or a cardholder's name) . Accordingly, for example, an application executed by a processor of a mobile device may synchronize with a dynamic security code generation algorithm that may be executed by a processor of the powered card. In so doing, for example, a processor of the mobile device may generate a dynamic security code in accordance with the security code generation algorithm and may compare the generated dynamic security code to a security code received from a powered card during authorization of a purchase transaction. If a match exists, for example, the purchase transaction may be authorized by the mobile device .

[0051] A mobile device may, for example, communicate security credentials received from a physical card via a contactless communication channel to a network entity (e.g., an authorization server) . Accordingly, for example, the authorization server may analyze the

received security credentials and may either confirm or deny that the security credentials are authentic. A message may, for example, be communicated from the authorization server to the mobile device to either authorize or deny the purchase transaction.

[0052] A mobile device may, for example, arrange security credentials (e.g., payment information) stored within a memory of the mobile device as one or more virtual payment cards that may be provided on a display of the mobile device. Accordingly, for example, a user of a mobile device may select one or more virtual cards from a displayed list of virtual cards for use during a purchase transaction. In so doing, for example, a user may retrieve a physical payment card from his or her wallet that corresponds to the virtual payment card selected for use and may communicate (e.g., via a contactless communication channel) payment information from the physical payment card to a processor of the mobile device. Upon verification that the communicated payment information matches at least a portion of payment information stored within a memory of the mobile device, a processor of the mobile device may authorize the purchase transaction using the stored payment information.

[0053] A physical payment card may, for example, be used as a master physical payment card to authorize purchase transactions that are to be completed by the mobile device using stored payment information that does not match payment information received from the physical payment card. For example, a master physical payment card may be associated with a particular issuer and a mobile device may store several virtual cards within a memory of the mobile device having the same

issuer. Upon receipt of payment information from the master physical payment card, a processor of a mobile device may authorize purchase transactions using one or more virtual cards stored within a memory of the mobile device that may share the same issuer as the issuer of the master physical payment card.

[0054] Other devices (e.g., RFID enabled keys) may, for example, communicate security credentials via a contactless communication channel to a processor of a mobile device to authorize other transactions (e.g., non-purchase transactions) that may be conducted by the mobile device. Accordingly, for example, a processor of a mobile device may communicate commands to a wireless device (e.g., a user's car) to perform certain functions (e.g., start the engine of the user's car). In so doing, for example, a user may present an ignition key to the mobile device to communicate security credentials (e.g., a key code matched to the user's car) from the ignition key to the mobile device to authorize the requested function. Upon verification that the key code matches the key code of the user's car, for example, a processor of the mobile device may authorize the requested function and may communicate the associated command to the user's car to execute the requested function.

[0055] Any function may, for example, be authorized to be performed by a processor of a mobile device. Accordingly, for example, any decision to perform a function by a mobile device may be authorized by a processor of the mobile device. In so doing, for example, any function (e.g., checking a balance of a banking account or transitioning from paper bank statements to e-statements) that may be performed by a

processor of a mobile device may be authorized by the processor upon verification that security credentials (e.g., a bank account number) communicated to the processor from a contactless communication device (e.g., a bank card associated with the bank account) matches at least a portion of security credentials (e.g., banking information) that may be stored within a memory of the mobile device.

[0056] Any mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may be an authorization terminal. Accordingly, for example, any mobile device may accept payment information from any physical payment card, store such payment information within a memory of the mobile device, require that the same (or associated) physical payment card communicate payment information to a processor of the mobile device, and complete a purchase transaction with network entities (e.g., an issuer or a payment server) upon verification that the communicated payment information matches at least a portion of payment information stored within a memory of the mobile device .

[0057] A mobile device may include a contactless communication device. Accordingly, for example, a mobile device may communicate with any card having contactless communication capability. For example, a card (e.g., a non-powered card) may include a near-field communication device (e.g., an RFID tag) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. In so doing, for example, a non-powered card may communicate one,

two, and/or three tracks of magnetic stripe information to a processor of a mobile device before and/or during a purchase transaction conducted by the mobile device.

[0058] A card (e.g., a powered card) may include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device. A powered card may, for example, include a battery, a processor, memory, and a manual input interface (e.g., one or more buttons) that may allow a user of the powered card to programmably communicate information to a mobile device. For example, a powered payment card may include a feature associated with a button that allows a user to, for example, pay with credit or pay with debit. Accordingly, for example, a powered payment card may communicate such a payment selection within discretionary data fields of one or more tracks of magnetic stripe data.

[0059] A powered card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the powered card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device and processed by a processor of the mobile device as data communicated by the powered card.

[0060] A powered card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a

display of a mobile device and information may be communicated from the mobile device to the powered card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a powered card as data communicated by a mobile device.

[0061] A powered card may, for example, include a light source (e.g., an LED) to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the powered card. A powered card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the powered card through a contactless communication channel. A mobile device may, for example, include sound emission capabilities that may be detected by a microphone of a powered card as data communicated by the mobile device through a contactless communication channel.

[0062] A card may include a dynamic magnetic communications device, which may take the form of a magnetic encoder or a magnetic emulator. A magnetic encoder, for example, may be utilized to modify information that is located on a magnetic medium, such that a magnetic stripe reader may then be utilized to read the modified magnetic information from the magnetic medium. A magnetic emulator, for example, may be provided to generate electromagnetic fields that directly communicate data to a read-head of a magnetic stripe reader. A magnetic emulator, for example, may

communicate data serially to a read-head of the magnetic stripe reader. A magnetic emulator, for example, may communicate data in parallel to a read-head of the magnetic stripe reader.

[0063] All, or substantially all, of the front surface, as well as the rear surface, of a card may be implemented as a display (e.g., bi-stable, non bi-stable, LCD, or electrochromic display) . Electrodes of a display may be coupled to one or more touch sensors, such that a display may be sensitive to touch (e.g., using a finger or a pointing device) and may be further sensitive to a location of the touch. The display may be sensitive, for example, to objects that come within a proximity of the display without actually touching the display.

[0064] A dynamic magnetic stripe communications device may be implemented on a multiple layer board (e.g., a two-layer flexible printed circuit board) . A coil for each track of information that is to be communicated by the dynamic magnetic stripe communications device may then be provided by including wire segments on each layer and interconnecting the wire segments through layer interconnections to create a coil. For example, a dynamic magnetic stripe communications device may include two coils such that two tracks of information may be communicated to two different read-heads included in a read-head housing of a magnetic stripe reader. A dynamic magnetic communications device may include, for example, three coils such that three tracks of information may be communicated to three different read-heads included in a read-head housing of a magnetic stripe reader.

[0065] Input and/or output devices may be included on a card, for example, to facilitate data exchange with the card. For example, an integrated circuit (IC) may be included on a card and exposed from the surface of the card. Such a chip (e.g., an EMV chip) may communicate information to a chip reader (e.g., an EMV chip reader) . A contactless device (e.g., one or more RFID antennas and one or more associated RFID chips) may be included in a card, for example, to exchange information with an RFID device.

[0066] One or more detectors may be provided in a card, for example, to sense the presence of an external object, such as a person or device, which in turn, may trigger the initiation of a communication sequence with the external object. The sensed presence of the external object may then be communicated to a processor of the card, which in turn may direct the exchange of information between a card and the external object. Accordingly, timing aspects of the information exchange between an external object and the various I/O devices provided on a card may also be determined by circuitry (e.g., a processor) provided on a card.

[0067] The sensed presence of the external object or device may include the type of object or device that is detected and, therefore, may then determine the type of communication that is to be used with the detected object or device. For example, a detected object may include a determination that the object is a read-head housing of a magnetic stripe reader. Such an identifying detection, for example, may activate a dynamic magnetic stripe communications device so that information may be communicated to the read-head of the magnetic stripe reader. Information may be

communicated by a dynamic magnetic stripe communications device, for example, by re-writing magnetic information on a magnetic medium that is able to be read by a magnetic stripe reader or electromagnetically communicating data to the magnetic stripe reader.

[0068] As per another example, a detected object may include a determination that the object is an RFID enabled device. Such an identifying detection, for example, may cause RFID data to be communicated by a processor of a card to an RFID chip of a card. The RFID data may be temporarily contained within the RFID chip until the RFID data is communicated to a detected RFID device by an RFID antenna on the card. The RFID data may, for example, be erased from the RFID chip after being communicated to the RFID device.

[0069] A card may, for example, be an assembly of multiple printed circuit boards, electronics, one or more RFID antennas, and one or more associated RFID chips. An RFID antenna may, for example, be fabricated on one printed circuit board and an associated RFID chip may, for example, be attached to a separate printed circuit board. Communications (e.g., RFID data transfer between the RFID chip and the RFID antenna) may, for example, be transferred between separate printed circuit boards via conductive paths established between the separate printed circuit boards. An RFID antenna and an associated RFID chip may, for example, reside on the same printed circuit board so as to reduce a number of conductive traces that may be required between separate printed circuit boards.

[0070] A card assembly may, for example, be laminated such that all printed circuit boards,

electronic circuitry and components are covered in a polymer. For example, an electronics package may be provided between two layers of polymer and a liquid polymer may be introduced between these layers and hardened to form a card. A laminated card assembly may, for example, be devoid of electrical contacts on either surface of the laminated card. A laminated card assembly may, for example, provide electrical contacts (e.g., EMV chip contacts) on one or more surfaces of a laminated card assembly.

[0071] A mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may include one or more RFID antennas and associated RFID chips. Accordingly, for example, any mobile device may establish an RFID communication channel with any other RFID enabled device (e.g., an RFID enabled card) . A computing device, such as a desktop computer, may be an RFID enabled device. Accordingly, for example, any RFID enabled device (e.g., an RFID enabled card or an RFID enabled mobile device) may establish an RFID communication channel with any RFID enabled computing device.

Brief Description of the Drawings

[0072] The principles and advantages of the present invention can be more clearly understood from the following detailed description considered in conjunction with the following drawings, in which the same reference numerals denote the same structural elements throughout, and in which:

[0073] FIG. 1 is an illustration of a mobile devices constructed in accordance with the principles of the present invention;

[0074] FIG. 2 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0075] FIG. 3 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0076] FIG. 4 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0077] FIG. 5 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0078] FIG. 6 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0079] FIG. 7 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0080] FIG. 8 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0081] FIG. 9 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0082] FIG. 10 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0083] FIG. 11 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0084] FIG. 12 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0085] FIG. 13 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0086] FIG. 14 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0087] FIG. 15 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0088] FIG. 16 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0089] FIG. 17 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0090] FIG. 18 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0091] FIG. 19 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0092] FIG. 20 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0093] FIG. 21 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0094] FIG. 22 is an illustration of a mobile funds transfer system constructed in accordance with the principles of the present invention;

[0095] FIG. 23 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0096] FIG. 24 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0097] FIG. 25 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0098] FIG. 26 is a flow chart of processes constructed in accordance with the principles of the present invention;

[0099] FIG. 27 is an illustration of a mobile devices constructed in accordance with the principles of the present invention;

[0100] FIG. 28 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0101] FIG. 29 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0102] FIG. 30 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0103] FIG. 31 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0104] FIG. 32 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0105] FIG. 33 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0106] **FIG.** 34 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0107] **FIG.** 35 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0108] **FIG.** 36 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0109] **FIG.** 37 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0110] **FIG.** 38 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0111] **FIG.** 39 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0112] **FIG.** 40 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0113] **FIG.** 41 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0114] **FIG.** 42 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0115] **FIG.** 43 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0116] **FIG.** 44 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0117] **FIG.** 45 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0118] **FIG.** 46 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0119] **FIG.** 47 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0120] **FIG.** 48 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0121] **FIG.** 49 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0122] **FIG.** 50 is an illustration of a mobile application constructed in accordance with the principles of the present invention;

[0123] **FIG.** 51 is a flow chart of processes constructed in accordance with the principles of the present invention;

[0124] **FIG.** 52 is an illustration of mobile devices constructed in accordance with the principles of the present invention;

[0125] **FIG.** 53 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0126] **FIG.** 54 is an illustration of a mobile authorization system constructed in accordance with the principles of the present invention;

[0127] **FIG.** 55 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0128] **FIG.** 56 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0129] **FIG.** 57 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0130] **FIG.** 58 is an illustration of a mobile authorization system constructed in accordance with the principles of the present invention;

[0131] **FIG.** 59 is an illustration of a mobile authorization system constructed in accordance with the principles of the present invention;

[0132] **FIG.** 60 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0133] **FIG.** 61 is a flow chart of processes constructed in accordance with the principles of the present invention;

[0134] **FIG.** 62 is an illustration of cards constructed in accordance with the principles of the present invention;

[0135] **FIG.** 63 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0136] **FIG.** 64 is an illustration of mobile devices constructed in accordance with the principles of the present invention;

[0137] **FIG.** 65 is an illustration of a card constructed in accordance with the principles of the present invention;

[0138] **FIG.** 66 is an illustration of a card constructed in accordance with the principles of the present invention;

[0139] FIG. 67 is an illustration of a card constructed in accordance with the principles of the present invention;

[0140] FIG. 68 is an illustration of a card constructed in accordance with the principles of the present invention;

[0141] FIG. 69 is an illustration of a card constructed in accordance with the principles of the present invention;

[0142] FIG. 70 is an illustration of a card constructed in accordance with the principles of the present invention;

[0143] FIG. 71 is an illustration of a system constructed in accordance with the principles of the present invention;

[0144] FIG. 72 is an illustration of a system constructed in accordance with the principles of the present invention; and

[0145] FIG. 73 is an illustration of process flow charts constructed in accordance with the principles of the present invention.

Detailed Description of the Invention

[0146] FIG. 1 shows mobile device 100. Mobile device 100 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device) . Accordingly, mobile device 100 may be operated in a mobile environment while a user of mobile device 100 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising) . In addition, for example, mobile device 100 may perform multiple functions

simultaneously (e.g., a person may carry on a conversation while at the same time browsing and purchasing products on the internet).

[0147] Mobile device 100 may include audio processing devices (e.g., microphone 108 and speaker 110). Accordingly, for example, mobile device 100 may receive voice commands from a user via microphone 108 and may process such commands to perform a function. For example, a user may place mobile device 100 into a desired operational mode by speaking a command into microphone 108 that is associated with the desired operational mode. In so doing, for example, mobile device 100 may engage in hands-free operation by receiving voice commands via microphone 108 and performing functions associated with the received voice commands.

[0148] Mobile device 100 may receive data input via microphone 108. For example, a voice-band modem may generate signals in a voice-band frequency range that may be received by microphone 108. A processor of mobile device 100 may interpret the received audible information as data signals and may process the data signals as, for example, data values and/or control data input.

[0149] Mobile device 100 may include camera 102. Camera 102 may capture one or more frames of video data and store the video data within a memory of mobile device 100. Accordingly, for example, a processor of mobile device 100 may receive one or more frames of video information via camera 102 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 100 may receive optical information that is sensed by camera

102 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 100 as data values and/or control data.

[0150] Mobile device 100 may include manual input interface 112. Manual input interface 112 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 100 may enter information into mobile device 100 via manual interface 112 to cause a processor of mobile device 100 to enter a particular mode of operation. Manual interface 112 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile device 100) during a particular mode of operation of mobile device 100.

[0151] Mobile device 100 may include display 104. Display 104 may provide visible information that may be utilized by a user during interaction with mobile device 100. A portion or all of display 104 may be touch sensitive such that objects making contact with display 104 or objects coming within a proximity of display 104 may be detected by a processor of mobile device 100. Accordingly, for example, mobile payment graphical user interface 106 may be provided by display 104 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, textual input

boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 100.

[0152] FIG. 1 shows architecture 150. User interface 152 may, for example, be included within architecture 150 to allow user interaction with architecture 150. For example, a dedicated key pad or keyboard may be included within user interface 152 to allow alphanumeric data entry into architecture 150.

[0153] Architecture 150 may include one or more displays 154. Display 154 may, for example, be touch-sensitive. Accordingly, for example, display 154 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 154. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of display 154 may be detected by processor 158 as alphanumeric data entry.

[0154] Alphanumeric entry boxes may, for example, be rendered onto display 154. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 152 and/or a virtual keypad rendered onto display 154 to select alphanumeric characters to be placed within the alphanumeric entry box in accordance with a character position identified by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 158 may receive alphanumeric characters as typed into a alphanumeric entry box of display 154 and may use such alphanumeric characters as data input.

[0155] Display 154 may, for example, provide data output from architecture 150. For example, display 154 may communicate data using a series of light pulses. Accordingly, for example, processor 158 may cause one or more portions of display 154 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 154 via light pulses having varying characteristics. Display 154 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode) .

[0156] Architecture 150 may include one or more transceivers 156. Transceiver 156 may communicate information to and/or may receive information from one or more devices. Transceiver 156 may, for example, communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly, for example, transceiver 156 may allow a mobile device (e.g., mobile device 100 of FIG. 1) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 100 of FIG. 1) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 156 may exchange information with one or more other mobile devices via one or more associated cellular stations .

[0157] Transceiver 156 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 156 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 156 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 100 of FIG. 1) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network .

[0158] Architecture 150 may include contactless communication device 162, which may communicate via any one or more contactless communication methodologies, such as for example, near field communications (e.g., RFID) , Bluetooth, touch simulation, light pulsing (e.g., via an LED), and electromagnetic data communication (e.g., via a dynamic magnetic stripe communications device) . Accordingly, for example, contactless communication device 162 may be compatible with any contactless device, such as for example, an RFID enabled payment card and a contactless reader (e.g., a magnetic stripe reader or an NFC reader) .

[0159] A non-powered card may, for example, communicate with contactless communications device 162.

Contactless communication device 162 may, for example, establish a carrier field (e.g., an RF field) that may be modulated by a device (e.g., an RFID tag) of a non-powered payment card. In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by contactless communications device 162 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 162 by modulating the RF field produced by contactless communications device 162.

[0160] A powered card may, for example, communicate with contactless communication device 162. A powered card may, for example, include a processor, a battery, a memory, wireless communications devices (e.g., a dynamic magnetic stripe communications device or RFID) and other electronics (e.g., buttons) that may allow a user to interact with the powered card to perform one or more functions. Accordingly, for example, a powered card may be used to communicate specific information to contactless communication device 162 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 162 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications .

[0161] Contactless communication device 162 may receive variable data sets from a powered card based upon, for example, manual input provided to a powered card. For example, a button associated with an on-line

purchase may be pressed on the powered card that causes a variable data set (e.g., account number and expiration date) to be communicated from the powered card to contactless communication device 162.

[0162] Discretionary data may, for example, be communicated by a powered card based upon which button was pressed on the powered card. In so doing, for example, a security code (e.g., "111") may be communicated within a discretionary data field when a button associated with a particular feature (e.g., pay with credit) is pressed on the powered card. As per another example, a different security code (e.g., "222") may be communicated within a discretionary data field when a button associated with a different feature (e.g., pay with debit) is pressed on the powered card. Accordingly, for example, processor 158 may identify what type of device may be in communication with contactless communication device 162 by analyzing the data communicated to contactless communication device 162.

[0163] Architecture 150 may include memory 160 and/or processor 158 may include internal memory. Accordingly, for example, application code may be stored within memory 160 and/or processor 158 and executed by processor 158 in support of functions performed by architecture 150. For example, an application (e.g., a graphical user interface) may be executed by architecture 150 and displayed onto display 154, which may be used to interact with a user of a mobile device (e.g., mobile device 100 of FIG. 1). Persons skilled in the art will appreciate that executable application code may be communicated to architecture 150 via any one or more interfaces of

architecture 150 (e.g., user interface 152, display 154, transceiver 156, and/or contactless communication device 162).

[0164] Application data (e.g., payment card data) may be stored within memory 160 and accessed by processor 158 during operation. For example, payment card data may be stored within memory 160 and recalled by processor 158 during a financial transaction being conducted by a mobile device (e.g., mobile device 100 of FIG. 1). Once recalled, processor 158 may communicate the payment card data via transceiver 156 and/or contactless communication device 162 to complete a financial transaction.

[0165] FIG. 2 shows network topology 200 that may include, for example, mobile device 202 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile device 202 may, for example, include a contactless interface that may initiate, sustain, and/or terminate communication channel 226 between contactless device 204 and mobile device 202. Contactless device 204 and mobile device 202 may communicate via channel 226 using any number of contactless mediums, which may include for example, visible, audible, capacitive, electromagnetic, magnetic, and/or RF mediums.

[0166] Mobile device 202 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 212 and/or payment network 214) and/or one or more wireless networks (e.g., mobile network 210). Mobile device 202 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile device 202 to communicate

information (e.g., voice and data) to cellular network access infrastructure 206 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 206 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0167] Mobile device 202 may, for example, communicate with wireless access point 208 over a wireless interface (e.g., a Bluetooth interface or a Wi-Fi interface). Accordingly, for example, mobile device 202 may access one or more wired networks (e.g., IP network 212 and/or payment network 214) and/or one or more wireless networks (e.g., mobile network 210) without the need to first gain access to cellular network access infrastructure 206.

[0168] Contactless device 204 may, for example, be a powered card or a non-powered card (e.g., a powered payment card or a non-powered payment card). Accordingly, for example, payment information (e.g., a payment account number and a card expiration date) may be communicated from contactless device 204 to mobile device 202 in support of a financial transaction being conducted by mobile device 202. In so doing, for example, items for purchase on IP network 212 (e.g., the internet) may be accessed by a browser of mobile device 202 via an access point (e.g., wireless access point 208 or cellular network access infrastructure 206). Mobile device 202 may, for example, complete a purchase transaction by first obtaining required payment information from contactless device 204 and

then communicating such payment information to network entities (e.g., payment server 216 and/or issuer 220).

[0169] Payment server 216 may, for example, contact issuer 220 via a network (e.g., payment network 214) with payment information received from mobile device 202 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile device 202 via any one or more delivery options (e.g., via a short messaging service of mobile network 210 or an email delivery service of IP network 212).

[0170] A payment receipt may, for example, be provided to mobile device 202 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile device 202 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0171] A mobile device (e.g., mobile device 224) may, for example, include a contactless communication device (e.g., an RFID) that may initiate, sustain, and/or terminate contactless communication channel 228 with merchant terminal 218. Accordingly, for example, mobile device 224 may communicate payment information to merchant terminal 218 to complete a financial transaction. In so doing, for example, mobile device 224 may first receive payment information via contactless communication channel 230 from contactless device 222 (e.g., a non-powered card), temporarily store the received payment information within a memory of mobile device 224, and forward the payment information onto merchant terminal 218 to complete a financial transaction. As per another example, mobile device 224 may provide previously stored financial

information associated with one or more payment cards (e.g., one or more non-powered payment cards). Accordingly, for example, payment information may be recalled from a memory of mobile device 224 and communicated to merchant terminal 218 via contactless communication channel 228 to complete a financial transaction using merchant terminal 218.

[0172] FIG. 3 shows system 300, which may include mobile device 302 and payment card 304. Mobile device 302 may, for example, be a laptop computer, a PDA, a mobile telephonic device (e.g., a smartphone), an MP3 player, a GPS, or any other mobile device. Display 308 may be a touch-sensitive display (e.g., sensitive to a change in capacitance). Payment card 304 may, for example, be a powered payment card or a non-powered payment card.

[0173] Mobile device 302 and payment card 304 may each include a contactless communication device (e.g., RFID) that may communicate via a contactless communication channel that may be formed between mobile device 302 and payment card 304 after coming into proximity to one another. Payment card 304 may, for example, be tapped onto display 308 of mobile device 302 to establish a proximity relationship that forms a communication channel between payment card 304 and mobile device 302. As per another example, payment card 304 may be brought within a proximity distance (e.g., up to two inches) of mobile device 302 to establish a contactless communication channel between mobile device 302 and payment card 304.

[0174] A processor of mobile device 302 may, for example, execute application code that may generate a graphical user interface (GUI) onto display 308 of

mobile device 302. Message 306 of a GUI may invite a user of mobile device 302 to begin a mobile payment by tapping a payment card against display 308. As per another example, by tapping payment card 304 against mobile device 302, mobile device 302 may autonomously determine that a mobile payment is desired and then generate a mobile payment GUI onto display 302.

[0175] Mobile device 302 may, for example, autonomously determine a type of card that may be tapped against it. For example, a processor of mobile device 302 may receive payment card data that may be indicative of a non-powered payment card (e.g., payment card data received from a non-powered card may not provide a security code associated with the card). As per another example, a processor of mobile device 302 may receive data that may be indicative of a powered card (e.g., payment card data received may contain a dynamically generated security code). Payment card data received from a powered card may, for example, include a dynamic security code that may change depending upon a type of transaction being conducted (e.g., debit or credit transaction).

[0176] As per another example, payment card 304 may be a powered payment card that may include electronics to simulate a human touch (e.g., payment card 304 may generate a change in capacitance that may be sensed by display 308). Through a series of simulated touches, payment card 304 may communicate a series of data bits to display 308, which may then be processed by a processor of mobile device 302. In so doing, for example, a contactless communication channel may be established where data is transferred from payment card

304 to mobile device 302 via a series of simulated touches .

[0177] Payment card 304 may, for example, include a light sensor. Accordingly, for example, payment card 304 may be sensitive to light pulses generated within a region of display 308. The light sensor of payment card 304 may receive a series of light pulses, which may be construed by a processor of payment card 304 as data generated by mobile device 302. In so doing, for example, payment card 304 may receive an optical data stream represented by a series of light pulses generated by display 308. As such, a two-way communication channel may be formed, where simulated touches may generate a data stream from payment card 304 to mobile device 302 and light pulses may generate a data stream from mobile device 302 to payment card 304 .

[0178] FIG. 4 shows GUI 400, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 400 may, for example, generate results of a card detection operation that may be performed by a processor of a mobile device. For example, card information may be exchanged between a card and a mobile device via a contactless communication channel that may identify a type of card that is being presented to the mobile device. Any type of card may be detected by a processor of a mobile device, such as for example, an airline card, a travel card, a bank card, a healthcare card, an identification card, and a loyalty rewards card. A card number communicated to a mobile device may, for example, be indicative of a card type (e.g., bank card 404) that is presented to a mobile device. Accordingly, for

example, a processor of a mobile device may identify a card type presented to the mobile device by analyzing a card number received from the card and may indicate the identified card type via GUI 400 (e.g., the identified card type may be generated onto GUI 400 having a different graphical presentation than the other card types listed) .

[0179] A GUI may, for example, provide navigation aids. A GUI may, for example, provide navigation aids that may be touch sensitive. For example, GUI 400 may include navigation aids 406 and 408 to enable a user to revert to a previous GUI or advance to a subsequent GUI. Accordingly, for example, a user may touch an area on a display of a mobile device that displays a navigation aid to activate the touched navigation aid. In so doing, for example, a user may touch navigation aid 406 to revert to the previous GUI or a user may touch navigation aid 408 to advance to the next GUI.

[0180] FIG. 5 shows GUI 500, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 500 may, for example, generate results of a payment card detection operation that may be performed by a processor of a mobile device. A non-powered payment card may, for example, communicate a single payment card number that may be associated with a number of payment options (e.g., debit, credit, or points). Accordingly, for example, GUI 500 may be generated to allow a user an opportunity to select which payment option (e.g., credit option 502) from a number of payment options is to be used to settle a payment transaction. Once identified, a payment option selection (e.g., credit option 502) may be communicated by a mobile device to

an issuer of the payment card to settle the transaction using the selected payment option.

[0181] As per another example, a powered payment card may include a user interface to allow a user to select from a number of payment options. A button on a powered payment card may, for example, be associated with one payment method (e.g., pay with credit) and another button may, for example, be associated with another payment method (e.g., pay with points). Data associated with the selected payment method may be communicated from a powered payment card to a mobile device. Accordingly, for example, a processor of a mobile device may detect the payment method communicated by a powered payment card (e.g., as communicated within a discretionary data field) and may autonomously generate a graphical representation of the payment method selected (e.g., GUI 500 may autonomously generate a graphical representation that credit method 502 was selected).

[0182] FIG. 6 shows GUI 600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 600 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. A mobile device may, for example, challenge a user of the mobile device to enter a PIN that may be associated with a payment card (e.g., VISA credit 602) that was previously presented to the mobile device for payment. GUI 600 may, for example, generate virtual pin pad 606 that may include touch-sensitive buttons having alphanumeric indicia associated with each button. A user may touch one or more buttons of pin pad 606 that may correspond to respective characters of a PIN and an

indication of the user's selection may appear within area 604. Characters displayed within area 604 may, for example, be hidden for security purposes.

[0183] Activation of virtual button 608 may, for example, cause a processor of a mobile device to compare a PIN entered by a user of the mobile device to a PIN that may be associated with the payment card presented to the mobile device for payment. The PIN may, for example, be stored within protected memory of the mobile device, so that a processor of the mobile device may locally determine the validity of the PIN entered. Alternately, for example, the mobile device may communicate the PIN to the issuing bank for a remote validation of the PIN entered. Persons skilled in the art will appreciate that a user interface (e.g., a keypad or keyboard) of a mobile device may be used instead of virtual pin pad 606 to enter the one or more characters of a PIN.

[0184] FIG. 7 shows GUI 700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 700 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. A mobile device may, for example, challenge a user of the mobile device to enter a security code that may be associated with a payment card (e.g., VISA credit 702) that was previously presented to the mobile device for payment. Such a security code (e.g., a CVV code) may, for example, be printed on the back of the payment card.

[0185] GUI 700 may, for example, generate virtual pin pad 706 that may include touch-sensitive buttons having alphanumeric indicia associated with each

button. A user may touch one or more buttons of pin pad 706 that may correspond to respective characters of a security code and an indication of the user's selection may appear within area 704. Characters displayed within area 704 may, for example, be hidden for security purposes.

[0186] Activation of virtual button 708 may, for example, cause a processor of a mobile device to compare a security code entered by a user of the mobile device to a security code that may be associated with the payment card presented to the mobile device for payment. The security code may, for example, be stored within protected memory of the mobile device, so that a processor of the mobile device may locally determine the validity of the security code entered. Alternately, for example, the mobile device may communicate the security code to the issuing bank for a remote validation of the security code entered. Persons skilled in the art will appreciate that a user interface (e.g., a keypad or keyboard) of a mobile device may be used instead of virtual pin pad 706 to enter the one or more characters of a security code.

[0187] FIG. 8 shows GUI 800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 800 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. A mobile device may, for example, maintain memory of one or more payment cards previously presented to the mobile device for payment. A mobile device may, for example, allow a user to store payment information within the mobile device that may be associated with a payment card to be used at some point in the future.

[0188] Accordingly, for example, a user may recall payment information previously stored in memory of a mobile device in order to complete a purchase transaction using the mobile device. In order to validate that a user of a mobile device is actually the owner of payment information recalled from memory of the mobile device, GUI 800 may challenge the user to present the physical payment card whose associated payment information was recalled from memory. In so doing, for example, GUI 800 may prevent a fraudulent user of a mobile device from authorizing a purchase using payment information stored in memory of the mobile device that is not owned by the fraudulent user.

[0189] A user may, for example, be required to present a physical payment card to GUI 800 by placing (or tapping) the physical payment card within a proximity of a display of a mobile device that is generating GUI 800. In so doing, for example, a contactless communication channel (e.g., an RFID communication channel) may be established between the physical payment card and the mobile device, such that payment information may be communicated from the physical payment card to the mobile device. Upon verification that the communicated payment information matches payment information stored in memory of the mobile device, the payment information may be validated and authorized to be communicated from the mobile device to a network entity (e.g., a payment server or the issuer of the payment card) for settlement of the purchase transaction.

[0190] FIG. 9 shows GUI 900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 900 may, for

example, include validation area 902 as generated by a processor of a mobile device. Validation area 902 may, for example, include one or more data exchange areas (e.g., data exchange areas 904 and 906). Icon 904 may, for example, be generated by GUI 900 within an area of a display of a mobile device that may be sensitive to touch (e.g., an area that may be sensitive to a capacitance change) . Area 906 may, for example, be generated by GUI 900 within an area of a display of a mobile device that may generate pulses of light.

[0191] A powered payment card may be validated for use by a mobile device through an exchange data with the powered payment card via data exchange areas 904 and 906. For example, a powered payment card may be pressed against validation area 902 so that a touch simulation device of the powered payment card aligns with data exchange area 904 and a light sensing device aligns with data exchange area 906. Accordingly, for example, the powered payment card may communicate information to a processor of a mobile device by simulating a series of touches in data exchange area 904 and data may be communicated to the powered payment card by a processor of the mobile device by generating a series of light pulses in data exchange area 906. In so doing, for example, a mobile device and a powered payment card may exchange validation information so that payment card information stored within the mobile device may be validated for use.

[0192] A mobile device may, for example, include a motion capture device (e.g., a camera) and a powered payment card may, for example, include a light source (e.g., an LED) . Accordingly, for example, information (e.g., validation information) may be exchanged between

a mobile device and a powered payment card such that information communicated by the powered payment card may be communicated as a series of light pulses while the camera of the mobile device captures the series of light pulses. A processor of the mobile device may construe the series of light pulses as information that may be used, for example, as validation information.

[0193] FIG. 10 shows GUI 1000 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1000 may be generated, for example, after payment card information has been communicated by either of a non-powered payment card or a powered payment card to a mobile device. A user of a mobile device may, for example, elect whether to store such payment card information within a memory location of the mobile device. If a user chooses not to store payment information received from a payment card (e.g., as elected by selection of radio button 1004), a mobile device may delete all payment information previously received from a payment card after the payment information is used to complete a purchase transaction. Accordingly, a user wishing to use the same payment card to complete a payment transaction in the future is required to present the payment card to the mobile device so that the payment card may communicate payment card information to the mobile device in order to complete the payment transaction. If a user chooses to store payment information received from a payment card (e.g., as elected by selection of radio button 1002), a mobile device may store a portion of, or all, payment information previously received from a payment card in accordance with a user's preference.

[0194] FIG. 11 shows GUI 1100 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1100 may, for example, offer storage options to a user of a mobile device that has elected to store a portion of, or all, payment card information previously communicated to the mobile device by a non-powered card or a powered card. A data storage option may, for example, be selected by a user of a mobile device (e.g., by touching a portion of text box 1102) that stores only a portion (e.g., an expiration date and payment card account number) of the payment card information into a memory of the mobile device. Accordingly, for example, a payment card may communicate one, two, and/or three tracks of magnetic stripe data to a mobile device, but the only payment information stored within a memory of the mobile device upon selection of text box 1102 is the expiration date and the payment card account number. All remaining information that may have been communicated by the payment card to the mobile device may be deleted by the mobile device .

[0195] Selection of text box 1104 may, for example, cause all payment information communicated by a payment card to a mobile device to be stored within a memory of the mobile device. Accordingly, for example, a mobile device may use a portion or all of the payment information stored within its memory to complete a purchase transaction. However, payment card validation information (e.g., a PIN or security code) may still be required to be entered by a user of the mobile device before the mobile device may complete a purchase transaction with the stored payment information.

[0196] Selection of box 1106 may, for example, cause all payment information communicated by a payment card to a mobile device to be stored within a memory of the mobile device. All validation information (e.g., a PIN or security code) that may be entered by a user of the mobile device to validate payment information received from a payment card may also be stored within a memory of the mobile device. Accordingly, for example, a mobile device may use a portion or all of the payment information, including validation information, stored within its memory to complete a purchase transaction.

[0197] Selection of box 1108 may, for example, cause all payment information, including discretionary data fields, communicated by a payment card to a mobile device to be stored within a memory of the mobile device. A powered payment card may, for example, allow a user of the powered payment card to select one or more options that may be associated with the powered payment card. A powered payment card may, for example, communicate indicia associated with the one or more selected options within discretionary data fields of magnetic stripe data that may be communicated to a mobile device .

[0198] For example, a user of a powered payment card may elect to pay for a purchase using rewards points by pressing a button on the powered payment card that is associated with a rewards points payment option. Accordingly, for example, a powered payment card may insert a rewards points payment code within a discretionary data field of a first, a second and/or a third track of magnetic stripe data and may communicate all track data, including the discretionary data field, to a mobile device. In so doing, for example, a

processor of a mobile device may detect such a payment code within a discretionary data field and may store payment information within a memory of the mobile device that is indicative of the rewards points payment code contained within the discretionary data field.

[0199] FIG. 12 shows GUI 1200 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1200 may, for example, offer a split-payment option to a user of a mobile device, such that the user may elect to split payment for a selected purchase between two or more payment accounts. The mobile device may, for example, communicate payment information for each of the selected split-payment accounts to respective network entities (e.g., issuer and payment servers) of the selected split-payment accounts in order to settle the amounts owing on each of the selected split-payment accounts .

[0200] A user may, for example, select option 1202 (e.g., by tapping a payment card against a display of a mobile device or by presenting a payment card within proximity to the mobile device) . In so doing, for example, a contactless communication channel (e.g., an RFID communication channel) may be established between the payment card and the mobile device so that payment information associated with the payment card may be communicated by the payment card to the mobile device and used as a split-payment account for a selected purchase .

[0201] An alternate contactless communication channel may be established, for example, by pressing a payment card against portion 1208. Accordingly, for example, a payment card may communicate payment

information associated with the payment card to a processor of a mobile device by simulating a series of touches at a location within portion 1208 (e.g., at icon 1210) and the processor of the mobile device may communicate information to the payment card by generating a series of light pulses at a location within portion 1208 (e.g., at location 1212) . In so doing, for example, payment information associated with the payment card may be received by a processor of a mobile device and used as a split-payment account to partially cover the purchase price of a selected purchase .

[0202] Other contactless communication channels may be established. For example, a processor of a payment card may communicate payment information to a mobile device by generating a series of light pulses (e.g., via an LED of the payment card) , which may be captured by a camera of the mobile device and construed by a processor of the mobile device as payment information. As per another example, a payment card may communicate payment information using audible sounds that may be received by a microphone of a mobile device and construed by a processor of the mobile device as payment information.

[0203] A payment account may, for example, be selected from a memory of the mobile device (e.g., by selecting radio button 1204) . Associated payment information may, for example, be selectively retrieved from a memory of the mobile device and used by the mobile device as a split-payment account in partial payment for a selected purchase. Alternately, for example, a split-payment option may be declined by a

user of a mobile device (e.g., by selecting radio button 1206).

[0204] FIG. 13 shows GUI 1300 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1300 may, for example, provide a summary of split-payment methods that may have been selected by a user of a mobile device. Portion 1302, for example, may display an amount owing for a particular selected purchase. Portions 1304-1308 may, for example, include an alphanumeric entry box to allow a user of a mobile device to input payment amounts (e.g., currency or points) that he or she wishes to apply towards a total amount owing as may be displayed in portion 1302. Portions 1304-1308 may, for example, include those payment accounts that a user of a mobile device previously selected as split-payment accounts.

[0205] Accordingly, for example, a user may elect to charge $10 against a VISA credit account, $35 against a M/C debit account, and 500 rewards points earned by the VISA credit account towards full payment of a $50 amount owing for a particular selected purchase. In so doing, for example, a mobile device may communicate with selected network entities (e.g., issuer and payment servers) to provide transaction information associated with each split-payment account selected, so that each amount owing may be settled.

[0206] Portions 1310-1314 may, for example, include alphanumeric entry boxes to allow a user of a mobile device to make comments on each account selected as a split-payment account. Accordingly, for example, a mobile device may communicate notes that may be entered by a user within portions 1310-1314 to, for example, a

payment server. In so doing, for example, receipts and/or account statements that may be generated by a network entity (e.g., an issuer or a payment server) may include such notes so that a user of a mobile device, upon receipt of such receipts and/or account statements, may be reminded of his or her thought process when such a split-payment was transacted.

[0207] FIG. 14 shows GUI 1400 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1400 may, for example, offer checkout options to a user of a mobile device to allow a level of integration between the user and one or more issuers of associated payment accounts used by the mobile device in settlement of a selected purchase.

[0208] For example, a user may utilize billing tag list 1402 to categorize a selected purchase into one of many purchase categories. A user's physical presence may, for example, be at a fast-food establishment where the user may select a food purchase from the fast-food establishment's website using a browser of the user's mobile device. Payment information used to settle a transaction associated with the selected food purchase may be collected and/or generated by the mobile device and forwarded onto a payment server and/or an associated issuer for settlement. In addition, the mobile device may forward a billing tag selected from billing tag list 1402 to the associated issuer, so that the associated issuer may label the selected transaction on a billing statement using the selected billing tag. In so doing, for example, a user may customize an accounting of the issuer's billing statement by using a mobile device to communicate

payment information and billing tags associated with selected purchases to track expenditures within the various purchase categories of billing tag list 1402.

[0209] A user of a mobile device may select receipt delivery options for each purchase that may be transacted using a mobile device. For example, a receipt delivery list may be generated by a processor of a mobile device so that a user of the mobile device may select a receipt delivery option. Accordingly, for example, the selected receipt delivery option along with payment information may be communicated by a mobile device to a payment server and the payment server (or other entity) may direct a delivery of the receipt based upon the receipt delivery option received .

[0210] A user may, for example, request delivery of a purchase receipt via text messaging (e.g., by selecting receipt delivery option 1406) . In so doing, for example, a mobile device may complete a purchase transaction with an entity of a payment network (e.g., a payment server) and may further request that the payment server deliver a receipt to the mobile device in a text message format. Accordingly, for example, in addition to providing payment information to the payment server, a mobile device may also provide a text message address (e.g., an SMS text message address) to the payment server. In so doing, for example, the mobile device may receive a receipt of the completed purchase transaction from the payment server via a text message at the text message address provided by the mobile device .

[0211] As per another example, a multimedia message (e.g., an MMS message containing rich content) may be

received by a mobile device from a payment server in the form of, for example, a graphical image (e.g., barcode), such that the barcode may be used as a proof-of-purchase (e.g., proof-of-purchase of an airline ticket and an associated barcode that gains access by the user of the mobile device to a particular seating assignment on the airplane.)

[0212] A receipt (e.g., a receipt received via multimedia messaging) may, for example, provide rewards to a user of the mobile device for completing payment transactions via a mobile device. For example, a mobile device may communicate indicia to a payment server that identifies a payment transaction as a mobile payment transaction. The communicated mobile payment indicia may, for example, trigger a payment server to not only provide a receipt for the purchase transaction to the mobile device, but also to provide a multimedia game that may be executed by the mobile device. As per an example, an animated trivia question may be communicated to a mobile device via an MMS message upon completion of a mobile payment transaction. Upon successfully answering the animated trivia question, a user of the mobile device may receive another MMS message that contains a coupon for free merchandise from the merchant whose goods were just purchased. As per another example, a receipt received from a payment server may itself contain coupons for discounted or free merchandise without requiring that a user of the mobile device perform any further actions beyond completing a mobile payment purchase with a mobile device.

[0213] A user may, for example, request delivery of a purchase receipt via email (e.g., by selecting

receipt delivery option 1408) . In so doing, for example, an email address associated with the user may be provided by the mobile device to a payment server in addition to any required payment information that may be required to complete a purchase transaction. Accordingly, for example, a payment server may address a receipt to an email address received from a mobile device during a mobile payment transaction.

[0214] A user may, for example, request delivery of a purchase receipt (e.g., by selecting receipt delivery option 1410) via a format that may be compatible with an accounting software package (e.g., QuickBooks) . For example, a mobile device may allow a user to categorize a particular purchase within a particular expense account (e.g., an office supply expense account) during a purchase transaction. Once the purchase transaction is completed, an electronic receipt may be communicated to the mobile device that may be tagged with the categorized expense account (e.g., the accounting software package may have its own address that receipts may be delivered to) . In so doing, for example, an accounting software package that may be executing on the mobile device may autonomously access the electronic receipt from its own address and may autonomously enter the expense in the correct category so that all purchases made by the mobile device may be correctly accounted for within the accounting software package .

[0215] A user may, for example, request delivery of a purchase receipt (e.g., by selecting receipt delivery option 1412) via a format that may be compatible with the bank that issued the selected payment account. Accordingly, for example, a payment server may forward

a receipt of the purchase transaction to the issuing bank and the issuing bank may format the receipt for delivery with the user's month-end account statement.

[0216] A user may, for example, enter comments about a purchase transaction that may be included within a receipt. For example, a user may enter comments 1404 that may remind the user to include the receipt within his or her tax records because the purchase may be deemed as tax deductible. Accordingly, for example, comments 1404 may accompany payment information communicated by a mobile device to a payment server. In so doing, for example, a payment server may add comments 1404 to a receipt generated by the payment server and may forward the receipt with the added comments to the user of the mobile device as dictated by the receipt delivery options requested by the user of the mobile device.

[0217] FIG. 15 shows GUI 1500 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1500 may, for example, offer a check-out option to a user of a mobile device, such that the user may elect to apply a rewards card to a selected purchase in order for the rewards card to accrue points for the purchase. The mobile device may, for example, submit rewards card information and transaction information to respective issuers of the rewards account so that the respective issuers may credit the rewards account accordingly.

[0218] A user may, for example, select option 1502 (e.g., by tapping a rewards card against a display of a mobile device or by presenting a rewards card within proximity to the mobile device) . In so doing, for example, a contactless communication channel (e.g., an

RFID communication channel) may be established between the rewards card and the mobile device so that information associated with the rewards card may be communicated by the rewards card to the mobile device.

[0219] An alternate contactless communication channel may be established, for example, by pressing a rewards card against portion 1508. Accordingly, for example, a rewards card may communicate information associated with the rewards card to a processor of a mobile device by simulating a series of touches within portion 1508 (e.g., at icon 1510) and the processor of the mobile device may communicate information to the rewards card by generating a series of light pulses within portion 1508 (e.g., at location 1512). In so doing, for example, rewards information associated with the rewards card may be received by a mobile device and communicated to an issuer of the rewards card so that the rewards account may be updated with the purchase transaction information.

[0220] Other contactless communication channels may be established. For example, a processor of a rewards card may communicate rewards information to a mobile device by generating a series of light pulses (e.g., via an LED of the rewards card), which may be captured by a camera of the mobile device and construed by a processor of the mobile device as rewards information. As per another example, a payment card may communicate payment information using audible sounds that may be received by a microphone of a mobile device and construed by a processor of the mobile device as payment information.

[0221] A rewards account may, for example, be selected from a memory of the mobile device (e.g., by

selecting radio button 1504) . Associated rewards information may, for example, be selectively retrieved from a memory of the mobile device and communicated by the mobile device to an issuer of the rewards account so that the rewards account may be credited with the selected purchase.

[0222] A user of a mobile device may, for example, place an order for a rewards card by selecting radio button 1506. Accordingly, for example, a mobile device may communicate payment information to a payment server to complete a purchase transaction and may also communicate a request that a rewards account be created. A payment server may, for example, forward the rewards account creation request to an issuer of a rewards account along with details of the purchase transaction, so that the issuer may first create the rewards account and may then credit the account according to the purchase transaction. Accordingly, for example, an electronic version of a newly created rewards card (e.g., a graphical representation of a newly created rewards card) may, for example, be communicated to a mobile device which may, for example, include a barcode representation of the rewards account information. In addition, rewards card information may, for example, be added to a memory of a mobile device for future access.

[0223] FIG. 16 shows GUI 1600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1600 may, for example, challenge a user of a mobile device to enter an access code that may be required to authenticate a purchase transaction. GUI 1600 may, for example, include virtual keyboard 1604 to allow a user of a

mobile device to enter such an access code. Alternately, for example, a manual input interface of a mobile device (e.g., a keyboard or a keypad) may be used to enter such an access code.

[0224] As a user of a mobile device enters each character of an access code, portion 1602 may reflect such entry. Such entries may, for example, be reflected within portion 1602 as protected characters (e.g., the actual value of each character may be blocked out) to protect the security and safety of the entered access code. Once an entered access code is verified and authenticated by a mobile device, the mobile device may complete the requested purchase transaction .

[0225] FIG. 17 shows GUI 1700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1700 may, for example, include portion 1702 that may display a graphical representation of a proof-of-purchase (e.g., a barcode) . Such a proof-of-purchase may be communicated to a mobile device via a network entity (e.g., a payment server) upon completion of a purchase transaction by the mobile device.

[0226] Accordingly, for example, portion 1702 may graphically display a proof-of-purchase that may be recognized by a reader (e.g., a barcode reader) . In so doing, for example, a system that may include a barcode reader may verify the validity of a proof-of-purchase barcode, which may then allow a user of a mobile device displaying such a barcode to enjoy the goods and/or services purchased by the user via the mobile device as acknowledged by the verified barcode. As per one example, such a verified barcode may allow entry onto

an airplane having a seat assignment that is encoded within the barcode. As per another example, a user may have made an on-line purchase of an appliance using his or her mobile device and may have requested pick-up of the purchased appliance at an appliance inventory warehouse. Upon arrival at the appliance inventory warehouse, a user may retrieve an electronic proof-of-purchase (e.g., a barcode) from a memory of the mobile device that was received by the user's mobile device upon completion of the appliance purchase transaction. A reader (e.g., a barcode reader) at the appliance inventory warehouse may read the user's barcode directly from a display of the user's mobile device, verify that a purchase was completed by the user's mobile device, and may authorize the appliance for pickup by the user.

[0227] FIG. 18 shows GUI 1800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1800 may, for example, enable a funds transfer to one or more financial accounts. GUI 1800 may, for example, enable a transfer of funds (e.g., by selecting radio button 1802) directly from one or more financial accounts into one or more financial accounts. GUI 1800 may, for example, generate a communication channel with a recipient of a funds transfer (e.g., by selecting radio button 1804) and may allow the recipient to interactively determine the financial account that is to receive the transferred funds.

[0228] FIG. 19 shows GUI 1900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1900 may, for example, enable a funds transfer to one or more

accounts. GUI 1900 may, for example, allow a user of a mobile device to select an object (e.g., by selecting an entry within menu list 1902) that may be associated with the funds transfer. GUI 1900 may, for example, allow a user to select an account (e.g., by selecting an entry within menu list 1904) that may be associated with the object selected within menu list 1902.

[0229] Accordingly, for example, a mobile device may include a memory within which a user may enter one or more potential recipients of a funds transfer. A processor of a mobile device may, for example, list each potential recipient of a funds transfer within menu list 1902. A user of a mobile device may, for example, select a recipient of a funds transfer by activating (e.g., touching) an entry within menu list 1902 that corresponds to the selected recipient. As per an example, a user's funds transfer recipient list, as may be reflected by menu list 1902, may include persons, financial accounts, inanimate objects, or any other type of object.

[0230] Once a selected funds transfer recipient is selected within menu list 1902, menu list 1904 may be populated. Accordingly, for example, a mobile device may include a memory within which a user may enter one or more accounts that may be associated with one or more potential recipients of a funds transfer. A processor of a mobile device may, for example, list each account in menu list 1904 that may be associated with the selected recipient of menu list 1902. A user of a mobile device may, for example, select an account for a funds transfer by activating (e.g., touching) an entry within menu list 1904 that corresponds to the selected account. As per an example, a user's funds

transfer account list, as may be reflected by menu list 1904, may include any account that may be associated with the selected recipient of menu list 1902.

[0231] FIG. 20 shows GUI 2000 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 2000 may, for example, enable a funds transfer from a source account (e.g., an account associated with a payment card that is tapped against a display of a mobile device) to a target account (e.g., a car loan account). Portion 2002 may, for example, list account details that may be associated with a target account (e.g., an account number associated with a car loan, the payoff amount, and the amount due). Portion 2002 may, for example, include details that may be associated with a target account that a mobile device has collected from a network entity (e.g., a bank) via a network connection between the mobile device and the network entity.

[0232] Portion 2004 (e.g., an alphanumeric entry box) may, for example, allow a user of a mobile device to enter an amount to be transferred (e.g., an amount that is equal to the minimum amount due on an installment payment agreement). GUI 2000 may, for example, request an identification of a source account from which the amount will be transferred. As per an example, a user of a mobile device may tap a payment card against a display of the mobile device to establish a contactless communication channel between the payment card and the mobile device within which payment information may be communicated from the payment card to the mobile device. As per another example, a payment card may communicate payment information to a mobile device via a series of touch

simulations (e.g., changes in capacitance generated by a payment card that may be detected by a touch-sensitive display of a mobile device) . A series of light pulses, or audible information, for example, may be communicated by the payment card to the mobile device in order to communicate payment information.

[0233] GUI 2000 may, for example, display a summary of payment information that may have been received by a mobile device from a payment card via a contactless communication channel. For example, portion 2006 may be displayed by GUI 2000 to allow a user of a mobile device to confirm the identity of a payment account from which an amount of money will be transferred. Once confirmed, the mobile device may communicate with network entities (e.g., an issuer of the source account and a bank associated with the target account) to complete the money transfer.

[0234] FIG. 21 shows GUI 2100 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 2100 may, for example, enable a funds transfer to an account associated with a person. A recipient may, for example, interactively select an account into which the funds will be transferred. Accordingly, for example, contact list 2102 may be displayed by GUI 2100 as a list of potential recipients of a money transfer. Contact method list 2104 may, for example, by displayed by GUI 2100 as a list of methods that may be used to contact the recipient as selected within contact list 2102. In so doing, for example, a person within contact list 2102 (e.g., Trace) may be selected by a user of a mobile device to be the recipient of a funds transfer and the recipient may be contacted, for

example, in accordance with a method selected in contact method list 2104 (e.g., transfer alert) .

[0235] FIG. 22 shows system 2200, which may include mobile device 2202, receiving device 2204, and network 2210. Mobile device 2202 may be a device used to coordinate a money transfer and receiving device 2204 may be a device used to coordinate receipt of a money transfer. Receiving device may, for example, be a mobile device. Receiving device, for example, may not be a mobile device (e.g., a desktop computer) . Devices 2202-2204 may communicate via network 2210, which may include any combination of cellular network resources, wireless network resources, and/or wired network resources .

[0236] Mobile device 2202 may, for example, include a processor that may render money transfer GUI 2206 onto a display of mobile device 2202. GUI 2206 may, for example, pause while a user of mobile device 2202 selects a payment account from which a money transfer may be withdrawn. Accordingly, for example, mobile device 2202 may wait until a payment card is brought within a proximity to, or a touch relationship with, mobile device 2202 (e.g., a payment card may be tapped onto a display of mobile device 2202) . Alternately, for example, a payment card may communicate with mobile device 2202 using any number of contactless methods (e.g., using light, sound, capacitive, magnetic or electromagnetic communication) . In so doing, for example, mobile device 2202 may establish a contactless communication channel with a payment card in which payment information is communicated from the payment card to mobile device 2202 and is summarized onto GUI 2206 for review by a user of mobile device 2202. A

user of mobile device 2202 may enter an amount of money for transfer, may verify a money amount for transfer, and may enter a message to be communicated to receiving device 2204 .

[0237] Mobile device 2202 may communicate payment information received from a payment card along with information received from a user of mobile device 2202 to a network entity (e.g., an issuer) where, for example, authorization of the transfer amount from the account selected is performed. Once authorized, mobile device 2202 may communicate a transfer alert along with a transfer alert message to receiving device 2204. Receiving device 2204 may, for example, present a transfer alert along with the associated transfer alert message onto GUI 2208. A user of receiving device 2204 may respond to the transfer alert message received from mobile device 2202 by sending an acknowledgment message to mobile device 2202 via network 2210.

[0238] A user of receiving device 2204 may, for example, be asked to enter account information that is to be used as the receiving account for the money transfer. Accordingly, for example, a user of receiving device 2204 may provide such account information any number of ways. For example, a payment card associated with a receiving account may be brought within a proximity, or a touching, relationship to receiving device 2204. In so doing, for example, a contactless communication channel (e.g., an RFID channel) may be formed to communicate such information. Alternately, a payment card may communicate with receiving device 2204 using any number of contactless methods (e.g., using light, sound, capacitive, magnetic or electromagnetic communication) . A user of receiving

device 2204 may verify the receive account information as it may be displayed onto GUI 2208.

[0239] Receiving device 2204 may, for example, communicate information associated with a receiving account to mobile device 2202 via network 2210. Accordingly, for example, mobile device 2202 may coordinate the money transfer via network 2210 with network entities (e.g., an issuer of the account used to provide money to transfer and an issuer of the account used to receive money for transfer) . Once the money transfer is completed, an acknowledgment message may be displayed onto GUI 2206 by a processor of mobile device 2202 and an acknowledgment message may be communicated by mobile device 2202 to receiving device 2204 and then displayed onto GUI 2208 by a processor of receiving device 2204.

[0240] FIG. 23 shows system 2300, which may include a mobile device 2302, a powered or non-powered payment card 2304, a remote application 2308 and network 2306. Mobile device 2302 may, for example, access remote application 2308 via network 2306 in order to complete a purchase transaction. Accordingly, for example, payment card 2304 may communicate payment information to mobile device 2302 via contactless communication channel 2312 and mobile device 2302 may communicate the payment information to remote application 2308 via communication channel 2310 to complete the purchase transaction .

[0241] Contactless communication channel 2312 may be any type of contactless communication channel, such as for example, an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel. Contactless communication channel 2312 may be a two-way

communication channel, where mobile device 2302 may communicate with payment card 2304 in order to, for example, enhance data communication between mobile device 2302 and payment card 2304 .

[0242] As per one example, payment card 2304 may communicate payment information (e.g., one, two, and/or three tracks of magnetic stripe data) to mobile device 2302 after payment card 2304 is tapped against mobile device 2302. Remote application 2308 may, for example, be an on-line payment application that does not require a fully populated magnetic stripe message to complete a purchase transaction, but may only require a subset of a fully populated magnetic stripe message (e.g., account number and expiration date) . Accordingly, for example, mobile device 2302 may filter payment information received from payment card 2304 to only include the subset of information that may be required by remote application 2308 and may communicate only the filtered payment information to remote application 2308 to complete the purchase transaction.

[0243] In general, for example, mobile device 2302 may filter payment information received from payment card 2304 into a filtered subset of payment data that may be required by remote application 2308 to complete a purchase transaction. In so doing, for example, mobile device 2302 may customize a payment message to remote application 2308 that includes only the filtered subset of data that is needed by remote application 2308 to complete the purchase transaction.

[0244] As per another example, mobile device 2302 may query payment card 2304 via contactless communication channel 2312 for only a subset of payment information that may be required by remote application

2308 to complete a purchase transaction. Accordingly, for example, a processor of payment card 2304 may receive the request and may only supply the requested payment information via contactless communication channel 2312 instead of communicating a complete magnetic stripe message.

[0245] FIG. 24 shows system 2400, which may include a mobile device 2402, a payment card 2404, a rewards card 2416, and items to be purchased 2410-2414. Mobile device 2402 may, for example, include a scanning device (e.g., a camera) that may be used to capture images (e.g., barcode images) . Accordingly, for example, a user of mobile device 2402 may activate an application within mobile device 2402 that generates GUI 2408 and that activates a camera to capture barcode images. A processor of mobile device 2402 may, for example, analyze captured barcode images to extract information from the barcode images and construe the extracted information as data input. Accordingly, for example, a camera of mobile device 2402 may be used to scan barcodes of items that the user wishes to purchase and a processor of mobile device 2402 may analyze the scanned information to keep a running total of items selected for purchase. In so doing, for example, a user of mobile device 2402 may wander through a shopping market while scanning barcode labels of items for purchase (e.g., items 2410-2414).

[0246] Mobile device 2402 may access a network (e.g., a local Wi-Fi hotspot) within a shopping market to determine those items that may be offered at a discount to rewards members of the shopping market. Accordingly, for example, a user may scan barcode image 2418 of rewards card 2416 to obtain an instant credit

for discounted items for purchase. As per another example, rewards card 2416 may establish a contactless communication channel with mobile device 2402 so that rewards card 2416 may communicate rewards account information to mobile device 2402 via any one of a number of contactless communication mediums (e.g., RF, capacitive, audible, visible, electromagnetic, or magnetic communication mediums) .

[0247] Once a user of mobile device 2402 finishes shopping, the user may present payment card 2404 to mobile device 2402 for payment. Accordingly, for example, contactless communication channel 2406 (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be created and payment information may be communicated from payment card 2404 to mobile device 2402 so that mobile device 2402 may complete the purchase transaction with a network entity (e.g., an issuer of payment card 2404) .

[0248] FIG. 25 shows system 2500, which may include mobile device 2502 and payment card 2504. Mobile device 2502 may interact with a merchant establishment (e.g., a restaurant) to gain entry into a user's tab at the merchant's establishment (e.g., a food and alcohol bill generated by the restaurant) . Accordingly, for example, a user may monitor each item on the bill, enter an additional amount into the bill (e.g., a tip), and then pay the bill all from the convenience of the user's mobile device 2502.

[0249] Interaction with a merchant establishment may be accomplished any number of ways. For example, mobile device 2502 may access a local Wi-Fi hotspot and may communicate information (e.g., an email address or text messaging address) to the merchant that identifies

a user of mobile device 2502. Accordingly, for example, a merchant may send a message (e.g., an email or text message) to the user-supplied address that may contain a link to the user's bill. A user may, for example, click on the link, enter a pass code to gain entry to the user's bill, and then monitor the bill being generated onto a display of mobile device 2502 via GUI 2508.

[0250] As per another example, mobile device 2502 may place a phone call to a merchant's phone number to establish a communication channel (e.g., a data call) between the merchant server and mobile device 2502. The merchant server may, for example, render GUI 2508 onto a display of mobile device 2502 so that a user of mobile device 2502 may directly interact with the merchant server.

[0251] GUI 2508 may be rendered onto a display of mobile device 2502 to allow a user to remotely interact with his or her bill. For example, a user's meal tab at a restaurant may be itemized by GUI 2508 and an alphanumeric entry box (e.g., box 2510) may allow the user to enter additional data (e.g., add a tip to the bill) . A user may, for example, review a total to be charged, verify such a total, and then present payment card 2504 to mobile device 2502 to settle the total amount. In so doing, for example, contactless communication channel 2506 may receive payment information from payment card 2504 via any number of contactless communication mediums (e.g., RF, capacitive, audible, visible, electromagnetic, or magnetic communication mediums) and may communicate such payment information to a network entity (e.g., an

issuer of payment card 2504) to complete a purchase transaction for the total amount of the user's bill.

[0252] FIG. 26 shows flow charts for process sequences 2610-2650. Process sequence 2610 may, for example, execute a payment application on a mobile device (e.g., as in step 2611) to request a user of the mobile device to present a payment card to the mobile device. In step 2612, a user may present a payment card (e.g., tap a payment card onto a display of a mobile device) to begin a payment transaction. In step 2613, a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a payment card and a mobile device to communicate payment information from the payment card to the mobile device. In step 2614, a purchase may be completed by a mobile device by communicating received payment information to network entities to settle a payment transaction.

[0253] Process sequence 2620 may, for example, autonomously detect that a payment card is in a touching or a proximity relationship to a mobile device (e.g., as in step 2621). In step 2622, a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a payment card and a mobile device to communicate payment information from the payment card to the mobile device. In step 2623, a purchase may be completed by a mobile device by communicating received payment information to network entities to settle a payment transaction.

[0254] Step 2631 of sequence 2630 may include presenting a card to a mobile device. A card may, for

example, be a powered card or a non-powered card. In steps 2632 and 2633, a contactless communication channel may be established between a card and a mobile device and information may be exchanged between the card and the mobile device.

[0255] A card may, for example, include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. A card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device.

[0256] A card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a card as data communicated by a mobile device.

[0257] A card may, for example, include a light source (e.g., an LED) to form a contactless communication channel. Accordingly, for example, a card may emit varying light pulses from an LED that may

be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the card. A card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the card through a contactless communication channel. A mobile device may, for example, include sound emission capabilities that may be detected by a microphone of a card as data communicated by the mobile device through a contactless communication channel.

[0258] Step 2641 of sequence 2640 may include selecting items for purchase using a mobile device. A mobile device may, for example, include a scanning device (e.g., a camera) that may be used by a mobile device to capture images of barcodes that may be associated with items for purchase (e.g., grocery items in a grocery store). Accordingly, for example, a mobile device may collect images of barcodes and a processor of the mobile device may analyze the images to retrieve information (e.g., item description and cost) of each item scanned. Each item's description, cost and other information may, for example, be displayed on a GUI that may be generated by a processor and presented to a display of the mobile device as in step 2642. A payment card may, for example, be presented to the mobile device (e.g., as in step 2643) and payment information may be exchanged between the payment card and the mobile device (e.g., as in step 2644) via a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel). In step 2645, a mobile device may communicate received payment

information to network entities (e.g., a payment server and/or an issuer) to complete the transaction.

[0259] In step 2651 of sequence 2650, for example, a mobile device may remotely access an electronic bill. For example, a merchant (e.g., a restaurant) may provide access to a bill (e.g., a restaurant tab for food and beverages) to a patron of the merchant via that patron's mobile device. As per one example, a merchant may provide a link to a bill via a message (e.g., an email message or a text message) that may be sent by the merchant to the patron's mobile device or that may be sent by the patron's mobile device to the merchant. The patron may click on the link and may be taken to a website that may provide access to the patron's tab via a browser that may be executing on the patron's mobile device. As per another example, a data call between a patron's mobile device and a merchant may execute an application (e.g., locally on the patron's mobile device and/or remotely on a merchant's server) to allow a patron to review his or her bill.

[0260] Each item on the patron's bill may, for example, include a description, cost and other information and may be displayed on a GUI that may be generated by a processor and presented to a display of the mobile device as in step 2652. A payment card may, for example, be presented to the mobile device (e.g., as in step 2653) and payment information may be exchanged between the payment card and the mobile device (e.g., as in step 2654) via a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel). In step 2655, a mobile device may communicate received payment information to network

entities (e.g., a payment server and/or an issuer) to complete the transaction.

[0261] FIG. 27 shows mobile device 2700. Mobile device 2700 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, for example, mobile device 2700 may be operated in a mobile environment while a user of mobile device 2700 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 2700 may perform multiple functions simultaneously (e.g., a person may carry on a conversation while at the same time browsing and purchasing products on the internet).

[0262] Mobile device 2700 may include audio processing devices (e.g., microphone 2708 and speaker 2710). Accordingly, for example, mobile device 2700 may receive voice commands from a user via microphone 2708 and may process such commands to perform a function. For example, a user may place mobile device 2700 into a desired operational mode by speaking a command into microphone 2708 that is associated with the desired operational mode. In so doing, for example, mobile device 2700 may engage in hands-free operation by receiving voice commands via microphone 108 and performing functions associated with the received voice commands.

[0263] Mobile device 2700 may receive data input via microphone 2708. For example, a voice-band modem may generate signals in a voice-band frequency range that may be received by microphone 2708. A processor of mobile device 2700 may interpret the received audible

information as data signals and may process the data signals as, for example, data values and/or control data input .

[0264] Mobile device 2700 may include camera 2702. Camera 2702 may capture one or more frames of video data and store the video data within a memory of mobile device 2700. Accordingly, for example, a processor of mobile device 2700 may receive one or more frames of video information via camera 2702 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 2700 may receive optical information that is sensed by camera 2702 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 2700 as data values and/or control data.

[0265] Mobile device 2700 may include manual input interface 2712. Manual input interface 2712 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 2700 may enter information into mobile device 2700 via manual interface 2712 to cause a processor of mobile device 2700 to enter a particular mode of operation. Manual interface 2712 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile device 2700) during a particular mode of operation of mobile device 2700.

[0266] Mobile device 2700 may include display 2704. Display 2704 may provide visible information that may be utilized by a user during interaction with mobile device 2700. A portion or all of display 2704 may be touch sensitive such that objects making contact with display 2704 or objects coming within a proximity of display 2704 may be detected by a processor of mobile device 2700. Accordingly, for example, mobile wallet graphical user interface 2706 may be provided by display 2704 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, textual input boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 2700.

[0267] Display 2704 may, for example, display graphical objects that may interact with a user of mobile device 2700. Accordingly, for example, a virtual card (e.g., a virtual payment card) may be rendered onto display 2704 having interactive components associated with such a virtual payment card. In so doing, for example, a virtual payment card displayed by display 2704 may itself include a virtual user interface (e.g., one or more virtual buttons) that may be sensitive to touch or proximity. Such virtual buttons may be associated with a feature (e.g., one or more tracks of magnetic stripe information may be communicated by the mobile device when a button is activated) . In so doing, for example, a feature activated on a virtual payment card displayed by display 2704 may cause mobile device 2700 to behave

like a payment card (e.g., one or more tracks of magnetic stripe information may be communicated by mobile device 2700 when a virtual button of a virtual payment card of display 2704 is activated) .

[0268] FIG. 27 shows architecture 2750. User interface 2752 may, for example, be included within architecture 2750 to allow user interaction with architecture 2750. For example, a dedicated key pad or keyboard may be included within user interface 2752 to allow alphanumeric data entry into architecture 2750.

[0269] Architecture 2750 may include one or more displays 2754. Display 2754 may, for example, be touch-sensitive. Accordingly, for example, display 2754 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 2754. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of display 2754 may be detected by processor 2758 as alphanumeric data entry.

[0270] Alphanumeric entry boxes may, for example, be rendered onto display 2754. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 2752 and/or a virtual keypad rendered onto display 2754 to select alphanumeric characters to be placed within the alphanumeric entry box having a character position identified, for example, by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 2758 may receive alphanumeric characters as typed into a alphanumeric entry box of display 2754 and may use such alphanumeric characters as data input.

[0271] Display 2754 may, for example, render a virtual representation of a card (e.g., one or more virtual payment cards stored within memory 2760) . Accordingly, for example, information (e.g., payment card number, cardholder name, bank logos and issuer identification) may be stored within memory 2760 and rendered onto display 2754 as a virtual representation of a card. In so doing, for example, virtual interactive objects (e.g., buttons, displays, light sources and light sensors) that may be associated with a virtual card on display 2754 may be utilized through interaction with display 2754 just as if the virtual card were physically present.

[0272] Display 2754 may, for example, provide data output from architecture 2750. For example, display 2754 may communicate data using a series of light pulses. Accordingly, for example, processor 2758 may cause one or more portions of display 2754 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 2754 via light pulses having varying characteristics. Display 2754 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0273] Architecture 2750 may include one or more transceivers 2756. Transceiver 2756 may communicate information to and/or may receive information from one or more devices. Transceiver 2756 may, for example, communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly,

for example, transceiver 2756 may allow a mobile device (e.g., mobile device 2700 of FIG. 27) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 2700 of FIG. 27) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 2756 may exchange information with one or more other mobile devices via one or more associated cellular stations .

[0274] Transceiver 2756 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 2756 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 2756 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 2700 of FIG. 27) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network .

[0275] Architecture 2750 may include contactless communication device 2762, which may communicate via

any one or more contactless communication methodologies, such as for example, near field communications (e.g., RFID), Bluetooth, touch simulation, light pulsing (e.g., via an LED), and electromagnetic data communication (e.g., via a dynamic magnetic stripe communications device) . Accordingly, for example, contactless communication device 2762 may be compatible with any contactless device, such as for example, an RFID enabled payment card and a contactless reader (e.g., a magnetic stripe reader or an NFC reader) .

[0276] A non-powered card may, for example, communicate with contactless communications device 2762. Contactless communication device 2762 may, for example, establish a carrier field (e.g., an RF field) that may be modulated by a device (e.g., an RFID tag) of a non-powered payment card. In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by contactless communications device 2762 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 2762 by modulating the RF field produced by contactless communications device 2762.

[0277] A powered card may, for example, communicate with contactless communication device 2762. A powered card may, for example, include a processor, a battery, a memory, wireless communications devices (e.g., a dynamic magnetic stripe communications device or RFID) and other electronics (e.g., buttons, displays, light sources and light sensors) that may allow a user to interact with the powered card to perform one or more functions. Accordingly, for example, a powered card

may be used to communicate specific information to contactless communication device 2762 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 2762 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications.

[0278] Contactless communication device 2762 may receive variable data sets from a powered card based upon, for example, manual input provided to a powered card. For example, a button associated with an on-line purchase may be pressed on the powered card that causes a variable data set (e.g., account number and expiration date) to be communicated from the powered card to contactless communication device 2762.

[0279] Discretionary data may, for example, be communicated by a powered card based upon which button was pressed on the powered card. In so doing, for example, a security code (e.g., "111") may be communicated within a discretionary data field when a button associated with a particular feature (e.g., pay with credit) is pressed on the powered card. As per another example, a different security code (e.g., "222") may be communicated within a discretionary data field when a button associated with a different feature (e.g., pay with debit) is pressed on the powered card. Accordingly, for example, processor 2758 may identify what type of device may be in communication with contactless communication device 2762 by analyzing the

data communicated to contactless communication device 2762 .

[0280] Architecture 2750 may include memory 2760 and/or processor 2758 may include internal memory. Accordingly, for example, application code may be stored within memory 2760 and/or processor 2758 and executed by processor 2758 in support of functions performed by architecture 2750. For example, an application (e.g., a mobile wallet graphical user interface) may be executed by architecture 2750 and displayed onto display 2754, which may be used to interact with a user of a mobile device (e.g., mobile device 2700 of FIG. 27) . Persons skilled in the art will appreciate that executable application code may be communicated to architecture 2750 via any one or more interfaces of architecture 2750 (e.g., user interface 2752, display 2754, transceiver 2756, and/or contactless communication device 2762) .

[0281] Application data (e.g., virtual payment card data) may be stored within memory 2760 and accessed by processor 2758 during operation. For example, payment card data may be stored within memory 2760 and recalled by processor 2758 during a financial transaction being conducted by a mobile device (e.g., mobile device 2700 of FIG. 27) . Once recalled, processor 2758 may communicate the payment card data via transceiver 2756 and/or contactless communication device 2762 to complete a financial transaction.

[0282] FIG. 28 shows network topology 2800 that may include, for example, mobile wallet 2802 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player) . Mobile wallet 2802 may, for example, include a contactless interface

that may initiate, sustain, and/or terminate a communication channel between a contactless device (e.g., an RFID enabled payment card) and mobile wallet 2802. A contactless device and mobile wallet 2802 may communicate using any number of contactless mediums, which may include for example, visible, audible, capacitive, electromagnetic, magnetic, and/or RF mediums .

[0283] Mobile wallet 2802 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 2812 and/or payment network 2814) and/or one or more wireless networks (e.g., mobile network 2810) . Mobile wallet 2802 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile wallet 2802 to communicate information (e.g., voice and data) to cellular network access infrastructure 2806 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers) . Persons skilled in the art will appreciate that cellular network access infrastructure 2806 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0284] Mobile wallet 2802 may, for example, communicate with wireless access point 2808 over a wireless interface (e.g., a Bluetooth interface or a Wi-Fi interface) . Accordingly, for example, mobile wallet 2802 may access one or more wired networks (e.g., IP network 2812 and/or payment network 2814) and/or one or more wireless networks (e.g., mobile

network 2810) without the need to first gain access to cellular network access infrastructure 2806.

[0285] Any contactless device (e.g., a powered payment card or a non-powered payment card) may, for example, communicate with mobile wallet 2802 via a contactless medium. Accordingly, for example, payment information (e.g., a payment account number and a card expiration date) may be communicated from a contactless device to mobile wallet 2802. In so doing, for example, items for purchase on IP network 2812 (e.g., the internet) may be accessed by a browser of mobile wallet 2802 via an access point (e.g., wireless access point 2808 or cellular network access infrastructure 2806) . Mobile wallet 2802 may, for example, complete a purchase transaction by first obtaining required payment information from a contactless device, storing such payment information and communicating such payment information to network entities (e.g., payment server 2816 and/or issuer 2820) .

[0286] Payment server 2816 may, for example, contact issuer 2820 via a network (e.g., payment network 2814) with payment information received from mobile wallet 2802 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile wallet 2802 via any one or more delivery options (e.g., via a short messaging service of mobile network 2810 or an email delivery service of IP network 2812) . Mobile wallet 2802 may allow a user to associate purchase categories (e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile wallet so that the user may receive a more detailed accounting of his or her expenditures on his or her receipt. Accordingly,

for example, a user may enjoy a higher degree of integration such that a user may customize a level of detail provided on a receipt via mobile wallet 2802.

[0287] A payment receipt may, for example, be provided to mobile wallet 2802 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile wallet 2802 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0288] A mobile wallet (e.g., mobile wallet 2824) may, for example, include a contactless communication device (e.g., an RFID) that may initiate, sustain, and/or terminate contactless communication channel 228 with merchant terminal 2818. Accordingly, for example, mobile wallet 2824 may communicate payment information to merchant terminal 2818 to complete a financial transaction. In so doing, for example, mobile wallet 2824 may first receive payment information via a contactless communication channel from one or more contactless devices (e.g., a non-powered card), store the received payment information within a memory of mobile wallet 2824, and forward the payment information onto merchant terminal 2818 to complete a financial transaction. Accordingly, for example, payment information may be recalled from memory within mobile wallet 2824, optionally authenticated and authorized by a user of mobile wallet 2824 and communicated to merchant terminal 2818 via contactless communication channel 2828 to complete a financial transaction using merchant terminal 2818. An electronic receipt may, for example, be generated by merchant terminal 2818 and communicated to mobile wallet 2824 via contactless communication channel 2828.

[0289] FIG. 29 shows system 2900, which may include mobile wallet 2902 and payment card 2904. Mobile wallet 2902 may, for example, be a laptop computer, a PDA, a mobile telephonic device (e.g., a smartphone), an MP3 player, a GPS, or any other mobile device. Display 2908 may be a touch-sensitive display (e.g., sensitive to a change in capacitance). Payment card 2904 may, for example, be a powered payment card or a non-powered payment card.

[0290] Mobile wallet 2902 and payment card 2904 may each include a contactless communication device (e.g., RFID) that may communicate via a contactless communication channel that may be formed between mobile wallet 2902 and payment card 2904 after coming into proximity to one another. Payment card 2904 may, for example, be tapped onto display 2908 of mobile wallet 2902 to establish a proximity relationship that forms a communication channel between payment card 2904 and mobile wallet 2902. As per another example, payment card 2904 may be brought within a proximity distance (e.g., up to two inches) of mobile wallet 2902 to establish a contactless communication channel between mobile wallet 2902 and payment card 2904.

[0291] A processor of mobile wallet 2902 may, for example, execute application code that may generate a graphical user interface (GUI) onto display 2908 of mobile wallet 2902. Message 2906 of such a GUI may invite a user of mobile wallet 2902 to begin storage of card information (e.g., payment card information) by tapping one or more cards (e.g., one or more payment cards) against display 2908. As per another example, by tapping a card (e.g., payment card 2904) against mobile wallet 2902, a processor of mobile wallet 2902

may autonomously determine that card information associated with the tapped card is to be stored within a memory of mobile wallet 2902 and a processor of mobile wallet 2902 may then generate a mobile wallet GUI onto display 2908 to autonomously download the card information and engage a user of mobile wallet 2902 to administer any other activities that may be associated with such an information download.

[0292] A processor of mobile wallet 2902 may, for example, autonomously determine a type of card that may be tapped against it. For example, a processor of mobile wallet 2902 may receive payment card data that may be indicative of a non-powered payment card (e.g., payment card data received from a non-powered card may not provide a security code associated with the card). As per another example, a processor of mobile wallet 2902 may receive data that may be indicative of a powered card (e.g., payment card data received may contain a dynamically generated security code). Payment card data received from a powered card may, for example, include a dynamic security code that may change depending upon a type of transaction being conducted (e.g., debit or credit transaction).

[0293] As per another example, payment card 2904 may be a powered payment card that may include electronics to simulate a human touch (e.g., payment card 2904 may generate a change in capacitance that may be sensed by display 2908). Through a series of simulated touches, payment card 2904 may communicate a series of data bits to display 2908, which may then be processed by a processor of mobile wallet 2902. In so doing, for example, a contactless communication channel may be established where data is transferred from payment card

2904 to mobile wallet 2902 via a series of simulated touches .

[0294] Payment card 2904 may, for example, include a light sensor. Accordingly, for example, payment card 2904 may be sensitive to light pulses generated within a region of display 2908. The light sensor of payment card 2904 may receive a series of light pulses, which may be construed by a processor of payment card 2904 as data generated by mobile wallet 2902. In so doing, for example, payment card 2904 may receive an optical data stream represented by a series of light pulses generated by display 2908. As such, a two-way communication channel may be formed, where simulated touches may generate a data stream from payment card 2904 to mobile wallet 2902 and light pulses may generate a data stream from mobile device 2902 to payment card 2904.

[0295] FIG. 30 shows GUI 3000, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3000 may, for example, provide a summary information screen that provides virtual card 3002 and associated identifying information. Virtual card 3002, for example, may be a virtual representation of a physical card that may have been tapped against a display of a mobile device to form a contactless communication channel between the physical card and a mobile device.

[0296] Card (e.g., payment card) information (e.g., track 1 and track 2 magnetic stripe data) may be communicated to the mobile device via a contactless communication channel and such information may be displayed within virtual card 3002 as summary information that may be associated with the physical

payment card. A payment card number communicated to a mobile device within a magnetic stripe message may, for example, include issuer identification as well as an issuing network identifier. Accordingly, for example, a processor of a mobile device may analyze the payment card number received from a physical payment card and may render a portion or all of the identifying information associated with the payment card number onto virtual card 3002. In so doing, for example, issuer identification 3004 as well as a logo representative of an issuing network identifier may be rendered onto virtual card 3002. Additionally, a portion or all of payment card number 3006 as well as cardholder's information (e.g., cardholder's name 3008) may be rendered onto virtual card 3002.

[0297] A portion or all of the card information received from a physical card may be stored within a memory of a mobile device. Alternately, for example, a portion or all of the card information received from a physical card may be collected by a mobile device and communicated by the mobile device to a remote server for storage and/or validation purposes. In so doing, for example, instead of storing payment card information within a memory of a mobile device, card identification 3010 may, for example, be stored within a mobile device and used as an index identifier to look up payment information that may be stored within a remote server. A processor of a mobile device may generate card identification 3010 and may display card identification 3010 within an alphanumeric entry box. In so doing, for example, a user of a mobile device may either accept, or change, card identification 3010 to a value that may later be used to remind the user of

which physical payment card is associated with card identification 3010 and to recall payment information associated with card identification 3010 that may be remotely stored.

[0298] FIG. 31 shows GUI 3100, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3100 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. GUI 3100 may, for example, challenge a user of the mobile device to enter a PIN that may be associated with a payment card (e.g., VISA credit 3102) that was previously presented to the mobile device so that payment information may be uploaded from the payment card to the mobile device via a contactless communication channel generated between the payment card and the mobile device. GUI 3100 may, for example, generate virtual pin pad 3106 that may include touch-sensitive buttons having alphanumeric indicia associated with each button. A user may touch one or more buttons of pin pad 3106 that may correspond to respective characters of a PIN and an indication of the user's selection may appear within area 3104. Characters displayed within area 3104 may, for example, be hidden for security purposes.

[0299] Activation of virtual button 3108 may, for example, cause a processor of a mobile device to compare a PIN entered by a user of the mobile device to a PIN that may be associated with the payment card presented to the mobile device for storage. The PIN may, for example, be stored within protected memory of the mobile device, so that a processor of the mobile device may locally determine the validity of the PIN

entered. Alternately, for example, the mobile device may communicate the PIN to, for example, the issuing bank for a remote validation of the PIN entered. Persons skilled in the art will appreciate that a user interface (e.g., a keypad or keyboard) of a mobile device may be used instead of virtual pin pad 3106 to enter the one or more characters of a PIN.

[0300] Upon validation that the correct PIN was entered, virtual card 3110 may be displayed. In particular, for example, account number 3112 may be fully populated within virtual card 3110 to indicate to a user of the mobile device that the PIN was correctly entered and to allow the user to compare account number 3112 against an account number printed on the physical payment card of which virtual card 3110 is a representation. Persons skilled in the art will appreciate that virtual payment cards may be stored within a mobile wallet without first requiring a user to validate the payment card using a PIN entry. An alternate form of validation (e.g., a security code) may, for example, be required for validation. As per another example, no validation may be required to store a virtual payment card onto a mobile wallet.

[0301] FIG. 32 shows system 3200, which may include mobile wallet 3202 and card 3206. Card 3206 may, for example, be a powered card (e.g., a powered payment card) . Accordingly, for example, card 3206 may include a processor, display 3212, a battery, manual input interfaces (e.g., buttons 3208 and 3210) and other electronic components (e.g., a light source, a light sensor and a touch simulator) . A user of powered card 3206 may, for example, interact with card 3206 to

select the information that may be communicated to mobile wallet 3202 from card 3206.

[0302] A user may, for example, press button 3208 and then tap card 3206 against display 3204 of mobile wallet 3202 to generate a contactless communication channel (an RFID communication channel) between card 3206 and mobile wallet 3202. Accordingly, for example, card 3206 may communicate payment information (e.g., one, two and/or three tracks of magnetic stripe data) that may be associated with a feature selected by pressing button 3208. In so doing, for example, card 3206 may communicate information (e.g., within a discretionary data field) associated with a selected feature (e.g., a VISA debit payment feature).

[0303] FIG. 33 shows GUI 3300, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3300 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. GUI 3300 may, for example, render virtual card 3310 so that a user of the mobile device may compare information 3312 and 3314 to information that the user intended to communicate to the mobile device.

[0304] Accordingly, for example, a user may have pressed a button on a powered payment card associated with a debit pay feature and may have communicated the debit pay feature (e.g., within a discretionary data field of a magnetic stripe message) to a mobile device via a contactless communication channel that may have been created between the powered payment card and the mobile device. In so doing, for example, a processor of a mobile device may analyze the debit pay feature received from the powered payment card and may render

an indication (e.g., "Pay Now" identifier 3314) onto virtual card 3310 to indicate that virtual payment card 3310 has been stored within the mobile device such that when used by a user of the mobile device to complete a payment transaction, authorizes an immediate deduction of funds from the user's payment account. Alphanumeric entry box 3316 may, for example, allow the user to tag stored virtual card 3310 with a card identifier that reminds the user of the debit functionality associated with virtual card 3310.

[0305] FIG. 34 shows GUI 3400, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3400 may, for example, render virtual card 3410 to allow a user to verify information previously communicated to a mobile device via a contactless communication channel that may be generated between a powered payment card and the mobile device. A user of a mobile device may, for example, press a button on a powered payment card that may be associated with a credit pay feature and may communicate the credit pay feature along with other payment information (e.g., payment account number 3412 and expiration date) via a contactless communication channel to the mobile device.

[0306] A processor of a mobile device may, for example, analyze information received from a powered payment card (e.g., information received via a discretionary data field) and may determine that payment information received from the powered payment card may be associated with a credit feature (e.g., "Pay Later" feature 3414) . Accordingly, for example, a processor of a mobile device may use identifier 3414 of

virtual card 3410 to signify such a credit payment feature .

[0307] Virtual card identifier 3416 may, for example, be an editable card identifier to allow a user of a mobile device to store and recall virtual card 3410 to/from a memory of a mobile device. Card identifier 3416 may, for example, be used by a mobile device to access virtual card 3410 from a remote location (e.g., a remote server) such that the mobile device need not store sensitive information that may be associated with virtual card 3410 within the mobile device .

[0308] GUI 3400 may, for example, allow an additional card to be associated with virtual card 3410. A rewards card may, for example, be associated with a credit account that may be associated with virtual card 3410. Accordingly, for example, rewards card information may be communicated to a mobile device by tapping the rewards card against portion 3418 to generate a contactless communication channel (e.g., an RFID communication channel) between the rewards card and the mobile device. As per another example, an identification card (e.g., a driver's license) may be associated with virtual card 3410. Accordingly, for example, identifying information (e.g., date of birth and a picture) associated with the holder of the identification card may be communicated to a mobile device and stored within the mobile device. In so doing, for example, stored identification information may be recalled from a memory of the mobile device to provide authentication information while completing a purchase transaction using the mobile device.

[0309] A user may, for example, select option 3420 to allow card information to be scanned into a mobile device using a scanning device (e.g., a camera) of the mobile device. Accordingly, for example, a card (e.g., a driver's license) may be scanned into a mobile device by selecting radio button 3420 and holding the driver's license in front of the mobile device while a snapshot of the driver's license is taken by a camera of the mobile device and stored in a memory location of the mobile device. A mobile device may alternately, for example, access identifying information (e.g., name, address, phone number, and picture) from a database (e.g., a motor vehicle database) that may be accessible from a network. Such information may be rendered onto a virtual identification card (e.g., a driver's license) that may be stored within a mobile device. In so doing, for example, user identification data may be recalled from a memory of a mobile device and rendered onto a display of the mobile device, so that a merchant may verify the validity of the user identification data when virtual card 3410 is used to complete a purchase transaction in the presence of the merchant.

[0310] Card information may be communicated via programming portion 3422. A powered card may, for example, provide touch simulation electronics and a light sensor such that when the powered card is placed against portion 3422, a two-way contactless communication channel may be created. Accordingly, for example, information may be communicated from the powered card to the mobile device through a series of touch simulations generated by the powered card and sensed by a portion within portion 3422 that is touch sensitive. In so doing, for example, a processor of a

mobile device may construe a series of touch simulations as a series of data bits communicated by a powered card that may be indicative of information associated with the powered card. GUI 3400 may, for example, provide a series of light pulses within portion 3422 that may be received by a light sensor of the powered card and construed by a processor of the powered card as data communicated by the mobile device.

[0311] FIG. 35 shows GUI 3500 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3500 may, for example, include upload area 3502 as generated by a processor of a mobile device. Upload area 3502 may, for example, include one or more data exchange areas (e.g., data exchange areas 3504 and 3506). Icon 3504 may, for example, be generated by GUI 3500 within an area of a display of a mobile device that may be sensitive to touch (e.g., an area that may be sensitive to a capacitance change) . Area 3506 may, for example, be generated by GUI 3500 within an area of a display of a mobile device that may generate pulses of light.

[0312] Information associated with a powered payment card may be uploaded for use by a mobile device by exchanging data with the powered payment card via data exchange areas 3504 and 3506. For example, a powered payment card may be pressed against upload area 3502 so that a touch simulation device of the powered payment card aligns with data exchange area 3504 and a light sensing device of the powered payment card aligns with data exchange area 3506. Accordingly, for example, the powered payment card may communicate information to a processor of a mobile device by simulating a series of touches in data exchange area 3504 and data may be

communicated to the powered payment card by a processor of the mobile device by generating a series of light pulses in data exchange area 3506. In so doing, for example, a mobile device and a powered payment card may exchange information so that payment card information may be stored within the mobile device.

[0313] Once payment card information is uploaded into a mobile device, GUI 3500 of the mobile device may display a summary of the uploaded information in validation area 3510. Accordingly, for example, one, two or three tracks of magnetic stripe information may be uploaded from a payment card into a mobile device via data exchange area 3504 of upload area 3502. A portion or all of the uploaded data may, for example, be rendered within validation area 3510, so that a user of the mobile device may validate that the correct payment card information was uploaded and stored within the mobile device.

[0314] FIG. 36 shows GUI 3600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3600 may, for example, render virtual card 3610 and may display a portion of information that may be associated with virtual card 3610. Accordingly, for example, a payment card (e.g., a gift card) may be brought within a proximity or touch relationship with a mobile device such that a contactless communication channel may be generated between the payment card and the mobile device. In so doing, for example, payment account information may be communicated from the payment card to the mobile device and a portion or all of the payment card information may be rendered onto virtual card 3610.

[0315] A user of a mobile device may, for example, customize a visual appearance of virtual card 3610 by utilizing any number of graphical user interface objects (e.g., list 3604 and alphanumeric input box 3612) that may be rendered by GUI 3600. A user may, for example, drag-and-drop logos from list 3604 onto virtual card 3610 to more clearly identify virtual card 3610. Accordingly, for example, a user may identify virtual card 3610 as a gift card (e.g., a Walmart gift card), using drag-and-drop operation 3608, having a particular network brand (e.g., a VISA network brand), using drag-and-drop operation 3606. A user may, for example, annotate virtual card 3610 using alphanumeric input box 3612 with any identifying information that may be useful to the user (e.g., information that may be used to recall virtual card 3610 from a memory of a mobile device) .

[0316] A mobile device may, for example, disallow certain customizations that may conflict with virtual card 3610. Accordingly, for example, a mobile device may prevent a user from applying a different network logo than was previously communicated by a physical card to the mobile device. In so doing, for example, a mobile device may prevent a user from customizing virtual card 3610 as, for example, a M/C network brand, when a payment card number previously communicated from a payment card to a mobile device indicated that the payment card was, for example, a payment card having a VISA network brand.

[0317] A credit balance, for example, may be communicated by a gift card to a mobile device via a contactless communication channel generated between the gift card and the mobile device and may be displayed as

account balance 3614 to represent an amount of credit that may be remaining on virtual card 3614 . Virtual card 3610 may, for example, be used by a mobile device to complete a purchase transaction in which payment card information associated with virtual card 3610 may be communicated to a merchant terminal (e.g., communicated via an RFID communication channel) and an amount of the purchase may be communicated from the merchant terminal to the mobile device. Accordingly, for example, account balance 3614 may be updated (e.g., reduced) by the amount of the purchase and displayed so that a user of the mobile device may be updated as to an amount of credit remaining on virtual card 3610.

[0318] A user of a mobile device may, for example, purchase additional credit to be added to virtual card 3610. Accordingly, for example, account balance 3614 may be updated (e.g., increased) when an amount of credit is added to virtual card 3610. In so doing, for example, an amount of credit added to virtual card 3610 may be communicated (e.g., communicated via an RFID communication channel) to a mobile device by a merchant terminal and updated via account balance 3614 so that a user of the mobile device may receive up-to-date information relating to a credit balance that may be available on virtual card 3610. As per an example, a user may recall a virtual payment card from a memory of a mobile device, activate the payment card for use, and use the mobile device to purchase additional credit on virtual card 3610 using the activated payment card as the payment vehicle.

[0319] FIG. 37 shows GUI 3700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3700 may, for

example, provide a visual representation of all virtual cards that may be stored within a memory of a mobile device (or within a remote server) and may display each virtual card within one or more categories that may be associated with each virtual card. A processor of a mobile device may, for example, analyze information received from a physical card via a contactless communication channel (e.g., an RFID, electromagnetic, visible, audible, capacitive, or magnetic communication channel) to determine a card category that may be associated with the corresponding virtual card.

[0320] An account number may, for example, be communicated by a card to a processor of a mobile device that may identify the card as a particular card type (e.g., bank card, rewards card, identification card, healthcare card, travel card or airline card) . Accordingly, for example, each virtual card stored within a memory of a mobile device may be assigned a category index by a processor of the mobile device and may then be rendered onto GUI 3700 in accordance with the category index assigned. As per another example, a user of a mobile device may assign a category index (e.g., card identification) to a virtual card after information associated with a corresponding physical card is communicated to the mobile device via a contactless communication channel.

[0321] One or more payment cards, for example, may be rendered onto GUI 3700 and each payment card may be aligned within category 3706. An ordering of each payment card in category 3706 may, for example, be established by a user of a mobile device via sort options 3702. A mobile device may, for example, maintain statistics (e.g., number of times each virtual

payment card is recalled from a memory of a mobile device and used to complete a purchase transaction via the mobile device). Accordingly, for example, upon selection of one of sort options 3702 (e.g., Most used), a processor of a mobile device may recall usage statistics that may be associated with each virtual payment card stored within a memory of a mobile device and may display each virtual payment card within category 3706 onto GUI 3700 in accordance with such usage statistics (e.g., the top virtual payment card displayed within category 3706 may have the most usages of all virtual payment cards stored within a memory of the mobile device).

[0322] A mobile device may, for example, maintain other information associated with virtual payment cards of category 3706. Accordingly, for example, a mobile device may access network devices (e.g., issuer servers) associated with each virtual payment card stored within the mobile device. In so doing, for example, a mobile device may collect information (e.g., credit limit and credit available) associated with each virtual payment card stored within a memory of the mobile device and may display each virtual payment card on GUI 3700 in accordance with sort options 3702 (e.g., the top card displayed within category 3706 may have the highest credit limit or may have the most credit available).

[0323] Category 3708 may, for example, be associated with all virtual gift cards that may be stored within a memory of a mobile device (or remote server). Information associated with each virtual gift card may, for example, include a merchant identifier, a merchant type identifier, and an amount of credit available.

Accordingly, for example, a user may select one of sort options 3704 (e.g., Most credit available) to display a list of virtual gift cards within category 3708 in a descending order, where the top virtual gift card of category 3708 may have the highest credit available.

[0324] A mobile device may, for example, be a locating device (e.g., a GPS) or may, for example, include location determination electronics . Accordingly, for example, a mobile device may determine its own location and may determine whether its location corresponds with a location of a merchant's place of business that may be associated with a virtual gift card of category 3708. In so doing, for example, a mobile device may determine that its location is within a Walmart store and if, for example, sort options 3704 is selected to "Location", then a processor of the mobile device may re-order the virtual gift cards of category 3706 such that a Walmart virtual gift card is displayed as the top card in the stack. Accordingly, for example, the Walmart virtual gift card may be conveniently located within GUI 3700 for selection by a user of a mobile device to use during a purchase transaction conducted between a contactless communication channel formed between the mobile device and a merchant terminal at the Walmart store.

[0325] Virtual cards may, for example, be autonomously sorted across categories depending upon a virtual card placement that may exist in a particular category. A virtual payment card may, for example, be selected to occupy a top card placement within category 3706. A virtual rewards card may, for example, be associated with the virtual payment card selected for top placement in category 3706. Accordingly, for

example, the associated virtual rewards card may be selected for top placement within category 3708 based upon its association with the virtual payment card selected for top placement within category 3706. As per another example, a virtual identification card (e.g., a virtual driver's license card) may be selected for top placement within category 3710 based upon its general association with any virtual payment card selected for top placement within category 3706 or its general association with any virtual gift card selected for top placement within category 3708.

[0326] FIG. 38 shows GUI 3800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3800 may, for example, provide a visual representation of all virtual cards that may be stored within a mobile device (or remote server) and may display each virtual card within one or more categories that may be associated with each virtual card. GUI 3800 may, for example, be rendered onto a touch-sensitive display of a mobile device, such that by touching a location of the display that corresponds to a location of a virtual card, that card may be selected for use. Accordingly, for example, a user may touch any area within virtual card 3804 to activate virtual card 3804 for use. In so doing, for example, indicia may be provided on GUI 3800 to indicate that virtual card 3804 has been selected for use (e.g., an outline of virtual card 3804 may be highlighted) and a copy of virtual card 3804 (e.g., virtual card 3802) may be rendered onto GUI 3800 to indicate to a user of the mobile device that virtual card 3802 has been selected for use.

[0327] FIG. 39 shows GUI 3900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3900 may, for example, allow a user of a mobile device to select (e.g., touch) one of the virtual cards rendered onto GUI 3900. Once selected, the virtual card may rise from its position (e.g., virtual card 3904 may be elevated above the neighboring virtual cards in category 3902) and may be highlighted to indicate the selection to a user. Once elevated, the selected virtual card (e.g., card 3904) may display relevant information associated with the virtual card (e.g., information displayed on a front surface of the virtual card such as account number and merchant affiliation) so that a user may verify that the selected virtual card is the virtual card that the user wishes to use. If the selected virtual card is not the virtual card that the user wishes to use, then the user may deselect (e.g., touch) the selected virtual card and the virtual card may fall back within the ranks of its neighboring virtual cards. If the selected virtual card is the virtual card that a user wishes to use, then the user may confirm (e.g., touch the selected virtual card twice) that the selected card is the desired virtual card for use.

[0328] FIG. 40 shows GUI 4000 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4000 may, for example, allow a user of a mobile device to use selected virtual card 4002 in some manner. A user may, for example, wish to complete a purchase transaction using the mobile device and selected virtual card 4004. Accordingly, for example, upon selection of option

4004, information associated with selected virtual card 4002 may be communicated from a mobile device to, for example, a merchant terminal to complete a purchase transaction. In so doing, for example, a contactless communication channel (e.g., an RFID communication channel) may be formed between the mobile device and the merchant terminal and payment information (e.g., payment account number and expiration date) may be communicated from the mobile device to the merchant terminal via the contactless communication channel. As per another example, other information (e.g., one, two, or three tracks of magnetic stripe information) that may be associated with virtual card 4002 may be communicated by the mobile device to the merchant terminal when the mobile device detects the presence of an RFID communication channel formed between the mobile device and the merchant terminal.

[0329] A mobile device may, for example, request electronic receipts to be delivered to the mobile device after purchase transactions are completed. Accordingly, for example, receipts may be delivered to the mobile device via an electronic delivery method (e.g., text messaging or email) and may be stored within a memory of the mobile device for future use. In so doing, for example, a user may select option 4006 to view a list of one or more receipts that may be associated with purchases conducted via the mobile device and virtual card 4002.

[0330] A mobile device may, for example, request electronic bank statements to be delivered to the mobile device at the end of each billing cycle of virtual card 4002. Alternately, for example, a mobile device may access a network entity (e.g., an issuer's

server) to retrieve bank statement information that may be associated with virtual card 4002. Accordingly, for example, a user of a mobile device may review any and all bank statements associated with virtual card 4002 that a user's mobile device may have collected via its network access capabilities (e.g., a wireless access point or cellular network access infrastructure).

[0331] A mobile device may, for example, allow virtual card 4002 to be associated with one or more virtual cards stored within a memory of the mobile device (or remote server). For example, virtual card 4002 may be associated with one or more cards (e.g., a rewards card and a driver's license) and a user of a mobile device may view such associations using a GUI of the mobile device.

[0332] A mobile device may, for example, allow virtual card 4002 to be associated with one or more virtual cards that may be stored within a memory of another mobile device and/or may allow virtual card 4002 to be associated with one or more physical cards not stored within any mobile device. Virtual card 4002 may, for example, be one of many (e.g., two) cards issued against the same general account (e.g., a husband and wife joint charge account). Accordingly, for example, a mobile device may recognize that virtual card 4002 is one of a pair of cards associated with such a joint account and may provide information to the user of the mobile device about such associations.

[0333] FIG. 41 shows system 4100, which may include a mobile device (e.g., mobile wallet 4102), merchant terminal 4106 and GUI 4108 that may be executed by a processor of mobile wallet 4102. A user of mobile wallet 4102 may recall a virtual card (e.g., a virtual

payment card) from a memory of mobile wallet 4102 (or from a remote server) and use mobile wallet 4102 to communicate payment information associated with the virtual payment card to a merchant terminal. Accordingly, for example, a user of mobile wallet 4102 may have selected a virtual payment account from within a memory of mobile wallet 4102 (or remote server) to complete a payment transaction.

[0334] Once mobile wallet 4102 is brought within a communication distance (e.g., within approximately 2 inches) of merchant terminal 4106, a contactless communication channel (e.g., RFID communication channel 4104) may be generated between mobile wallet 4102 and merchant terminal 4106. Payment information associated with a virtual payment card selected by a user of mobile wallet 4102 may, for example, be autonomously communicated by a processor of mobile wallet 4102 to merchant terminal 4106 via contactless communication channel 4104 once a presence of merchant terminal 4106 is detected by the processor of mobile wallet 4102.

[0335] Contactless communication channel 4104 may, for example, be a two-way communication channel. Accordingly, for example, merchant terminal 4106 may communicate information to mobile wallet 4102 via contactless communication channel 4104. In so doing, for example, merchant terminal 4106 may communicate a total sale amount to mobile wallet 4102 and may wait for a user of mobile wallet 4102 to acknowledge that the total sale amount is correct (e.g., a user of mobile wallet 4102 may press an acknowledgment key that causes mobile wallet 4102 to communicate a confirmation message to merchant terminal via contactless communication channel 4104). Further communication

from merchant terminal 4106 may query mobile wallet 4102 as to whether a user of mobile wallet 4102 requires cash back.

[0336] Once a purchase transaction is completed, a user of mobile wallet 4102 may request a receipt to be delivered to mobile wallet 4102 via any one of a number of mediums. A user may, for example, request that a receipt be delivered to mobile wallet 4102 at a later time (e.g., receipt queued for delivery at a later time via text messaging or email) . A user may, for example, request that a receipt be delivered to mobile wallet 4102 immediately. Accordingly, for example, an electronic receipt may be generated by merchant terminal 4106 and communicated to mobile wallet 4102 via contactless communication channel 4104.

[0337] An application executing on a mobile device (e.g., a receipt handler application associated with GUI 4108) may have its own address. Accordingly, for example, the receipt handler's address may be well known within a network (e.g., a payment network), such that a server (e.g., an email server associated with a merchant's payment server) may email an electronic receipt directly to the receipt handler application that may be running on the mobile device. In so doing, for example, one or more applications running on a mobile device may have well known addresses (e.g., email addresses and multimedia message addresses) associated with them, so that the applications may directly communicate with network entities to autonomously provide a user of the mobile device with up-to-date and valuable information.

[0338] FIG. 42 shows system 4200, which may include a mobile device (e.g., mobile wallet 4202), merchant

terminal 4212 and GUI 4204 that may be executed by a processor of mobile wallet 4202. Mobile wallet 4202 may, for example, complete a purchase transaction with merchant terminal 4212 by exchanging payment information with merchant terminal 4212 via a contactless communication channel (e.g., RFID communication channel 4214) . Merchant terminal 4212 may, for example, communicate electronic receipt 4206 to mobile wallet 4202 after a purchase transaction completes. Electronic receipt 4206 may, for example, be displayed by a processor of mobile wallet 4202 onto GUI 4204 so that a user of mobile wallet 4202 may view electronic receipt 4206 and may execute certain options that may be associated with electronic receipt 4206.

[0339] Mobile wallet 4202 may, for example, allow a user of mobile wallet 4202 to annotate electronic receipt 4206 with a note that may be entered into alphanumeric entry box 4208. Mobile wallet 4202 may, for example, allow electronic receipt 4206 to be associated with a virtual card (e.g., virtual payment card VISA 3456 that was used to complete the purchase transaction) stored within a memory of mobile wallet 1602 .

[0340] FIG. 43 shows GUI 4300 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4300 may, for example, allow a user of a mobile device to view receipts that may be associated with a selected virtual card. Accordingly, for example, a user of a mobile device may select a virtual card (e.g., virtual payment card 4302) and may view a summary of receipts that may be associated with virtual payment card 4302. In so doing, for example, a user may select summary receipt

4304 (e.g., by touching portion 4304 on GUI 4300) and a processor of the mobile device may retrieve details of summary receipt 4304 from a memory of the mobile device and display them in receipt detail area 4306.

[0341] FIG. 44 shows GUI 4400 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4400 may, for example, allow a user of a mobile device to view virtual cards stored within a memory of the mobile device (or remote server) that may be associated with a selected virtual card. Accordingly, for example, selected virtual card 4402 may have an association with virtual rewards card 4404 and selected virtual card 4402 may have an association with virtual identification card 4406.

[0342] A mobile device may, for example, access a user's rewards account by accessing a network entity (e.g., an issuer's server) to determine information associated with the rewards account (e.g., number of rewards points earned) . A mobile device may, for example, access the network entity on a regularly scheduled basis and store the retrieved rewards account information within a memory location of the mobile device. A mobile device may, for example, access the network entity only upon demand to retrieve rewards account information and may only display the retrieved rewards account information without storing the retrieved rewards account information.

[0343] GUI 4400 may, for example, allow a user to obtain further information that may be associated with virtual cards 4404 and/or 4406. A user may, for example, touch a display of a mobile device in the vicinity of virtual card 4404 to obtain other

information (e.g., a rewards point balance) associated with virtual card 4404. Accordingly, for example, a user may obtain a rewards points total that may be associated with virtual card 4404 and may touch virtual card 4404 again to conduct a purchase transaction with rewards points that may be associated with virtual card 4404. In so doing, for example, a mobile device may, for example, establish a contactless communication channel (e.g., an RFID communication channel) with a merchant terminal and may communicate points information that may be associated with virtual card 4404 so that a purchase transaction may be completed using rewards points that may be associated with virtual card 4404.

[0344] GUI 4400 may, for example, provide other information to a user concerning virtual card 4406. For example, a processor of a mobile device may detect that an expiration date of virtual card 4406 is approaching. Accordingly, for example, a user may touch a display in the vicinity of virtual card 4406 to automatically renew the driver's license using the mobile device. In so doing, for example, a mobile device may contact a network entity (e.g., a driver's license renewal server) to order a renewal driver's license. The renewal driver's license may, for example, be delivered to the user as a physical card, in which case the user may upload information associated with the physical driver's license into the mobile device via a contactless communication channel formed between the physical driver's license and the mobile device. Alternately, for example, a mobile device may receive an electronic copy of a virtual driver's license and replace information associated

with virtual card 4406 with the updated information received from a driver's license renewal server.

[0345] FIG. 45 shows system 4500, which may include mobile wallet 4502 and a powered card (e.g., powered payment card 4506) . Powered card 4506 may, for example, include a contactless communication device (e.g., an RFID) that may communicate with a contactless communication device (e.g., an RFID) of mobile wallet 4502. A GUI executed by a processor of mobile wallet 4502 may invite a user of powered card 4506 to tap powered card 4506 against display 4504 of mobile wallet 4502. Such contact with, or proximity to, mobile wallet 4502 may generate a contactless communication channel within which information may be exchanged between powered card 4506 and mobile wallet 4502.

[0346] As per another example, powered card 4506 may include circuitry that may simulate a touch. Display 4504 may be touch-sensitive. Accordingly, for example, powered card 4506 may communicate data to mobile wallet 4502 by simulating a series of touches that may be sensed by display 4504 and processed by a processor of mobile wallet 4502 as data received from powered card 4506. Powered card 4506 may include light sensor 4510. Accordingly, for example, a processor of mobile wallet 4502 may generate a series of light pulses on a portion of display 4504 that may be detected by light sensor 4510 of powered card 4506 and processed by a processor of powered card 4506 as data communicated by mobile wallet 4502. In so doing, for example, data may be communicated by powered card 4506 via a series of simulated touches and data may be communicated by mobile wallet 4502 via a series of light pulses.

[0347] Information communicated by powered card 4506 to mobile wallet 4502 may, for example, include payment information (e.g., payment account number, expiration date, and cardholder name) . Information communicated by powered card 4506 to mobile wallet 4502 may, for example, include other information relating to a configuration of powered card 4506 including, for example, whether or not a display exists and if so, at what location; whether or not a manual input interface (e.g., one or more buttons) exists and if so, at what location; and whether or not a light sensor exists and if so, at what location. Accordingly, for example, configuration information relating to powered card 4506 may be communicated to mobile wallet 4502, so that when a virtual card relating to powered card 4506 is generated and stored within mobile wallet 4502, the virtual card may employ all of the features that may be employed by its physical counterpart.

[0348] Information communicated by powered card 4506 may, for example, be encrypted. Decryption may, for example, be executed within mobile wallet 4502 so that information communicated by powered card 4506 may be stored within a memory of mobile wallet 4502 in a decrypted format. Alternately, for example, information communicated by powered card 4506 may be stored within a memory of mobile wallet 4502 in an encrypted format. Mobile wallet 4502 may, for example, authenticate itself to a network entity (e.g., an issuer server) such that each time encrypted information is recalled from a memory of mobile wallet 4502, a decryption key may be communicated by the network entity to mobile wallet 4502 for decryption purposes .

[0349] FIG. 46 shows GUI 4600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4600 may, for example, display virtual card 4602 that may employ all of the features of its physical counterpart. Accordingly, for example, manual input interfaces (e.g., virtual buttons 4606 through 4614) may have the same functionality on virtual card 4602 as they do on the physical counterpart to virtual card 4602. In so doing, for example, virtual buttons 4606 through 4614 may be displayed on portions of GUI 4600 that may be touch-sensitive, such that when virtual buttons 4606 through 4614 are touched, a processor of the mobile device may impart a functionality to the mobile device just as if the mobile device itself was the physical card (e.g., a PIN may be entered into virtual card 4602 via one or more buttons 4606-4614 to unlock virtual dynamic portion 4618 of virtual payment card number 4616).

[0350] A mobile device may, for example, provide a light-sensitive display, such that when virtual card 4602 is rendered onto the light-sensitive display, light sensor 4604 may exhibit the same functionality as its physical counterpart. Accordingly, for example, virtual card 4602 may be rendered so that light sensor 4604 exists on a light-sensitive portion of a display of a mobile device. A processor of the mobile device may, for example, detect light pulses sensed at light sensor 4604 as data communicated to virtual card 4602. In so doing, for example, virtual card 4602 may receive information that changes the functionality of virtual card 4602 (e.g., an expiration date of virtual payment card 4602 may be updated via light sensor 4604).

[0351] A mobile device may, for example, provide a display that may simulate touch. Accordingly, for example, virtual card 4602 may be rendered onto a display of a mobile device so that touch-simulating portion 4620 aligns with a portion of the display that may be capable of simulating touch. In so doing, for example, virtual card 4602 may communicate information to another device (e.g., another mobile device) when touch-simulating portion 4620 of GUI 4600 is pressed against another device (e.g., a touch-sensitive display of another mobile device) and simulates a series of touches that may be construed by a processor of the other device as data communicated to the other device.

[0352] Virtual display 4618 may, for example, display a dynamic portion of payment card number 4616 just as it would be displayed on the physical counterpart to virtual card 4602. For example, virtual card 4602 may be disabled for use when virtual display 4618 does not display a valid portion of virtual card number 4616. Upon entry of a password (e.g., a PIN may be entered by touching one or more buttons 4606-4614 that corresponds to the PIN), virtual card 4602 may be activated for use. Accordingly, for example, once a valid PIN is entered, virtual display 4618 may be populated with a remaining portion of virtual payment card number 4616 thereby activating virtual card 4602 for use. In so doing, for example, a mobile device that displays activated virtual card 4602 via GUI 4600 may communicate payment information (e.g., virtual payment card number 4616 and expiration date) to a device (e.g., a merchant terminal) via a contactless communication channel (e.g., an RFID communication channel) so that a purchase transaction may be

completed between the mobile device and the merchant terminal .

[0353] FIG. 47 shows GUI 4700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4700 may, for example, display virtual card 4702 that may employ all of the features of its physical counterpart. For example, a powered card (e.g., a powered payment card) may establish a contactless communication channel (e.g., an RFID communication channel) with a mobile device and communicate configuration and payment information that may be associated with the powered card. Accordingly, for example, a powered card may provide a manual interface (e.g., buttons) to allow a user to select a method of payment (e.g., credit, debit, or points) at the point of sale and may communicate such methods of payment to a mobile device. In so doing, for example, a mobile device may render virtual payment card 4702 having a virtual manual interface (e.g., virtual buttons 4704 through 4708), which a user may select (e.g., touch) in order to select a method of payment to be used by the mobile device when the mobile device communicates payment information to complete a purchase transaction.

[0354] A mobile device may, for example, establish a contactless communication channel (e.g., an RFID communication channel) with a merchant terminal to communicate payment information to the merchant terminal to complete a purchase transaction. Accordingly, for example, a user may touch one of virtual buttons 4704-4708 just prior to placing the mobile device within a proximity to the merchant terminal. In so doing, for example, the mobile device

may communicate one, two, and/or three tracks of magnetic stripe data to the merchant terminal and may include additional information (e.g., within a discretionary data field) to communicate a method of payment (e.g., credit, debit, or points) to the merchant terminal. Persons skilled in the art will appreciate that payment information may be communicated by a mobile device to a network entity (e.g., a payment server) via a wireless interface (e.g., a cellular interface) such that a method of payment (e.g., credit, debit, or points) may be communicated by the mobile device to the payment server to complete a remote purchase transaction.

[0355] FIG. 48 shows GUI 4800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4800 may, for example, allow a user of a mobile device to break a payment up into multiple payment methods for a single purchase. For example, a user of a mobile device may have provided a mobile device within a proximity to a merchant terminal, such that the mobile device may have communicated a method of payment (e.g., credit) to the merchant terminal based upon a user selection made via a GUI displayed by the mobile device. A processor of the mobile device may, for example, recognize that a virtual card selected by the user for payment may offer additional payment methods (e.g., debit and points). Accordingly, for example, GUI 4800 may be rendered by a processor of the mobile device to allow the user of the mobile device the option to spread the payment across several accounts by entering amounts into alphanumeric entry boxes 4804-4808. In so doing, for example, a user may spread a purchase across multiple payment

methods by entering an amount desired to be charged to each payment method (e.g., $5 credit, $5 debit, and 1500 points for a $25 total purchase). The mobile device may, for example, settle the transaction as three separate financial transactions by communicating payment information to one or more network entities (e.g., a payment server) that corresponds to each of the three financial transactions.

[0356] FIG. 49 shows GUI 4900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4900 may, for example, communicate a credit offer to a user of a mobile device that may have been communicated to the mobile device via any one of a number of electronic means (e.g., text messaging, email, or internet browser pop-up). A credit offer may, for example, be extended to a user of a mobile device to add a payment card to the user's mobile device. A credit offer (e.g., credit offer 4906) may, for example, be extended to a user of a mobile device to replace a virtual card (e.g., virtual payment card 4904) that already exists within the user's mobile device. Accordingly, for example, network entities may examine virtual cards and related information that may be stored within a memory of a mobile device and attempt to sway the user of the mobile device to opt into another virtual card offer that may be better for the user (e.g., the new virtual card may offer a lower interest rate than a user's current virtual payment card).

[0357] GUI 4900 may, for example, provide credit offer options 4908 to a user of a mobile device. Accordingly, for example, a user may elect to accept a new credit offer and cancel a current virtual payment

card with the same option. In so doing, for example, a mobile device may communicate with a network entity (e.g., an issuer of virtual payment card 4904) to cancel virtual payment card 4904 and may communicate with a network entity (e.g., an issuer for payment card offer 4906) to open the new payment account being offered .

[0358] Other options may be provided by GUI 4900. For example, a user may opt to accept the new credit offer, but keep virtual payment card 4904 as well. As per another example, a user may opt to accept the new credit offer, keep virtual payment card 4904, and transfer any balance that may be owing on virtual payment card 4904 to the new payment account now being offered.

[0359] FIG. 50 shows mobile application 5000 that may be executed by a processor of a mobile device and provided onto a display of the mobile device. Application 5000 may, for example, be any executable application that may reside within a memory of a mobile device. For example, application 5000 may be an internet browsing application that may allow a user of a mobile device to browse online for goods and/or services and may allow the user to purchase such goods and/or services from application 5000. As per another example, mobile application 5000 may be a gaming activity that may require a purchase transaction to continue on to a next level of play or to obtain gaming features for purchase.

[0360] Application 5000 may, for example, provide access to mobile wallet 5002 which may be another application running on a mobile device. Accordingly, for example, when application 5000 requires payment for

a particular function performed by application 5000 (e.g., a user wishes to purchase goods from an Amazon website), application 5000 may launch mobile wallet 5002 to allow a user to select a method of payment from mobile wallet 5002. A user may browse through each virtual card of mobile wallet 5002 by touching a virtual card to display the virtual card. Once a user has verified that a particular virtual card is the virtual card to be used to complete a purchase transaction, the user may touch the virtual card twice again to authorize a mobile device to complete a purchase transaction using payment information associated with the selected virtual card.

[0361] As per another example, a user may preselect payment options, such that mobile application 5000 need not launch mobile wallet 5002 to obtain a payment authorization. Instead, for example, a user may pre-authorize one virtual payment card within mobile wallet 5002 to be used by any other application running on a mobile device for purchase transactions. In so doing, for example, a user may pre-authorize payment information to be autonomously retrieved from mobile wallet 5002 without involving user interaction to authorize application 5000 for the purchase transaction.

[0362] FIG. 51 shows flow charts for process sequences 5110-5150. Process sequence 5110 may, for example, execute a mobile wallet application on a mobile device (e.g., as in step 5111) to request a user of the mobile device to present a card to the mobile device. In step 5112, a user may present a card to a mobile device (e.g., tap a card onto a display of a mobile device). In step 5113, a contactless

communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a card and a mobile device to communicate card information from the payment card to the mobile device. In step 5114, information may be stored within the mobile device or remote server (e.g., virtual cards may be generated, stored, and displayed by a GUI of the mobile device) for future use.

[0363] Process sequence 5120 may, for example, autonomously detect that a card is in a touching or a proximity relationship to a mobile device (e.g., as in step 5121) . In step 5122, a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a card and a mobile device to communicate information from the card to the mobile device. In step 5123, information associated with each physical card presented to the mobile device may be stored within the mobile device for future use.

[0364] Step 5131 of sequence 5130 may include presenting a card to a mobile device. A card may, for example, be a powered card or a non-powered card. In steps 5132 and 5133, a contactless communication channel may be established between a card and a mobile device and information may be exchanged between the card and the mobile device.

[0365] A card may, for example, include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. A card may, for example, include circuitry to simulate touch (e.g.,

a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device.

[0366] A card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a card as data communicated by a mobile device.

[0367] A card may, for example, include a light source (e.g., an LED) to form a contactless communication channel. Accordingly, for example, a card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the card. A card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the card through a contactless communication channel. A mobile device may, for example, include sound emission capabilities that may be detected by a microphone of a card as data communicated by the mobile device through a contactless communication channel.

[0368] Step 5141 of sequence 5140 may include arranging information contained within a memory of a mobile device and/or a remote server and rendering the information on a display of a mobile device. The rendered information may, for example, be virtual cards that are representative of physical card counterparts previously presented to the mobile device for upload.

[0369] The virtual cards may, for example, be arranged according to category (e.g., payment cards, gift cards and identification cards) . Within each category, virtual cards may be sorted according to any sort preference. For example, payment cards may be sorted in an order of most frequently used to least frequently used, in order of most available credit to least available credit, or in order of highest credit limit to lowest credit limit. Other cards (e.g., merchant gift cards) may be sorted in accordance with a user's location. For example, a mobile device may determine a location of its user and may sort virtual cards in response to the determined location (e.g., a virtual Walmart gift card may be displayed at the top of a gift card list based upon a user's location within a Walmart store) .

[0370] Virtual cards displayed by a GUI of a mobile device may, for example, be selected for use (e.g., as in step 5142) . A user may, for example, touch a virtual card among several virtual cards displayed by a mobile device to view information related to the touched virtual card. If desired for use, the touched virtual card may be touched twice again and activated for use (e.g., as in step 5143) . An activated virtual card may, for example, be used to complete a purchase transaction via the mobile device. An activated

virtual card may, for example, be deleted from a memory of the mobile device. Documents associated with an activated virtual card, such as purchase transaction receipts and bank statements, may be viewed from a display of a mobile device. Virtual cards that may be associated with an activated virtual card may be viewed from a display of a mobile device and activated themselves to perform other functions (e.g., an activated virtual payment card may be associated with a virtual rewards card, where the virtual rewards card may be activated to obtain and view the total number of rewards points that may be associated with the virtual rewards card) .

[0371] Step 5151 of sequence 5150 may include running an application on a mobile device. Such an application may be any executable application that may require purchase transactions to be completed while the application executes. As per one example, a user booking airline tickets using his or her mobile device may select their itinerary and may book their itinerary through a purchase transaction conducted by the mobile device. Accordingly, for example, the mobile application may request access to a mobile wallet application also running on the mobile device (e.g., as in step 5152), a user may grant access to the mobile wallet application (e.g., as in step 5153) by selecting a virtual payment card from within the mobile wallet and may authorize a purchase transaction to be conducted by the mobile application using the authorized virtual payment card. As per another example, a mobile application may autonomously request access to a mobile wallet application (e.g., as in step 5152) that has been pre-authorized by a user of the

mobile device (e.g., as in step 5153) such that the mobile application may autonomously conduct the purchase transaction without any further involvement with the user.

[0372] FIG. 52 shows mobile device 5200. Mobile device 5200 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, mobile device 5200 may be operated in a mobile environment while a user of mobile device 5200 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 5200 may perform multiple functions simultaneously (e.g., a person may carry on a conversation while at the same time browsing and authorizing purchases on the internet).

[0373] Mobile device 5200 may include audio processing devices (e.g., microphone 5208 and speaker 5210). Accordingly, for example, mobile device 5200 may receive voice commands from a user via microphone 5208 and may process such commands to perform a function. For example, a user may place mobile device 5200 into a desired operational mode by speaking a command into microphone 5208 that is associated with the desired operational mode. In so doing, for example, mobile device 5200 may engage in hands-free operation by receiving voice commands via microphone 5208 and performing functions associated with the received voice commands.

[0374] Mobile device 5200 may receive data input via microphone 5208. For example, a voice-band modem may generate signals in a voice-band frequency range that

may be received by microphone 5208. A processor of mobile device 5200 may interpret the received audible information as data signals and may process the data signals as, for example, data values and/or control data input .

[0375] Mobile device 5200 may include camera 5202. Camera 5202 may capture one or more frames of video data and store the video data within a memory of mobile device 5202. Accordingly, for example, a processor of mobile device 5200 may receive one or more frames of video information via camera 5202 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 5200 may receive optical information that may be sensed by camera 5202 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 5200 as data values and/or control data.

[0376] Mobile device 5200 may include manual input interface 5212. Manual input interface 5212 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 5200 may enter information into mobile device 5200 via manual interface 5212 to cause a processor of mobile device 5200 to enter a particular mode of operation. Manual interface 5212 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile

device 5200) during a particular mode of operation of mobile device 5200.

[0377] Mobile device 5200 may include display 5204. Display 5204 may provide visible information that may be utilized by a user during interaction with mobile device 5200. A portion or all of display 5204 may be touch sensitive such that objects making contact with display 5204 or objects coming within a proximity of display 5204 may be detected by a processor of mobile device 5200. Accordingly, for example, mobile authorization graphical user interface 5206 may be provided by display 5204 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, alphanumeric input boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 5200.

[0378] FIG. 52 shows architecture 5250. User interface 5252 may, for example, be included within architecture 5250 to allow user interaction with architecture 5250. For example, a dedicated key pad or keyboard may be included within user interface 5252 to allow alphanumeric data entry into architecture 5250.

[0379] Architecture 5250 may include one or more displays 5254. Display 5254 may, for example, be touch-sensitive. Accordingly, for example, display 5254 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 5254. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of

display 5254 may be detected by processor 5258 as alphanumeric data entry.

[0380] Alphanumeric entry boxes may, for example, be rendered onto display 5254. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 5252 and/or a virtual keypad rendered onto display 5254 to select alphanumeric characters to be placed within the alphanumeric entry box in accordance with a character position identified by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 5258 may receive alphanumeric characters as typed into a alphanumeric entry box of display 5254 and may use such alphanumeric characters as data input.

[0381] Display 5254 may, for example, provide data output from architecture 5250. For example, display 5254 may communicate data using a series of light pulses. Accordingly, for example, processor 5258 may cause one or more portions of display 5254 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 5254 via light pulses having varying characteristics. Display 5254 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0382] Architecture 5250 may include one or more transceivers 5256. Transceiver 5256 may communicate information to and/or may receive information from one or more devices. Transceiver 5256 may, for example,

communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly, for example, transceiver 5256 may allow a mobile device (e.g., mobile device 5200 of FIG. 52) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 5200 of FIG. 52) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 156 may exchange information with one or more other mobile devices via one or more associated cellular stations .

[0383] Transceiver 5256 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 5256 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 5256 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 5200 of FIG. 52) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network .

[0384] Architecture 5250 may include contactless communication device 5262, which may communicate via any one or more contactless communication methodologies, such as for example, near field communications (e.g., RFID), Bluetooth, touch simulation, light pulsing (e.g., via an LED), and electromagnetic data communication (e.g., via a dynamic magnetic stripe communications device) . Accordingly, for example, contactless communication device 5262 may be compatible with any contactless device, such as for example, an RFID enabled payment card and a contactless reader (e.g., a magnetic stripe reader or an NFC reader) .

[0385] A non-powered card may, for example, communicate with contactless communications device 5262. Contactless communication device 5262 may, for example, establish a carrier field (e.g., an RF field) that may be modulated by a device (e.g., an RFID tag) of a non-powered payment card. In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by contactless communications device 5262 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 5262 by modulating the RF field produced by contactless communications device 5262.

[0386] A powered card may, for example, communicate with contactless communication device 5262. A powered card may, for example, include a processor, a battery, a memory, wireless communication devices (e.g., a dynamic magnetic stripe communications device or RFID) and other electronics (e.g., buttons) that may allow a user to interact with the powered card to perform one

or more functions. Accordingly, for example, a powered card may be used to communicate specific information to contactless communication device 5262 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 5262 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications .

[0387] Contactless communication device 5262 may receive variable data sets from a powered card based upon, for example, manual input provided to a powered card. For example, a button associated with an on-line purchase may be pressed on the powered card that causes a variable data set (e.g., account number and expiration date) to be communicated from the powered card to contactless communication device 5262.

[0388] Discretionary data may, for example, be communicated by a powered card based upon which button was pressed on the powered card. In so doing, for example, a security code (e.g., "Ill") may be communicated within a discretionary data field when a button associated with a particular feature (e.g., pay with credit) is pressed on the powered card. As per another example, a different security code (e.g., "222") may be communicated within a discretionary data field when a button associated with a different feature (e.g., pay with debit) is pressed on the powered card. A powered card may, for example, communicate a different security code no matter what feature may be selected on the powered card. Accordingly, for

example, processor 5258 may identify what type of device may be in communication with contactless communication device 5262 by analyzing the data communicated to contactless communication device 5262.

[0389] Any device having contactless communication capability may communicate with contactless communication device 5262 to authorize functions that may be performed by a mobile device. An RFID enabled device (e.g., an RFID equipped automobile key) may, for example, communicate with contactless communication device 5262 to authorize functions that may be performed by a mobile device (e.g., mobile device 5200 of FIG. 52) on a device that may be controlled by the RFID enabled device (e.g., an automobile that corresponds to the RFID equipped automobile key). For example, processor 5258 may execute an automobile application that may wirelessly communicate with an automobile to perform remote functions (e.g., start an engine of the automobile or unlock the driver's door). Through use of an RFID equipped key, for example, such functions may be authorized to be performed by a mobile device (e.g., mobile device 5200 of FIG. 52) once the RFID equipped key has communicated the necessary security credentials (e.g., a key code) to an application running on a processor of the mobile device to establish that a one-to-one correspondence exists between the automobile and the RFID equipped key.

[0390] Architecture 5250 may include memory 5260 and/or processor 5258 may include internal memory. Accordingly, for example, application code may be stored within memory 5260 and/or processor 5258 and executed by processor 5258 in support of functions performed by architecture 5250. For example, an

application (e.g., a graphical user interface) may be executed by processor 5258 and displayed onto display 5254, which may be used to interact with a user of a mobile device (e.g., mobile device 5200 of FIG. 52). Persons skilled in the art will appreciate that executable application code may be communicated to architecture 5250 via any one or more interfaces of architecture 5250 (e.g., user interface 5252, display 5254, transceiver 5256, and/or contactless communication device 5262).

[0391] Application data (e.g., security credentials) may be stored within memory 5260 and accessed by processor 5258 during operation. For example, security credentials may be stored within memory 5260 and recalled by processor 5258 to authorize a function that may be performed by processor 5258 of a mobile device (e.g., mobile device 5200 of FIG. 52). Accordingly, for example, processor 5258 of a mobile device may challenge a user of the mobile device to produce security credentials to authorize any function that may be performed by the mobile device. A processor of the mobile device may, for example, validate the security credentials locally within the mobile device itself. Alternately, for example, security credentials may be forwarded to a network entity (e.g., an authorization server) for remote validation.

[0392] FIG. 53 shows network topology 5300 that may include, for example, mobile device 5302 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile device 5302 may, for example, include a contactless interface that may initiate, sustain, and/or terminate communication channel 5326 between contactless device

5304 and mobile device 5302. Contactless device 5304 and mobile device 5302 may communicate via channel 5326 using any number of contactless mediums, which may include for example, visible, audible, capacitive, electromagnetic, magnetic, and/or RF mediums.

[0393] Mobile device 5302 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 5312 and/or payment network 5314) and/or one or more wireless networks (e.g., mobile network 5310). Mobile device 5302 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile device 5302 to communicate information (e.g., voice and data) to cellular network access infrastructure 5306 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 5306 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0394] Mobile device 5302 may, for example, communicate with wireless access point 5308 over a wireless interface (e.g., a Bluetooth interface or a Wi-Fi interface). Accordingly, for example, mobile device 5302 may access one or more wired networks (e.g., IP network 5312 and/or payment network 5314) and/or one or more wireless networks (e.g., mobile network 5310) without the need to first gain access to cellular network access infrastructure 5306.

[0395] Contactless device 5304 may, for example, be a powered card, a non-powered card (e.g., a powered

payment card or a non-powered payment card) or any contactless enabled device (e.g., an RFID enabled device). Accordingly, for example, security credentials may be communicated via a contactless communication channel from contactless device 5304 to mobile device 5302 to authenticate a purchase transaction that may be performed by mobile device 5302. In so doing, for example, items for purchase on IP network 5312 (e.g., the internet) may be accessed by a browser of mobile device 5302 via an access point (e.g., wireless access point 5308 or cellular network access infrastructure 5306), payment information may be retrieved from a memory of mobile device 5302, a user of mobile device 5302 may be challenged for security credentials (e.g., at least a portion of a payment account number and a card expiration date communicated to mobile device 5302 from a payment card corresponding to the payment information retrieved from a memory of mobile device 5302), such payment information may be authenticated by such security credentials, and such payment information may be communicated to network entities (e.g., issuer 5320) to complete the purchase transaction.

[0396] Issuer 5320 may, for example, contact authorization server 5316 via a network (e.g., payment network 5314) with payment information and security credentials received from mobile device 5302 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile device 5302 via any one or more delivery options (e.g., via a short messaging service of mobile network 5310 or an email delivery service of IP network 5312). Mobile device 5302 may

allow a user to associate purchase categories (e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile device so that the user may receive a more detailed accounting of his or her expenditures on his or her receipt. Accordingly, for example, a user may enjoy a higher degree of integration such that a user may customize a level of detail provided on a receipt via mobile device 5302.

[0397] A payment receipt may, for example, be provided to mobile device 5302 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile device 5302 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0398] A processor of mobile device 5302 may, for example, authorize wireless device 5334 to perform functions that may be authenticated by contactless device 5304 (e.g., via security credentials communicated by contactless device 5304 to a processor of mobile device 5302). Accordingly, for example, a processor of mobile device 5302 may require security credentials to be communicated by contactless device 5304 via contactless communication channel 5326 and based upon a validity of the security credentials communicated, the processor may communicate instructions to wireless device 5334 via contactless communication channel 5336 to perform some function. As per another example, a processor of mobile device 5302 may communicate instructions (e.g., via wireless access point 5308 or cellular network access infrastructure 5306) to wireless device 5334 (e.g., a car or a home) to perform a function (e.g., start the

engine of the car) based upon a validity of security credentials communicated by contactless device 5304.

[0399] A processor of mobile device 5302 may, for example, locally validate security credentials communicated by contactless device 5304. Alternately, for example, mobile device 5302 may forward security credentials communicated by contactless device 5304 to a network entity (e.g., authorization server 5332) for remote validation.

[0400] A mobile device (e.g., mobile device 5324) may, for example, include a contactless communication device (e.g., an RFID device) that may initiate, sustain, and/or terminate contactless communication channel 5328 with merchant terminal 5318. Accordingly, for example, a processor of mobile device 5324 may communicate payment information to merchant terminal 5318 to complete a financial transaction. In so doing, for example, a processor of mobile device 5324 may receive payment information via contactless communication channel 5330 from contactless device 5322 (e.g., a powered or a non-powered card) and store the received payment information within a memory of mobile device 5324. To complete a purchase transaction, contactless device 5322 may, for example, be presented to mobile device 5324 and may communicate security credentials (e.g., at least a portion of a payment card number and a cardholder's name) via contactless communication channel 5330. A processor of mobile device 5324 may validate the security credentials and may forward the payment information onto merchant terminal 5318 to complete the purchase transaction.

[0401] FIG. 54 shows system 5400, which may include mobile device 5402 and contactless devices 5408-5414.

Mobile device 5402 may, for example, be a laptop computer, a PDA, a mobile telephonic device (e.g., a smartphone) , an MP3 player, a GPS, or any other mobile device. Display 5404 may be a touch-sensitive display (e.g., sensitive to a change in capacitance) . Contactless devices may, for example, include non-powered payment card 5408, identification card (e.g., driver's license 5410), powered payment card 5412, key 5414, and any other device capable of communicating security credentials to mobile device 5402 via a contactless communication channel that may be formed with mobile device 5402.

[0402] Mobile device 5402 and contactless devices 5408-5414 may each include a contactless communication device (e.g., an RFID device) that may communicate via a contactless communication channel that may be formed between mobile device 302 and contactless devices 5408-5414 after coming into proximity to one another. Contactless devices 5408-5414 may, for example, be tapped onto display 5404 of mobile device 5402 to establish a proximity relationship that forms a communication channel with mobile device 5402. As per another example, contactless devices 5408-5414 may be brought within a proximity distance (e.g., up to two inches) of mobile device 5402 to establish a contactless communication channel with mobile device 5402 .

[0403] A processor of mobile device 5402 may, for example, execute application code that may generate a graphical user interface (GUI) onto display 5404 of mobile device 5402. Message 5406 of a GUI may invite a user of mobile device 5402 to begin a mobile authorization by tapping a contactless device against

display 5404. As per another example, by tapping a contactless device against mobile device 5402, a processor of mobile device 5402 may autonomously determine that a mobile authorization is desired and may then generate a mobile authorization GUI onto display 5404.

[0404] Mobile device 5402 may, for example, autonomously determine a type of contactless device that may be tapped against it. For example, a processor of mobile device 5402 may receive security credentials that may be indicative of a non-powered payment card (e.g., security credentials received from non-powered payment card 5408 may include at least a portion of a payment card number and a cardholder's name). As per another example, a processor of mobile device 5402 may receive security credentials that may be indicative of a powered card (e.g., security credentials received from powered card 5412 may contain a dynamically generated security code). Security credentials received from powered card 5412 may, for example, include a dynamic security code that may change for each function authorized by powered card 5412.

[0405] A contactless device (e.g., key 5414) may, for example, be a key that may start the ignition of a car, open a door to a home, or open a safe deposit box. Key 5414 may, for example, include a contactless communication device (e.g., an RFID device) that may communicate security credentials to a processor of mobile device 5402. Once security credentials received from key 5414 are validated, a processor of mobile device 5402 may effect an operation that may eliminate the need to physically use key 5414 to perform the

operation (e.g., a user of mobile device 5402 may remotely start the engine of the user's car by running an application on a processor of mobile device 5402 to validate security credentials received from key 5414 and wirelessly communicate with a wireless device of the user's car to start its ignition) . As per an example, the user's physical key 5414 may, for example, be locked inside the user's car, in which case the user may select another contactless device (e.g., identification card 5410) to present to mobile device 5402. Identification card 5410 may, for example, communicate security credentials to a processor of mobile device 5402 and once the processor authorizes the identify of the user of mobile device 5402, mobile device 5402 may, for example, wirelessly communicate with the user's car to unlock its doors so that the user may retrieve key 5414 that may have been previously locked within the user's car.

[0406] Powered payment card 5412 may, for example, include electronics to simulate a human touch (e.g., powered payment card 5412 may generate a change in capacitance that may be sensed by display 5404) . Through a series of simulated touches, powered payment card 5412 may communicate a series of data bits to display 5404, which may then be processed by a processor of mobile device 5402 as security credentials. In so doing, for example, a contactless communication channel may be established where data is transferred from powered payment card 5412 to a processor of mobile device 5402 via a series of simulated touches to authorize a function to be performed (or commanded to be performed) by a processor of mobile device 5402.

[0407] Powered payment card 5412 may, for example, include a light sensor. Accordingly, for example, powered payment card 5412 may be sensitive to light pulses generated within a region of display 5404. The light sensor of powered payment card 5412 may receive a series of light pulses, which may be construed by a processor of powered payment card 5412 as data generated by a processor of mobile device 5402. In so doing, for example, powered payment card 5412 may receive an optical data stream represented by a series of light pulses generated by display 5404. As such, a two-way communication channel may be formed, where simulated touches may generate a data stream from powered payment card 5412 to mobile device 5402 and light pulses may generate a data stream from mobile device 5402 to powered payment card 5412.

[0408] Mobile device 5402 may, for example, include a motion-capture device (e.g., a camera) . Identification card (e.g., driver's license 5410) may, for example, include a barcode. Accordingly, for example, a contactless communication channel may be formed between identification card 5410 and mobile device 5402 where a camera of mobile device 5402 may capture an image of the barcode of identification card 5410. In so doing, for example, a processor of mobile device 5402 may analyze the barcode image and extract information from the barcode image that may be construed by the processor as security credentials that when validated, may authorize a processor of mobile device 5402 to perform (or cause to perform) any function .

[0409] As per another example, a user's photograph may appear on identification card 5410. Accordingly,

for example, a camera of mobile device 5402 may capture an image of the picture and a processor of mobile device 5402 may construe the captured image as a security credential. In so doing, for example, a processor of mobile device 5402 may compare a scanned image of a user's picture to an image contained within a memory of mobile device 5402 (or contained within a memory of a remote authorization server) for authorization. As per yet another example, a user may snap a picture of himself or herself with a camera of mobile device 5402 so that a processor of mobile device 5402 may scan the snapped picture for authorization purposes .

[0410] Mobile device 5402 may, for example, require authorization before being activated for use. Accordingly, for example, a processor of mobile device 5402 may require a password to be entered and verified before a processor of mobile device 5402 may unlock functions available to be performed by mobile device 5402. In so doing, for example, one or more contactless devices 5408-5414 may be presented to mobile device 5402 and security credentials may be communicated by the one or more contactless devices 5408-5414 in lieu of providing a password to mobile device 5402. Upon validation of the security credentials, a processor of mobile device 5402 may unlock those functions that may be available to be executed by the processor of mobile device 5402.

[0411] FIG. 55 shows GUI 5500, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 5500 may, for example, provide a summary of each card that may be available for use within a memory of the mobile device

(e.g., each card may be displayed as virtual cards having visible and functional features that are substantially the same as their physical counterparts).

[0412] Physical card (e.g., payment card) information (e.g., track 1, track 2, and/or track 3 magnetic stripe data) may be communicated by the physical card to the mobile device via a contactless communication channel and such information may be displayed within a virtual card (e.g., virtual payment card 5502) as summary information that may be associated with the physical payment card. A payment card number communicated to a processor of a mobile device may, for example, include issuer identification as well as an issuing network identifier. Accordingly, for example, a processor of a mobile device may analyze the payment card number received from a physical payment card and may render a portion or all of the identifying information associated with the payment card number onto virtual payment card 5502. In so doing, for example, issuer identification as well as a logo representative of an issuing network identifier may be rendered onto virtual payment card 5502. Other virtual payment cards may, for example, be sorted behind virtual payment card 5502 in virtually any order (e.g., most popular to least popular, highest credit limit to lowest credit limit, or highest credit available to lowest credit available). Other virtual cards (e.g., virtual gift card 404 and virtual driver's license 5506) may be stored within a memory of a mobile device as well.

[0413] FIG. 56 shows GUI 5600, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 5600 may, for

example, allow a selection of a virtual card contained within a memory of a mobile device to be authorized for use by its physical counterpart. Accordingly, for example, a user may touch anywhere within the vicinity of virtual card 5604 as it is being displayed by GUI 5600. Such a selection may be verified by highlighting attributes of a selected card (e.g., highlighting an outline of virtual card 5604) and by displaying the selected virtual card within verification region 502. In so doing, for example, a user of a mobile device may view a virtual card that is selected for authorization (e.g., as viewed within region 5602) so that the user may retrieve the physical card that corresponds to the virtual card that is to be authorized.

[0414] Once retrieved, a user may tap the physical card against region 5602. Accordingly, for example, a contactless communication channel (e.g., an RFID communication channel) may be formed between the physical card and the mobile device, such that security credentials may be communicated from the physical card to the mobile device via the contactless communication channel to authorize virtual payment card 5602 for use. In so doing, for example, a physical card may communicate security credentials (e.g., at least a portion of a payment card number of the physical card and/or a cardholder's name) to a processor of the mobile device and the processor may compare the received security credentials to security credentials stored within a memory of the mobile device that may be associated with virtual payment card 5602. If the processor of the mobile device determines that the received security credentials match at least a portion of the security credentials associated with virtual

payment card 5602, then virtual card 5602 may be authorized for use.

[0415] FIG. 57 shows GUI 5700, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 5700 may, for example, allow the authorization of a virtual card via an alternate contactless communication channel. For example, GUI 5700 may display a virtual payment card (e.g., virtual payment card 5702) in a region within GUI 5700 that may provide a touch-sensitive area 5704 and area 5706 that may be capable of producing light pulses having varying characteristics (e.g., intensity, pulse width, and/or color) .

[0416] A user's physical card that corresponds to virtual payment card 5702 may, for example, be a powered card having touch-simulation electronics and a light sensor. Accordingly, for example, the user's physical card may be pressed against region 5702, such that the touch simulation electronics of the physical card aligns with touch-sensitive portion 5704 and the light sensor of the physical card aligns with portion 5706. In so doing, for example, a contactless communication channel may be formed between the user's physical card and the mobile device, such that data may be communicated from the user's physical card to the mobile device through a series of simulated touches generated by the physical card and sensed at portion 5704 by a processor of the mobile device. Such communicated data may be construed by a processor of the mobile device as security credentials communicated by the user's physical card.

[0417] Security credentials that may be communicated (e.g., via a capacitive, visible, audible,

electromagnetic, magnetic, or RFID-based contactless communication channel) to a mobile device by a powered payment card may, for example, include a dynamic security code that may change with each use. Accordingly, for example, a network entity (e.g., an authorization server) may be synchronized with the user's powered payment card, such that when a dynamic security code of the powered payment card changes, so does the corresponding dynamic security code of the authorization server. In so doing, for example, a dynamic security code received by a mobile device from a powered payment card during authorization of virtual payment card 5702 may be communicated by a processor of the mobile device to an authorization server for verification that the dynamic security code matches the dynamic security code maintained by the authorization server. If so, virtual payment card 5702 may be authorized for use by the mobile device (e.g., payment information associated with virtual payment card 5702 may be communicated by the mobile device to complete a purchase transaction) .

[0418] FIG. 58 shows system 5800 that may include mobile terminal 5802, payment card 5808, network 5814 and authorization server 5810. A processor of mobile device 5802 may, for example, execute an application (e.g., GUI 5804) that allows a user of mobile device 5802 to perform any financial account management function (e.g., change from paper statements to e-statements, transfer money from one account to another or open a checking account) .

[0419] Prior to authorizing the financial account management function, GUI 5804 may challenge a user of mobile device 5802 to tap a card against mobile device

5802 that may be associated with the transaction. Accordingly, for example, a payment card (e.g., payment card 5808) that may be associated with the financial accounts used for the financial account management function may be used as a security credential to authorize the transaction. In so doing, for example, security credentials communicated by payment card 5808 to mobile device 5802 via contactless communication channel 5806 (e.g., an RFID communication channel) may be relayed by mobile device 5802 to authorization server 5810 via communication channel 5812 for authorization of the financial account management function. Once authorized, a processor of mobile device 5802 may receive the authorization from authorization server 5810 and may contact other network entities (e.g., a payment server of network 5814) to complete the financial account management function.

[0420] Payment card 5808 need not be directly related to the financial accounts involved with a financial account management function. Instead, authorization server 5810 may, for example, maintain links between various financial accounts that may be owned by a user of a mobile device. Accordingly, for example, while payment card 5808 may not be used as the source account from which money is to be transferred to an auto loan account, payment card 5808 may nevertheless be linked with the source account (e.g., M/C 1234). In so doing, for example, authorization server 5810 may recognize the link between payment card 5808 and the source account (e.g., M/C 1234) and may authorize the money transfer due to the recognized link.

[0421] Payment card 5808 may, for example, be a powered payment card. Accordingly, for example, a dynamic security code may be communicated from payment card 5808 to a processor of mobile device 5802 (e.g., via a discretionary data field of a magnetic stripe message communicated by payment card 5808) along with other identifying information (e.g., at least a portion of a dynamic payment card number or a cardholder's name). In so doing, for example, the dynamic security code and/or other optional identifying information may serve as the security credential that authorizes mobile device 5802 to perform the requested function. The dynamic security code and/or other optional identifying information may, for example, be relayed to authorization server 5810. Accordingly, for example, authorization server 5810 may analyze the security code and any other optional identifying information to determine whether the requested function is to be authorized. If so, the authorization may be communicated by authorization server 5810 to a processor of mobile device 5802 via communication channel 5812 so that the function may be completed.

[0422] FIG. 59 shows system 5900 that may include mobile terminal 5902, key 5908, network 5912 and car 5914. A processor of mobile device 5902 may, for example, execute an automobile application (e.g., GUI 5904) that may allow a user of mobile device 5902 to establish wireless link 5910 between car 5914 and mobile device 5902. Accordingly, for example, a user of mobile device 5902 may communicate wireless commands to car 5914 via wireless communication channel 5910.

[0423] A user may, for example, start his or her car from the convenience and warmth of the user's office at

work when temperatures outside may warrant a time period within which car 5914 may need to warm up. Accordingly, for example, a user may start his or her car via commands communicated by a processor of mobile device 5902 to car 5914 prior to leaving the office for the day. In so doing, for example, a processor of mobile device 5902 may require authorization to issue the command, in which case the user may be challenged to present key 5908 within a communication distance from mobile device 5902 to form contactless communication channel 5906. Security credentials may, for example, be communicated from key 5908 to a processor of mobile device 5902 via contactless communication channel 5906 and the processor may compare the received security credentials to security credentials stored within a memory of mobile device 5902 (or a remote authorization server). If a match is found, for example, a processor of mobile device 5902 may be authorized to issue one or more commands 5916 to car 5914.

[0424] A wireless device of car 5914 may, for example, communicate to a processor of mobile device 5902 via communication channel 5910. Accordingly, for example, once a command is authorized and sent to a wireless device of car 5914 by a processor of mobile device 5902, the wireless device of car 5914 may respond with an acknowledgment that the command (e.g., "Start car") was executed. A wireless device of car 5914 may, for example, provide status to a display of mobile device 5902. Accordingly, for example, a wireless device of car 5914 may report a gasoline level status to mobile device 5902 via communication channel 5910 so that the user of mobile device 5902 may know

that leaving car 5914 running for a length of time may deplete the car's gas reserves.

[0425] FIG. 60 shows GUI 6000, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 6000 may, for example, allow a user of a mobile device to determine how certain functions that may be performed by the mobile device may be authorized. GUI 6000 may, for example, provide authorization options 6002 to determine how the mobile device itself may be authorized for use. A PIN, for example, may be required to be entered in order to activate the mobile device for use. As per another example, a memory of the mobile device may contain information associated with any physical card. Accordingly, for example, authorization to activate the mobile device may require that a user produce a physical card (e.g., a driver's license) that may correspond to a virtual card (e.g., a virtual driver's license) that may be stored within a memory of the mobile device. Alternately, for example, a physical card that corresponds to any virtual card or any virtual bank card stored within a memory of the mobile device may be used to authorize the mobile device for use .

[0426] Banking functions performed by a mobile device may, for example, be authorized as defined by options 6004. A mobile device may, for example, be equipped with scanning capability, such that biometrics (e.g., fingerprints) may be taken from the user of the mobile device and verified before banking functions may be authorized. As per another example, a dynamic security code communicated to a processor of a mobile device by a powered payment card via a contactless

communication channel may authorize banking functions to be performed by the mobile device.

[0427] Functions associated with remote operation of a car may, for example, be authorized as defined by options 6006. A mobile device may, for example, be equipped with a camera, such that only when a picture of an authorized user is taken with the camera and verified by a processor of the mobile device will that user be able to issue remote commands (e.g., unlock driver's door) to the user's car.

[0428] Other functions, such as remote house functions, may be authorized as defined by options 6008. For example, a garage door of a user's house may be commanded to be opened by the user's mobile device, but only if a house key communicates security credentials (e.g., a key code) to a processor of the user's mobile device via a contactless communication channel. Alternately, for example, a user may disable any house functions to be conducted by the user's mobile device.

[0429] FIG. 61 shows flow charts for process sequences 6110-6140. Process sequence 6110 may, for example, execute an authorization setup application (e.g., a GUI) on a mobile device that allows a user of the mobile device to select authorization options (e.g., as in steps 6111-6112) to be enforced by a processor of the mobile device (e.g., as in step 6113). For example, banking functions that may be performed by a mobile device may first require that a physical bank card be placed in proximity to the mobile device so that the physical bank card may communicate security credentials to a processor of the mobile device via a contactless communication channel that may be formed

between the physical banking card and the mobile device. In so doing, for example, a processor of the mobile device may compare the security credentials received from the physical card to security credentials stored within a memory of the mobile device (or remote authorization server). Upon a successful comparison, a processor of a mobile device may authorize banking functions to be performed by the mobile device.

[0430] A memory of a mobile device may, for example, contain a number of virtual cards that may correspond to information communicated to a processor of the mobile device via physical card counterparts to the virtual cards. Such virtual cards may, for example, be selected (e.g., as in step 6121 of sequence 6120) to perform a function in conjunction with the mobile device (e.g., payment information associated with a virtual payment card may be selected to complete a purchase transaction using the mobile device). In step 6122, a user of a mobile device may be required to produce a physical card that corresponds to the selected virtual card. A contactless communication channel (e.g., an RFID communication channel) may be formed between the physical card and the mobile device so that security credentials may be communicated from the physical card to a processor of the mobile device via the contactless communication channel (e.g., as in step 6123). In step 6124, a processor of a mobile device may compare the security credentials to security credentials stored within a memory of the mobile device (or remote authorization server) that corresponds to a physical card. Upon a favorable comparison, a processor of a mobile device may authorize the selected virtual card for use.

[0431] Any function (e.g., non-purchase transactions) that may be performed by a mobile device may be requested (e.g., as in step 6131 of sequence 6130) and challenged (e.g., as in step 6132 of sequence 6130). For example, a processor of a mobile device may be requested to perform any function (e.g., remotely start the engine of a user's car) and a processor of the mobile device may first require security credentials to be presented before the function may be performed. Security credentials may, for example, be any information that may be communicated to a mobile device by a contactless device (e.g., an RFID enabled ignition key) via a contactless communication channel. A processor of the mobile device may authorize the requested function if the security credentials are verified (e.g., as in step 6133) and may deny the requested function if the security credentials are not verified (e.g., as in step 6134).

[0432] In step 6141 of sequence 6140, a user of a mobile device may request a function to be performed by a mobile device. Upon receipt of security credentials communicated by a contactless communication device to a processor of the mobile device (e.g., as in step 6142), the security credentials may be forwarded (e.g., as in step 6143) to a remote authorization server for verification. In step 6144, the remote authorization server may communicate a message to a processor of the mobile device to either grant or deny authorization for the mobile device to perform the requested function.

[0433] FIG. 62 shows card 6200 that may include, for example, a dynamic number that may be entirely, or partially, displayed using a display (e.g., display 6206). A dynamic number may include a permanent

portion such as, for example, permanent portion 6204 and a dynamic portion such as, for example, dynamic portion 6206. Card 6200 may include a dynamic number having permanent portion 6204 and permanent portion 6204 may be incorporated on card 6200 so as to be visible to an observer of card 6200. For example, labeling techniques, such as printing, embossing, laser etching, etc., may be utilized to visibly implement permanent portion 6204.

[0434] Card 6200 may include a second dynamic number that may be entirely, or partially, displayed via a second display (e.g., display 6208). Display 6208 may be utilized, for example, to display a dynamic code such as a dynamic security code. Card 6200 may also include third display 6222 that may be used to display graphical information, such as logos and barcodes. Third display 6222 may also be utilized to display multiple rows and/or columns of textual and/or graphical information.

[0435] Persons skilled in the art will appreciate that any one or more of displays 6206, 6208, and/or 6222 may be implemented as a bi-stable display. For example, information provided on displays 6206, 6208, and/or 6222 may be stable in at least two different states (e.g., a powered-on state and a powered-off state). Any one or more of displays 6206, 6208, and/or 6222 may be implemented as a non-bi-stable display. For example, the display is stable in response to operational power that is applied to the non-bi-stable display. Other display types, such as LCD or electro-chromic, may be provided as well.

[0436] Other permanent information, such as permanent information 6220, may be included within card

6200, which may include user specific information, such as the cardholder's name or username. Permanent information 6220 may, for example, include information that is specific to card 6200 (e.g., a card issue date and/or a card expiration date) . Information 6220 may represent, for example, information that includes information that is both specific to the cardholder as well as information that is specific to card 6200.

[0437] Card 6200 may accept user input data via any one or more data input devices, such as buttons 6210-6218. Buttons 6210-6218 may be included to accept data entry through mechanical distortion, contact, or proximity. Buttons 6210-6218 may be responsive to, for example, induced changes and/or deviations in light intensity, pressure magnitude, or electric and/or magnetic field strength. Such information exchange may then be determined and processed by a processor of card 6200 as data input. An RFID chip may, for example, include memory that may be populated with data to be communicated via RFID antenna 6224 when one or more buttons 6210-6218 are pressed. Accordingly, for example, once a button is pressed, RFID data may be loaded into an RFID chip memory and once an RFID communication channel is formed (e.g., once card 6200 is brought within an RFID communication distance of an RFID enabled device) the data in RFID chip memory may be communicated via an RFID communication channel using RFID antenna 6224. Once RFID data is communicated, or after a configurable delay period, the RFID chip memory may be erased.

[0438] FIG. 62 shows architecture 6250, which may include one or more processors 6254. One or more processors 6254 may be configured to utilize external

memory 6252, internal memory of processor 6254, internal memory of RFID chip 6262, or a combination of external memory 6252, internal memory of RFID chip 6262, and internal memory of processor 6254 for dynamically storing information, such as executable machine language, related dynamic machine data, RFID data and user input data values.

[0439] One or more of the components shown in architecture 6250 may be configured to transmit information to processor 6254 and/or may be configured to receive information as transmitted by processor 6254. For example, one or more displays 6256 may be coupled to receive data from processor 6254. The data received from processor 6254 may include, for example, at least a portion of dynamic numbers and/or dynamic codes. The data to be displayed on the display may be displayed on one or more displays 6256.

[0440] One or more displays 6256 may be, for example, touch sensitive and/or proximity sensitive. For example, objects such as fingers, pointing devices, etc., may be brought into contact with displays 6256, or in proximity to displays 6256. Detection of object proximity or object contact with displays 6256 may be effective to perform any type of function (e.g., transmit data to processor 6254). Displays 6256 may have multiple locations that are able to be determined as being touched, or determined as being in proximity to an object.

[0441] Persons skilled in the art will appreciate that a card (e.g., card 6200 of FIG. 62) may, for example, be a self-contained device that derives its own operational power from one or more batteries 6258. Furthermore, one or more batteries 6258 may be

included, for example, to provide operational power for a period of time (e.g., approximately 2-4 years) . One or more batteries 6258 may be included, for example, as rechargeable batteries.

[0442] Input and/or output devices may be implemented on architecture 6250. For example, integrated circuit (IC) chip 6260 (e.g., an EMV chip) may be included on architecture 150 to communicate information to a chip reader (e.g., an EMV chip reader) via contacts that may be formed on a surface of a card (e.g., card 6200 of FIG. 62) . Other input and/or output devices may be included on architecture 6250, for example, to provide any number of input and/or output capabilities within architecture 6250. For example, other input and/or output devices may include an audio device capable of receiving and/or transmitting audible information. Other input and/or output devices may include a device that exchanges analog and/or digital data using a visible data carrier. Alternately, for example, other input and/or output devices may include a device that is sensitive to a non-visible data carrier, such as an infrared data carrier or electromagnetic data carrier.

[0443] A dynamic magnetic stripe communications device may be included within architecture 6250 to communicate information to, for example, a read-head of a magnetic stripe reader via, for example, electromagnetic signals. For example, electromagnetic field generators 6270-6274 may be included to communicate one or more tracks of electromagnetic data to read-heads of a magnetic stripe reader. Electromagnetic field generators 6270-6274 may include, for example, a series of electromagnetic elements,

where each electromagnetic element may be implemented as a coil wrapped around one or more materials (e.g., a magnetic material and/or a non-magnetic material). Additional materials may be placed outside the coil (e.g., a magnetic material and/or a non-magnetic material).

[0444] Electrical excitation by processor 6254 of one or more coils of one or more electromagnetic elements via, for example, driving circuitry 6264 may be effective to generate electromagnetic fields from one or more electromagnetic elements. One or more electromagnetic field generators 6270-6274 may be utilized to communicate electromagnetic information to, for example, one or more read-heads of a magnetic stripe reader.

[0445] Timing aspects of information exchange between architecture 6250 and the various I/O devices implemented on architecture 6250 may be determined by processor 6254. Detector 6266 may be utilized, for example, to sense the proximity and/or actual contact, of an external device, which in turn, may trigger the initiation of a communication sequence. The sensed presence and/or touch of the external device may then be communicated to a controller (e.g., processor 6254), which in turn may direct the exchange of information with the external device. The sensed presence and/or touch of the external device may be effective to, for example, determine the type of device or object detected.

[0446] For example, the detection may include the detection of, for example, a read-head of a magnetic stripe reader. In response, processor 6254 may activate one or more electromagnetic field generators

6270-6274 to initiate a communications sequence with, for example, one or more read-heads of a magnetic stripe reader. The timing relationships associated with communications between one or more electromagnetic field generators 6270-6274 and one or more read-heads of a magnetic stripe reader may be provided through use of the detection of the magnetic stripe reader.

[0447] Persons skilled in the art will appreciate that processor 6254 may provide user-specific and/or card-specific information through utilization of any one or more of buttons 6210-6218, RFID chip 6262, RFID antenna 6268, IC chip 6260, electromagnetic field generators 6270-6274, and any other input and/or output device. RFID antenna 6268 may, for example, be brought within a communication distance of an RFID enabled device which may be generating a carrier field (e.g., an RF field) . In so doing, RFID antenna 6268 may collect energy from the RF field which may then be detected by RFID chip 6262. RFID chip 6262 may, for example, communicate a presence of an RFID communication device to processor 6252. Processor 6252 may, in turn, populate a memory of RFID chip 6262 with user-specific and/or card-specific information (e.g., a payment account number, cardholder name, and a dynamic security code) that may then be communicated to the RFID enabled device via RFID antenna 168.

[0448] RFID antenna 6268 may be configured to receive data from an RFID device (e.g., an RFID tag) . Accordingly, for example, RFID chip 6262 may interrogate the capabilities of an RFID device and may receive data from the RFID device upon a determination that the RFID device may communicate data. RFID antenna 6268 may, for example, be provided as two or

more RFID antennas that may be used to enhance RFID data communication and/or reception with an RFID enabled device.

[0449] FIG. 63 shows network topology 6300 that may include, for example, mobile device 6302 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile device 6302 may, for example, include a contactless interface that may initiate, sustain, and/or terminate communication channel 6326 between card 6304 and mobile device 6302. Card 6304 and mobile device 6302 may communicate via channel 6326 via a contactless communication medium (e.g., an RF medium).

[0450] Mobile device 6302 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 6312 and/or payment network 6314) and/or one or more wireless networks (e.g., mobile network 6310). Mobile device 6302 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile device 6302 to communicate information (e.g., voice and data) to cellular network access infrastructure 6306 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 6306 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0451] Mobile device 6302 may, for example, communicate with wireless access point 6308 over a wireless interface (e.g., a Bluetooth interface or a

Wi-Fi interface) . Accordingly, for example, mobile device 6302 may access one or more wired networks (e.g., IP network 6312 and/or payment network 6314) and/or one or more wireless networks (e.g., mobile network 6310) without the need to first gain access to cellular network access infrastructure 6306.

[0452] Card 6304 may, for example, be a powered card or a non-powered card (e.g., a powered payment card or a non-powered payment card) . Accordingly, for example, payment information (e.g., a payment account number and a card expiration date) may be communicated from card 6304 to mobile device 6302 in support of a financial transaction being conducted by mobile device 6302. In so doing, for example, items for purchase on IP network 6312 (e.g., the internet) may be accessed by a browser of mobile device 6302 via an access point (e.g., wireless access point 6308 or cellular network access infrastructure 6306) . Mobile device 6302 may, for example, complete a purchase transaction by first obtaining required payment information from card 6304 and then communicating such payment information to network entities (e.g., payment server 6316 and/or issuer 6320) .

[0453] Payment server 6316 may, for example, contact issuer 6320 via a network (e.g., payment network 6314) with payment information received from mobile device 6302 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile device 6302 via any one or more delivery options (e.g., via a short messaging service of mobile network 6310 or an email delivery service of IP network 6312) . Mobile device 6302 may allow a user to associate purchase categories

(e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile device so that the user may receive a more detailed accounting of his or her expenditures on his or her receipt. Accordingly, for example, a user may enjoy a higher degree of integration such that a user may customize a level of detail provided on a receipt via mobile device 6302. A payment receipt may, for example, be provided to mobile device 6302 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile device 6302 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation .

[0454] A device (e.g., mobile device 6328 and/or card 6322) may, for example, include a contactless communication device (e.g., an RFID device) that may initiate, sustain, and/or terminate a contactless communication channel (e.g., an RFID communications channel) with merchant terminal 6318. Accordingly, for example, card 6322 and/or mobile device 6328 may communicate payment information to merchant terminal 6318 to complete a financial transaction. In so doing, for example, mobile device 6328 and/or card 6322 may first receive a request from a user to communicate payment information to merchant terminal 6318.

[0455] As per an example, a user of card 6322 may press a button on card 6322 that may cause payment information to be transferred to a memory of a processor (e.g., an RFID chip) . An associated RFID antenna may, for example, sense the presence of merchant terminal 6318 by detecting an RF carrier field that may be generated by an RFID device of merchant terminal 6318. Once the presence of merchant terminal

6318 is sensed, payment information may be transferred from an RFID chip of card 6322 to an RFID antenna of card 6322 to communicate the payment information via an RFID communication channel to merchant terminal 6318 to complete a financial transaction.

[0456] As per another example, card 6322 may be a non-powered card (e.g., a non-powered payment card) . Accordingly, for example, card 6322 may include an RFID chip and associated RFID antenna that may be brought within proximity to merchant terminal 6318. An RFID antenna of card 6322 may sense an RF carrier field generated by merchant terminal 6318 and may derive operational power from the RF carrier field. The operational power may, for example, be collected by an RFID antenna of card 6322 and provided to an associated RFID chip of card 6322 in order to energize the RFID chip of card 6322. Once energized, an RFID chip of card 6322 may modulate an RF carrier field generated by merchant terminal 6318 to, for example, communicate payment information from card 6322 to merchant terminal 218 to complete a purchase transaction.

[0457] Any computing device (e.g., desktop computer 6330) may, for example, provide contactless communication electronics (e.g., an RFID reader) that may communicate with a contactless communication device (e.g., card 6332 and/or mobile device 6334) . Accordingly, for example, any information that may be communicated by card 6332 (e.g., payment information) may be received by computing device 6330 (e.g., received via an RFID communication channel established between card 6332 and computing device 6330) and forwarded onto a network entity (e.g., issuer 6320 and/or payment server 6316) to complete a purchase

transaction. Persons skilled in the art will appreciate that any RFID information may be exchanged between computing device 6330 and an RFID enabled device (e.g., card 6332 and/or mobile device 6334).

[0458] FIG. 64 shows mobile device 6400. Mobile device 6400 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, mobile device 6400 may be operated in a mobile environment while a user of mobile device 6400 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 6400 may perform multiple functions simultaneously (e.g., a person may carry on a conversation while at the same time browsing and purchasing products on the internet).

[0459] Mobile device 6400 may include audio processing devices (e.g., microphone 6408 and speaker 6410). Accordingly, for example, mobile device 6400 may receive voice commands from a user via microphone 6408 and may process such commands to perform a function. For example, a user may place mobile device 6400 into a desired operational mode by speaking a command into microphone 6408 that is associated with the desired operational mode. In so doing, for example, mobile device 6400 may engage in hands-free operation by receiving voice commands via microphone 6408 and performing functions associated with the received voice commands.

[0460] Mobile device 6400 may receive data input via microphone 6408. For example, a voice-band modem may generate signals in a voice-band frequency range that

may be received by microphone 6408. A processor of mobile device 6400 may interpret the received audible information as data signals and may process the data signals as, for example, data values and/or control data input .

[0461] Mobile device 6400 may include camera 6402. Camera 6402 may capture one or more frames of video data and store the video data within a memory of mobile device 6400. Accordingly, for example, a processor of mobile device 6400 may receive one or more frames of video information via camera 6402 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 6400 may receive optical information that is sensed by camera 6402 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 6400 as data values and/or control data.

[0462] Mobile device 6400 may include manual input interface 6412. Manual input interface 6412 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 6400 may enter information into mobile device 6400 via manual interface 6412 to cause a processor of mobile device 6400 to enter a particular mode of operation. Manual interface 6412 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile

device 6400) during a particular mode of operation of mobile device 6400.

[0463] Mobile device 6400 may include display 6404. Display 6404 may provide visible information that may be utilized by a user during interaction with mobile device 6400. A portion or all of display 6404 may be touch sensitive such that objects making contact with display 6404 or objects coming within a proximity of display 6404 may be detected by a processor of mobile device 6400. Accordingly, for example, RFID operations graphical user interface 6406 may be provided by display 6404 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, textual input boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 6400.

[0464] FIG. 64 shows architecture 6450. User interface 6452 may, for example, be included within architecture 6450 to allow user interaction with architecture 6450. For example, a dedicated key pad or keyboard may be included within user interface 6452 to allow alphanumeric data entry into architecture 6450.

[0465] Architecture 6450 may include one or more displays 6454. Display 6454 may, for example, be touch-sensitive. Accordingly, for example, display 6454 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 6454. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of

display 6454 may be detected by processor 6458 as alphanumeric data entry.

[0466] Alphanumeric entry boxes may, for example, be rendered onto display 6454. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 6452 and/or a virtual keypad rendered onto display 6454 to select alphanumeric characters to be placed within the alphanumeric entry box in accordance with a character position identified by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 6458 may receive alphanumeric characters as typed into a alphanumeric entry box of display 6454 and may use such alphanumeric characters as data input.

[0467] Display 6454 may, for example, provide data output from architecture 6450. For example, display 6454 may communicate data using a series of light pulses. Accordingly, for example, processor 6458 may cause one or more portions of display 6454 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 6454 via light pulses having varying characteristics. Display 6454 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0468] Architecture 6450 may include one or more transceivers 6456. Transceiver 6456 may communicate information to and/or may receive information from one or more devices. Transceiver 6456 may, for example,

communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly, for example, transceiver 6456 may allow a mobile device (e.g., mobile device 6400 of FIG. 64) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 6400 of FIG. 64) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 356 may exchange information with one or more other mobile devices via one or more associated cellular stations .

[0469] Transceiver 6456 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 6456 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 6456 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 6400 of FIG. 64) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network .

[0470] Architecture 6450 may include RFID chip 6464, RFID antenna 6462, and optional RFID antenna 6466 which may combine to communicate with an RFID enabled device via an RFID communication channel. Accordingly, for example, architecture 6450 may be compatible with any RFID device, such as for example, an RFID enabled card, an RFID reader, and an RFID enabled computing device (e.g., an RFID enabled desktop computer) . RFID antenna 6466 may, for example, be provided to enhance RFID data communication and/or reception.

[0471] RFID antenna 6462 and/or RFID antenna 6466 may, for example, establish an RF carrier field that may be modulated by an RFID device (e.g., an RFID tag of a non-powered payment card) . In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by RFID antenna 6462 and/or RFID antenna 6466 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to RFID antenna 6462 and/or RFID antenna 6466 by modulating the RF field produced by RFID antenna 6462 and/or RFID antenna 6466.

[0472] A powered card may, for example, communicate with RFID antenna 6462 and/or RFID antenna 6466. A powered card may, for example, include a processor, a battery, a memory, a wireless communications device (e.g., a powered RFID device) and other electronics (e.g., buttons) that may allow a user to interact with the powered card to perform one or more functions. Accordingly, for example, a powered card may be used to communicate specific information to RFID antenna 6462 and/or RFID antenna 6466 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively

communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to RFID antenna 6462 and/or RFID antenna 6466 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications .

[0473] RFID chip 6464 may, for example, receive RFID data from processor 6458 and may store such RFID data temporarily. Accordingly, for example, once an RFID communication channel is formed with an RFID enabled device, RFID data contained within RFID chip 6464 may be communicated to the RFID enabled device via RFID antenna 6462 and/or RFID antenna 6466. RFID antennas 6462 and 6466 may, for example, communicate the same RFID data to an RFID enabled device. RFID antennas 6462 and 6466 may, for example, communicate different RFID data sets to an RFID enabled device and the differences between the RFID data sets communicated may provide multiple other channels of data that may be communicated (e.g., an amplitude difference between RFID data sets may be an RFID data channel and a phase difference between RFID data sets may be an additional RFID data channel) .

[0474] Architecture 6450 may include memory 6460 and/or processor 6458 may include internal memory. Accordingly, for example, application code may be stored within memory 6460 and/or processor 6458 and executed by processor 6458 in support of functions performed by architecture 6450. For example, an application (e.g., a graphical user interface) may be executed by processor 6458 and displayed onto display 6454, which may be used to interact with a user of a mobile device (e.g., mobile device 6400 of FIG. 64) .

Persons skilled in the art will appreciate that executable application code may be communicated to architecture 6450 via any one or more interfaces of architecture 6450 (e.g., user interface 6452, display 6454, transceiver 6456, and/or RFID antennas 6462 and/or 6466) .

[0475] Application data (e.g., payment data) may be temporarily stored within RFID chip 6464 and communicated by RFID antenna 6462 and/or RFID antenna 6466 during operation. For example, payment data may be temporarily communicated to RFID chip 6464 by processor 6458 during a financial transaction being conducted via an RFID communication channel between a mobile device (e.g., mobile device 6400 of FIG. 64) and another RFID device (e.g., a merchant terminal) . Once RFID data is communicated (or after a configurable delay period has expired) , processor 6458 may cause the payment data stored within RFID chip 6464 to be erased so as to reduce an ability of an RFID skimmer to access data from RFID chip 6464.

[0476] FIG. 65 shows card 6500, which may be a powered card and may include, for example, board 6502, board 6504, dynamic magnetic communications device 6506, RFID chip 6518, board 6508, battery 6514, conductive leads 6520-6526 and RFID antenna 6516. Additional circuitry may be provided on board 6502, which may include, for example, processor 6530, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6506, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons) .

[0477] All boards, circuitry, and other components of card 6500 may be laminated to form card assembly 6510. Such a lamination may, for example, be implemented using a series of lamination process steps, such that an electronics package containing boards 6502, 6504, and/or 6508 and associated electronics may be encapsulated by an injection molding process (e.g., a reaction injection molding process), whereby a silicon-based material or a polyurethane-based material may be injected and cured (e.g., using temperature and/or chemical reaction) to form the electronics package. The electronics package may then be sandwiched between layers of laminate (e.g., layers of polymer laminate) . Accordingly, for example, both surfaces of card assembly 6510 may be formed by a layer of laminate such that no electrical contacts exist on either surface of card assembly 6510. Alternately, for example, a surface of card assembly 6510 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6510 to provide connectivity from a surface of card assembly 6510 to a processor (e.g., an EMV chip) of card 6500.

[0478] RFID antenna 6516 may, for example, be formed using an additive technique, whereby patterns of a conductive element (e.g., copper) may be applied to a PCB substrate (e.g., applied to either side of board 6508) according to a patterning mask definition layer. RFID antenna 6516 may, for example, be formed using a subtractive technique whereby patterns of a conductive element (e.g., copper) may be removed from a pre-plated PCB substrate (e.g., removed from either side of board 6508) according to an etching mask definition layer. Other non-PCB fabrication techniques may be used to

implement RFID antenna 6516 as may be required by a particular application.

[0479] Conductive leads 6520 and 6522 may, for example, provide electrical conductivity between board 6508 and board 6502. Accordingly, for example, RFID data signals received by RFID antenna 6516 may be communicated to RFID chip 6518 via conductive leads 6520 and 6522. RFID data signals to be communicated by RFID antenna 6516 (e.g., RFID data signals provided to RFID chip 6518 via processor 6530) may, for example, be received from RFID chip 6518 via conductive leads 6520 and 6522. Conductive leads 6524 and 6526 may, for example, provide electrical conductivity between board 6508 and board 6502 so that operational power may be provided to the active electrical components that may exist on board 6502 from battery 6514 . Conductive leads 6520-6526, for example, may use conductive adhesive, soldering paste, or any other type of conductive applications to provide electrical conductivity between boards 6508 and 6502.

[0480] FIG. 66 shows card 6600, which may be a powered card and may include, for example, board 6602, board 6604, dynamic magnetic communications device 6606, RFID chip 6618, board 6608, battery 6614, conductive leads 6620-6626 and RFID antenna 6616. Additional circuitry may be provided on board 6602, which may include, for example, processor 6630, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6606, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons) . All boards, circuitry, and other components of card 6600

may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6610 having no exposed contacts. Alternately, for example, a surface of card assembly 6610 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6610 to provide connectivity from a surface of card assembly 6610 to a processor (e.g., an EMV chip) of card 6600.

[0481] RFID antenna 6616 may, for example, be formed using additive and/or subtractive techniques to define patterns of a conductive element (e.g., copper) to form RFID antenna 6616 (e.g., on either side of board 6604). Conductive leads 6620 and 6622 may, for example, provide electrical conductivity between board 6604 and board 6602. Accordingly, for example, RFID data signals received by RFID antenna 6616 may be communicated to RFID chip 6618 via conductive leads 6620 and 6622. RFID data signals to be communicated by RFID antenna 6616 (e.g., as may be provided to RFID chip 6618 by processor 6630) may be received from RFID chip 6618 via conductive leads 6620 and 6622. Conductive leads 6624 and 6626 may, for example, provide electrical conductivity between board 6608 and board 6602 so that operational power may be provided to the active electrical components that may exist on board 6602 from battery 6614.

[0482] FIG. 67 shows card 6700, which may be a powered card and may include, for example, board 6702, board 6704, dynamic magnetic communications device 6706, RFID chip 6718, board 6708, battery 6714, conductive leads 6722-6726 and RFID antenna 6716. Additional circuitry may be provided on board 6702,

which may include, for example, processor 6730, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6706, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons) . All boards, circuitry, and other components of card 6700 may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6710 having no exposed contacts. Alternately, for example, a surface of card assembly 6710 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6710 to provide connectivity from a surface of card assembly 6710 to a processor (e.g., an EMV chip) of card 6700.

[0483] RFID antenna 6716 may, for example, be formed using additive and/or subtractive techniques to define patterns of a conductive element (e.g., copper) to form RFID antenna 6716 (e.g., on either side of board 6704) . One or more conductive leads 6722 may, for example, provide electrical conductivity between RFID chip 6718 of board 6704 and processor 6730 of board 6702. Accordingly, for example, while data exchanged between RFID chip 6718 and RFID antenna 6716 may remain on board 6704, one or more conduction paths 6722 may be provided so that data that is to be communicated by RFID antenna 6716 may first be communicated to RFID chip 6718 by processor 6730 that may exist, for example, on board 6702. Conductive leads 6724 and 6726 may, for example, provide electrical conductivity between board 6708 and board 6702 so that operational power may be provided to the active electrical

components that may exist on boards 6702 and 6704 from battery 6714.

[0484] FIG. 68 shows card 6800, which may be a powered card and may include, for example, board 6802, board 6804, dynamic magnetic communications device 6806, RFID chip 6818, board 6808, battery 6814, conductive leads 6824-6826 and RFID antenna 6816. Additional circuitry may be provided on board 6802, which may include, for example, processor 6830, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6806, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons). All boards, circuitry, and other components of card 6800 may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6810 having no exposed contacts. Alternately, for example, a surface of card assembly 6810 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6810 to provide connectivity from a surface of card assembly 6810 to a processor (e.g., an EMV chip) of card 6800.

[0485] RFID antenna 6816 may, for example, be formed using additive and/or subtractive techniques to define patterns of a conductive element (e.g., copper) to form RFID antenna 6816 (e.g., on a top side of board 6802). Accordingly, for example, RFID antenna 6816 may be applied to board 6802 at a location proximate to a location of board 6804. In so doing, for example, RFID antenna 6816 may be applied to board 6802 below a location where board 6804 attaches to board 6802 and

conduction paths may be extended to RFID chip 6818 from RFID antenna 6816 (e.g., via conductive traces on board 6802) . Conductive leads 6824 and 6826 may, for example, provide electrical conductivity between board 6808 and board 6802 so that operational power may be provided to the active electrical components that may exist on board 6802 from battery 6814 . Persons skilled in the art will appreciate that RFID antenna 6816 may be placed anywhere on any board (e.g., around a perimeter of board 6802) so as to maximize an effectiveness of RFID antenna 6816.

[0486] Persons skilled in the art will further appreciate that any combination of processors, EMV chips, display drivers, dynamic magnetic stripe communications device drivers, RFID chips, and associated circuitry may be combined into one or more application specific integrated circuits (ASIC) . Accordingly, for example, a core processor may interoperate with an ASIC that combines the functionalities of an RFID chip, a dynamic magnetic stripe communications device driver, and a display driver. Alternately, for example, a core processor, RFID chip, a dynamic magnetic stripe communications device driver, a display driver and associated electronics may be consolidated into a single ASIC. As per another example, a core processor and an RFID chip may be provided as discrete components that may interoperate with an ASIC that may be dedicated to dynamic magnetic stripe communications device driver functions and another ASIC that may be dedicated to display driver functions .

[0487] FIG. 69 shows card 6900, which may include multiple RFID antennas (e.g., RFID antennas 6902-6904)

and associated RFID chips (e.g., RFID chips 6906-6908). Additional circuitry may be provided on card 6900, which may include, for example, a processor, an EMV chip, a display, a display driver, driver circuitry for a dynamic magnetic stripe communications device, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons) . All boards, circuitry, and other components of card 6900 may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6912 having no exposed contacts. Alternately, for example, a surface of card assembly 6912 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6912 to provide connectivity from a surface of card assembly 6912 to a processor (e.g., an EMV chip) of card 6900.

[0488] Processor 6910 may, for example, provide data to RFID chips 6906 and/or 6908 that may be communicated by RFID antenna 6902 and/or RFID antenna 6904, respectively. Processor 6910 may, for example, receive data from RFID chips 6906 and/or 6908 that may be received by RFID antenna 6902 and/or RFID antenna 6904, respectively.

[0489] Card 6900 may, for example, be placed within a communication distance of one or more RFID devices (e.g., one or more RFID enabled merchant terminals) in order to conduct a purchase transaction. Accordingly, for example, processor 6910 may communicate track 1 and track 2 magnetic stripe data to the RFID enabled merchant terminal via RFID chip 6906 and associated RFID antenna 6902. Alternately, for example, processor

6910 may communicate track 1 and track 2 magnetic stripe data to the RFID enabled merchant terminal via RFID chip 6908 and associated RFID antenna 6904.

[0490] As per another example, processor 6910 may utilize both RFID antennas 6902 and 6904 and associated RFID chips 6906 and 6908, respectively, to increase communication efficiency. Accordingly, for example, processor 6910 may communicate track 1 magnetic stripe data to RFID chip 6906 and track 2 magnetic stripe data to RFID chip 6908, so that track 1 magnetic stripe data may be communicated to an RFID enabled merchant terminal via RFID antenna 6902 and track 2 magnetic stripe data may be communicated to an RFID enabled merchant terminal via RFID antenna 6904. In so doing, for example, two tracks of magnetic stripe data may be communicated in half the time.

[0491] As per yet another example, RFID data communicated to RFID chips 6906 and 6908 by processor 6910 may be communicated in a fashion such that multiple channels of information may be communicated in addition to the first and second channels of information communicated by RFID chips 6906 and 6908. For example, phase, frequency, and/or amplitude differences between data communicated by RFID chip 6906/RFID antenna 6902 and data communicated by RFID chip 6908/RFID antenna 6904 may be used to communicate multiple channels of information. Accordingly, for example, a first set of information may be communicated by RFID chip 6906/RFID antenna 6902, a second set of information may be communicated by RFID chip 6908/RFID antenna 6904, and a third set of information may be communicated as an amplitude difference between each data element of the first and second information sets.

A fourth set of information may be communicated, for example, as a phase difference between each data element of the first and second data sets. A fifth set of information may be communicated, for example, as a rate of change of the phase difference (e.g., frequency difference) between each data element of the first and second information sets. Persons skilled in the art will appreciate that any number of channels of information may be communicated by a pair of RFID communicators when differences between RFID data sets communicated by each RFID communicator are exploited as data channels.

[0492] A pair of RFID communicators may, for example, be used to increase accuracy of RFID data communicated. For example, the same RFID data may be communicated by RFID chip 6906/RFID antenna 6902 as is communicated by RFID chip 6908/RFID antenna 6904 so as to increase a probability that an RFID reader may receive RFID data that was intended to be communicated. Accordingly, for example, an RFID reader that may be spatially oriented such that data reception quality from a first RFID communicator is diminished in relation to a data reception quality from a second RFID communicator, may nevertheless receive a complete set of RFID data due to the redundant RFID communication configuration .

[0493] An RFID reader may, for example, employ collision avoidance algorithms, so that communications received from a first RFID communicator do not trump communications received from a second RFID communicator. Accordingly, for example, processor 6910 of card 6900 may communicate to such an RFID reader that dual RFID communicators may be present within card

6900. In so doing, for example, the RFID reader may activate its collision avoidance algorithm to accept RFID communications from both RFID communicators (e.g., RFID chip 6906/RFID antenna 6902 and RFID chip 6908/RFID antenna 6904) simultaneously.

[0494] RFID data may, for example, be received by RFID chip 6906/RFID antenna 6902 and RFID chip 6908/RFID antenna 6904. Accordingly, for example, card 6900 may be an RFID reader that may utilize a pair of RFID readers (e.g., a first RFID reader is provided by RFID chip 6906/RFID antenna 6902 and a second RFID reader is provided by RFID chip 6908/RFID antenna 6904). In so doing, for example, processor 6910 may impose an RFID communication protocol that accepts RFID data form each RFID reader simultaneously.

[0495] FIG. 70 shows card 7000 that may include, for example, configuration 7002. Configuration 7002 may include, for example, button 7004, button 7008, display 7006 and display 7010. Button 7004 may be associated with display 7006. Button 7004 may be pressed to utilize the option described by display 7006. Button 7008 may be associated with display 7010. Button 7008 may be pressed to utilize the option described by display 7010. A card may include additional buttons or displays or may not include the number of buttons or displays of card 7000. For example, a card may include only a single button (e.g., button 7004).

[0496] A user of card 7000 may, for example, select options 7006 or 7010 when card 7000 is to be used (e.g., when card 7000 is to be utilized at a point-of-sale terminal to complete a purchase transaction). Accordingly, for example, a user of card 7000 may press button 7004 to select option 7006 if the user wishes to

exchange RFID data between card 7000 and an RFID device. Alternately, for example, a user of card 7000 may press button 7008 to select option 7010 if the user wishes to communication information to a magnetic stripe reader.

[0497] A user may, for example, press button 7008 to prepare card 7000 for communications with a magnetic stripe reader. Accordingly, for example, a processor of card 7000 may initiate a mode of operation upon activation of option 7010, whereby the processor searches for the presence of a read-head housing of a magnetic stripe reader. Once option 7010 is activated, a user may bring card 7000 within a communication distance of a magnetic stripe reader (e.g., the user may swipe card 7000 through a magnetic stripe reader). Upon the detection of the read-head housing of the magnetic stripe reader, the processor may communicate one, two, and/or three tracks of magnetic stripe data to a read-head of the detected magnetic stripe reader via dynamic magnetic stripe communications device 7014.

[0498] Alternately, for example, a user may press button 7004 to prepare card 7000 for communication with an RFID device. Accordingly, for example, a processor of card 7000 may initiate a mode of operation upon activation of option 7006, whereby a processor of card 7000 provides magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to an RFID chip of card 7000. Once option 7006 is activated, a user may bring card 7000 within a communication distance of an RFID reader (e.g., the user may wave card 7000 within an RFID communication distance of an RFID reader) and an RFID communication sequence between card 7000 and an RFID reader may be completed where

RFID data may be provided to RFID antenna 7012 from an RFID chip on card 7000 and communicated from RFID antenna 7012 to the RFID reader.

[0499] Upon activation of option 7006, a processor of card 7000 may activate passive RFID communications or active RFID communications using RFID antenna 7012 and an associated RFID chip. Passive RFID communications, for example, may require little or no energy to be expended by card 7000. Instead, RFID antenna 7012 may collect energy from an RFID reader when a user of card 7000 brings card 7000 within a communication distance of the RFID reader. The energy collected by RFID antenna 7012 may, for example, provide power to an RFID chip of card 7000. In so doing, for example, an RFID chip of card 7000 may communicate with a processor of card 7000, so that the processor may populate a memory of the RFID chip with information (e.g., payment information) that may be needed to complete a transaction (e.g., a purchase transaction) . Once populated with information, the RFID chip of card 7000 may communicate the information to RFID antenna 7012, which may then communicate the information to the RFID reader.

[0500] Active RFID communications from card 7000 may, for example, utilize battery power from within card 7000. Accordingly, for example, once card 7000 is brought within a communication distance of an RFID reader, RFID antenna 7012 may detect the RFID reader and may wake an RFID chip from a low-power state. In so doing, for example, an RFID antenna 7012 may detect energy from an RFID reader and an RFID chip of card 7000 may utilize battery power of card 7000 to receive information from a processor of card 7000 and to

provide the received information to RFID antenna 7012 for subsequent communication to an RFID reader.

[0501] Card 7000 may, for example, operate as an RFID reader, such that when brought within a communication distance of another RFID device, an RFID chip of card 7000 may interrogate the RFID device to determine whether the RFID device is to receive information from card 7000 (e.g., the RFID device is operating as an RFID reader) or whether the RFID device is to communicate information to card 7000 (e.g., the RFID device is operating as an RFID tag) . Accordingly, for example, an RFID chip of card 7000 may interrogate the RFID device to determine that the RFID device is an RFID tag an that RFID data may be communicated from the RFID device to an RFID chip of card 7000. In so doing, for example, an RFID chip of card 7000 may receive information, such as executable machine code, payment information, or any other type of information that may be required by card 7000 to operate as intended and may forward such information to a processor of card 7000 to be stored within a memory of card 7000. As per one example, an RFID chip of card 7000 may receive personalization information (e.g., cardholder information and cardholder account information) to prepare card 7000 for use as a payment card.

[0502] FIG. 71 shows system 7100, which may include card 7102 and one or more RFID devices (e.g., mobile devices 7104 and 7106) . Card 7102 may, for example, communicate with multiple RFID devices simultaneously. A user of card 7102 may, for example, enable RFID communications with card 7102 by pressing one of buttons 7112 or 7114. Accordingly, for example, payment information (e.g., payment account number and

cardholder name) may be communicated from a core processor within card 7102 and stored within one or more RFID chips of card 7102. Data indicative of which button was pushed (e.g., discretionary data indicative of either credit button 7112 or debit button 7114) may also be communicated and stored within the one or more RFID chips of card 7102.

[0503] As per one example, card 7102 may provide two RFID communication devices that may detect an RF carrier field that may be generated by each of mobile devices 7104 and 7106. Users of mobile devices 7104 and 7106 may, for example, be husband and wife who may wish to store payment information associated with card 7102 on respective memory locations of mobile devices 7104 and 7104 so that such payment information may be used to complete purchase transactions using mobile devices 7104 and 7106.

[0504] A first RFID communication device of card 7102 may establish RFID communication channel 7110 with an RFID reader of mobile device 7104 and a second RFID communication device of card 7102 may establish communication channel 7108 with an RFID reader of mobile device 7106. Accordingly, for example, the first and second RFID communication devices of card 7102 may communicate payment information temporarily stored within an RFID chip of each respective RFID communication device of card 7102. In so doing, for example, mobile devices 7104 and 7106 may store payment information communicated via RFID communication channels 7110 and 7108, respectively, within respective memory locations of mobile devices 7104 and 7106. Mobile devices 7104 and 7106 may later recall such payment information from their respective memory

locations, communicate the stored payment information via channels 7116 and 7118, respectively, of payment network 7120, and complete payment transactions with network entity 7122 using payment information received from card 7102.

[0505] FIG. 72 shows system 7200, which may include mobile device 7202, a stationary device (e.g., desktop computer 7204), payment network 7206, and network entity 7208. An application (e.g., RFID operations GUI 7212) may be executed by a processor of mobile device 7202 and may, for example, report a detection of an RFID device to a display of mobile device 7202. Such an RF device may, for example, include any device (e.g., desktop computer 7204) that may be RFID equipped. An RFID antenna and associated RFID chip may, for example, exist within desktop computer 7204 such that when mobile device 7202 is brought within an RFID communication distance of desktop computer 7204, an RFID antenna of mobile device 7202 may detect its presence, report the same to an RFID chip within mobile device 7202, which may then be reported to a processor of mobile device 7202 and reported to a user of mobile device 7202 via GUI 7212.

[0506] GUI 7212 may, for example, ask the user of mobile device 7202 whether he or she wishes to allow an RFID connection between mobile device 7202 and desktop computer 7204. The user may indicate his or her wish via radio buttons 7214 and may also indicate whether information (e.g., payment information) stored within a memory of mobile device 7202 is to be communicated to desktop computer 7204 via an RFID communication channel previously authorized by the user of mobile device 7202 (e.g., by selecting one of radio buttons 7216). If so,

then such information may be communicated to desktop computer 7204 by mobile device 7202 and stored within a memory of desktop computer 7204. In so doing, for example, payment information communicated by mobile device 7202 to desktop computer 7204 may subsequently be communicated by desktop computer 7204 via communication channel 7210 of payment network 7206 to complete a purchase transaction (e.g., an online purchase of items contained within a shopping cart generated by an internet browser of desktop computer 7204) via network entity 7208.

[0507] A flow diagram of communication sequences is shown in FIG. 73. Step 7311 of sequence 7310 may, for example, include activating an RFID search within a card. Accordingly, for example, a user interface (e.g., one or more buttons) of a card may be associated with a communication feature on the card, whereby pressing one of the buttons may activate an RFID communication device on the card. In step 7312, an RFID device may be detected by the card and an RFID connection may be established between the card and the RFID device. RFID data may, for example, be transferred to an RFID chip on the card (e.g., as in step 7313) and the RFID data contained within an RFID chip on the card may, for example, be communicated via an RFID antenna on the card to the RFID device (e.g., as in step 7314) . Once RFID data is communicated, RFID data contained within an RFID chip on the card may be erased so as to reduce a likelihood of skimming RFID data from the RFID chip on the card.

[0508] Step 7321 of sequence 7320 may, for example, include activating an RFID search within a mobile device. Accordingly, for example, a user interface

(e.g., a GUI executing on a processor of the mobile device) may be associated with a communication feature on the mobile device, whereby interfacing with the GUI may activate an RFID communication channel between a detected RFID device and the mobile device (e.g., as in step 7322) . In step 7323, RFID data may, for example, be transferred to an RFID chip on the mobile device and the RFID data contained within an RFID chip on the mobile device may, for example, be communicated via an RFID antenna on the mobile device to the RFID device (e.g., as in step 7324) . Once RFID data is communicated, RFID data contained within an RFID chip on the mobile device may be erased so as to reduce a likelihood of skimming RFID data from the RFID chip on the mobile device.

[0509] Step 7331 of sequence 7330 may, for example, include transferring RFID data from a core processor to an RFID chip on a card or a mobile device in preparation for communicating the RFID data via an RFID antenna on the card or the mobile device. If a timeout period that may be set in step 7332 expires before the RFID data is communicated by the card or mobile device (e.g., as in step 7333), then RFID data previously transferred to the RFID chip may be erased from the RFID chip by the core processor.

[0510] Step 7341 of sequence 7340 may, for example, include transferring RFID data from a core processor to an RFID chip on a card or a mobile device in preparation for communicating the RFID data via two RFID antennas on the card or the mobile device. In step 7342, the same data may be transferred to both RFID antennas. Alternately, for example, different data may be transferred each RFID antenna. In step

7343, both RFID antennas may communicate data to an RFID reader. As per one example, the same data may be communicated by both RFID antennas so as to increase a reliability of data communication. As per another example, different data may be communicated by each RFID antenna in order to increase an efficiency of data communication. As per yet another example, different data may be communicated by each RFID antenna, where differences (e.g., phase, frequency, and/or amplitude) may be used to communicate multiple other data channels .

[0511] Persons skilled in the art will appreciate that the present invention is not limited to only the embodiments described. Instead, the present invention more generally involves mobile information and the exchange thereof. Persons skilled in the art will also appreciate that the apparatus of the present invention may be implemented in other ways than those described herein. All such modifications are within the scope of the present invention, which is limited only by the claims that follow.

What is claimed is:

1. A method, comprising:

accessing a network using a mobile device;

selecting an object for purchase from said network using said mobile device;

communicating payment information from a payment card to said mobile device using a contactless communication channel; and

communicating said payment information from said mobile device to said network to complete a purchase transaction for said object.

2. A method, comprising:

communicating source account information to a first mobile device using a first contactless communication channel;

communicating target account information to a second mobile device using a second contactless communication channel;

communicating said target account information from said second mobile device to said first mobile device; and

coordinating a money transfer from said source account into said target account using said first mobile device.

3. The method of claim 1, wherein said mobile device is a laptop computer.

4. The method of claim 1, wherein said mobile device is a PDA.

5. The method of claim 1, wherein said mobile device is a phone.

6. The method of claim 1, wherein said contactless communication channel is an RFID communication channel.

7. The method of claim 1, wherein said mobile device and said payment card are brought within a proximity distance of up to two inches to establish said contactless communication channel.

8. The method of claim 1, wherein said payment card is a powered card.

9. The method of claim 1, wherein said payment card is a non-powered card.

10. The method of claim 1, wherein said payment card simulates a series of touches to a display of said mobile device to establish at least a portion of said contactless communication channel.

11. The method of claim 1, wherein said mobile device communicates an optical data stream to said payment card to establish at least a portion of said contactless communication channel.

12. The method of claim 2, wherein a powered card communicates said target account information.

13. The method of claim 2, wherein a non-powered card communicates said target account information.

14. The method of claim 2, wherein a powered card communicates said source account information.

15. The method of claim 2, wherein a non-powered card communicates said source account information.

16. The method of claim 2, wherein said first mobile device is a laptop computer..

17. The method of claim 2, wherein said first mobile device is a PDA.

18. The method of claim 2, wherein said first mobile device is a phone.

19. The method of claim 2, wherein said second mobile device is a laptop computer..

20. The method of claim 2, wherein said second mobile device is a PDA.

21. The method of claim 2, wherein said second mobile device is a phone.

22. A method, comprising:

establishing a contactless communication channel between one or more physical cards and a mobile device;

communicating information from said physical card to said mobile device using said contactless communication channel;

creating a mobile wallet of virtual cards within a memory of said mobile device from said communicated information; and

selecting one of said virtual cards to complete a purchase transaction using said mobile device.

23. The method of claim 22, wherein said mobile device is a laptop.

24. The method of claim 22, wherein said mobile device is a PDA.

25. The method of claim 22, wherein said mobile device is a phone.

26. The method of claim 22, wherein said mobile device is an MP3 device.

27. The method of claim 22, wherein said mobile device is a GPS device.

28. The method of claim 22, wherein said physical card is a non-powered card.

29. The method of claim 22, wherein said physical card is a powered card.

30. The method of claim 22, wherein said contactless communication channel is an RFID communication channel.

31. The method of claim 22, wherein said mobile device and said physical card are brought within a proximity distance of up to two inches to establish said contactless communication channel.

32. The method of claim 22, wherein said physical card simulates a series of touches to a display of said mobile device to establish at least a portion of said contactless communication channel.

33. The method of claim 22, wherein said mobile device communicates an optical data stream to said physical card to establish at least a portion of said contactless communication channel.

34. The method of claim 22, wherein establishing said contactless communication channel comprises entering a PIN associated with said physical card to authorize said communicated information.

35. The method of claim 22, wherein said communicated information is selected based on manual input entered into said physical card.

36. The method of claim 22, wherein said communicated information includes payment information associated with a first payment account selected by pressing a first button of said physical card.

37. The method of claim 22, wherein said virtual cards include gift cards.

38. The method of claim 22, wherein said mobile device includes a graphical user interface to modify a visual appearance of said virtual cards as displayed by said mobile device.

39. The method of claim 22, wherein said communicated information is used to create a visual appearance of said virtual cards as displayed by said mobile device.

40. The method of claim 22, wherein said virtual cards are sorted onto a display of said mobile device based on manual input selection received by a graphical user interface of said mobile device.

41. The method of claim 22, wherein completing said purchase transaction includes establishing a second contactless communication channel between said mobile device and a merchant terminal and communicating payment information associated with said selected virtual card to said merchant terminal via said second contactless communication channel.

42. A method, comprising:

executing an application on a processor of a mobile device to perform a function;

communicating information to said mobile device from a contactless device using a contactless communication channel;

confirming said communicated information matches at least a portion of predetermined information; and

executing said function from said mobile device based on said confirmation.

43. The method of claim 42, wherein said mobile device is a laptop.

44. The method of claim 42, wherein said mobile device is a PDA.

45. The method of claim 42, wherein said mobile device is a phone.

46. The method of claim 42, wherein said mobile device is an MP3 device.

47. The method of claim 42, wherein said mobile device is a GPS device.

48. The method of claim 42, wherein said contactless device is a non-powered card.

49. The method of claim 42, wherein said contactless device is a powered card.

50. The method of claim 42, wherein said contactless device is an automobile key.

51. The method of claim 42, wherein said contactless device is a home door key.

52. The method of claim 42, wherein said contactless device is a key to a safe deposit box.

53. The method of claim 42, wherein said contactless communication channel is an RFID communication channel.

54. The method of claim 42, wherein a camera of said mobile device establishes said contactless communication channel.

55. The method of claim 42, wherein said contactless device is a powered card, said mobile device and said powered card being brought within a proximity distance of up to two inches to establish said contactless communication channel.

56. The method of claim 42, wherein said contactless device is a powered card, said powered card simulating a series of touches to a display of said mobile device to establish at least a portion of said contactless communication channel.

57. The method of claim 42, wherein said contactless device is a powered card, said mobile device communicating an optical data stream to said powered card to establish at least a portion of said contactless communication channel.

58. The method of claim 42, wherein said predetermined information exists on a memory of said mobile device.

59. The method of claim 42, wherein said predetermined information exists on a memory of a remote authorization server.

60. The method of claim 42, wherein said contactless device is a non-powered card, said non-powered card providing said communicated information to authorize a purchase transaction based on payment account information associated with said non-powered card.

61. The method of claim 42, wherein said function is executed by a device external to said mobile device.

62. A card, comprising:

a first board including a first RFID chip and a first RFID antenna; and

a second board including a processor, wherein first data is transferred from said processor to said first RFID chip via conductive terminals between said first and second boards and wherein said first data is communicated from said first RFID chip to a first RFID communication channel via said first RFID antenna.

63. A card, comprising:

a first board including a first RFID antenna; and

a second board including a first RFID chip and a processor, wherein first data is transferred from said processor to said RFID chip and wherein said first data is communicated from said first RFID chip to a first RFID communication channel via said first RFID antenna.

64. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, said first and second data being the same.

65. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel

via said second RFID antenna, said first and second data being different.

66. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a difference between said first and second data forms information for a third RFID communication channel.

67. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a first difference between said first and second data forms information for a third RFID communication channel and a second difference between said first and second data forms information for a fourth RFID communication channel .

68. The card of claim 62, wherein said first data is erased from said first RFID chip after said first data is communicated from said first RFID chip to said first RFID communication channel.

8 . The card of claim 1, wherein said first data is erased from said first RFID chip after a delay period has expired.

69. The card of claim 62, wherein said first and second boards are encapsulated, said encapsulation being laminated between first and second lamination layers .

70. The card of claim 62, further comprising a dynamic magnetic stripe communications device.

71. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, said first and second data being the same .

72. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, said first and second data being different .

73. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a first difference between said first and second data forms information for a third RFID communication channel.

74. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a first difference between said first and second data forms information for a third RFID communication channel and a second difference between said first and second data forms information for a fourth RFID communication channel.

75. The card of claim 63, wherein said first data is erased from said first RFID chip after said first data is communicated from said first RFID chip to said first RFID communication channel.

76. The card of claim 63, wherein said first data is erased from said first RFID chip after a delay period has expired.

77. The card of claim 63, wherein said first and second boards are encapsulated, said encapsulation being laminated between first and second lamination layers .

78. The card of claim 63, further comprising a dynamic magnetic stripe communications device.

79. A method comprising:

communicating first data from a device to a reader via a first RFID communication channel;

communicating second data from said device to said reader via a second RFID communication channel;

receiving said first and second data via said reader; and

avoiding collisions between said first and second data within said reader.

80. The method of claim 79, wherein said first and second data are different.

81. A system, comprising:

means for accessing a network;

means for selecting an object for purchase from said network;

means for communicating payment information from a payment card to a mobile device; and

means for communicating said payment information from said mobile device to a network to complete a purchase transaction for said object.

82. A system, comprising:

means for communicating source account information to a first mobile device;

means for communicating target account information to a second mobile device;

means for communicating said target account information from said second mobile device to said first mobile device; and

means for coordinating a money transfer from said source account into said target account.

83. A system, comprising:

means for establishing a contactless communication channel between one or more physical cards and a mobile device;

means for communicating information from said physical card to said mobile device using said contactless communication channel;

means for creating a mobile wallet of virtual cards within a memory of said mobile device from said communicated information; and

means for selecting one of said virtual cards to complete a purchase transaction using said mobile device.

84. A system, comprising:

means for executing an application on a mobile device to perform a function;

means for communicating information to said mobile device from a contactless device;

means for confirming said communicated information matches at least a portion of predetermined information; and

means for executing said function from said mobile device based on said confirmation.

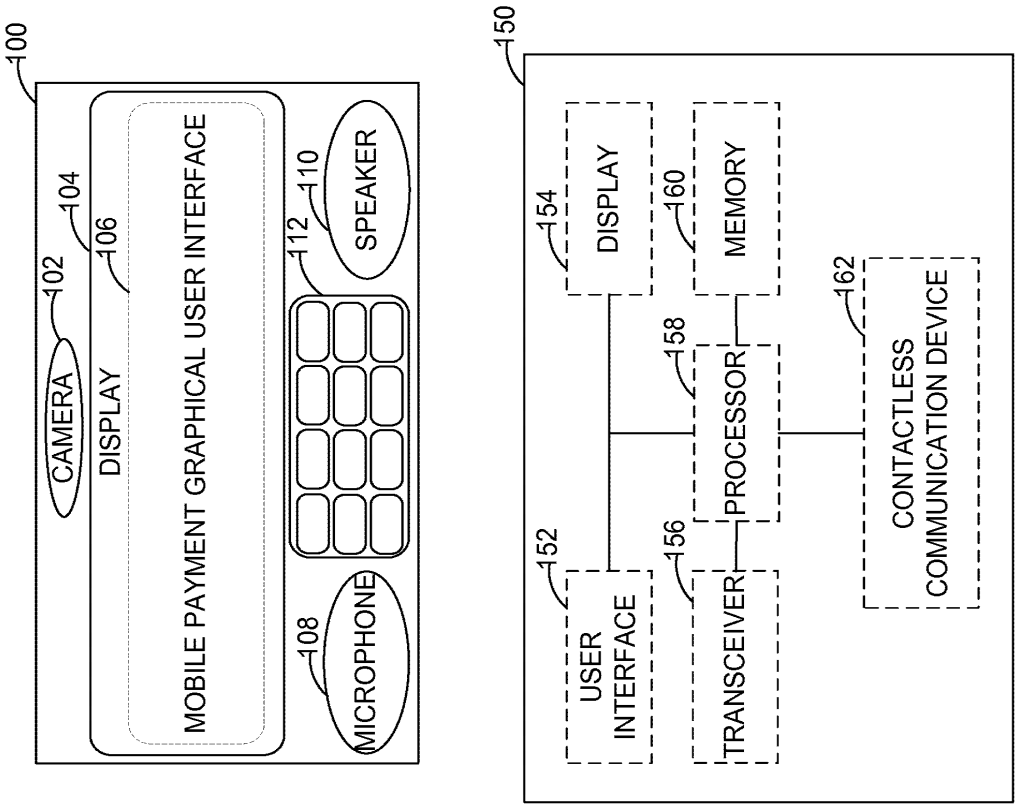

100
CAMERA
102
DISPLAY
104
MOBILE PAYMENT GRAPHICAL USER INTERFACE
106
MICROPHONE
108
SPEAKER
110
112
150
USER INTERFACE
152
DISPLAY
154
TRANSCEIVER
156
PROCESSOR
158
MEMORY
160
CONTACTLESS COMMUNICATION DEVICE
162

FIG. 1

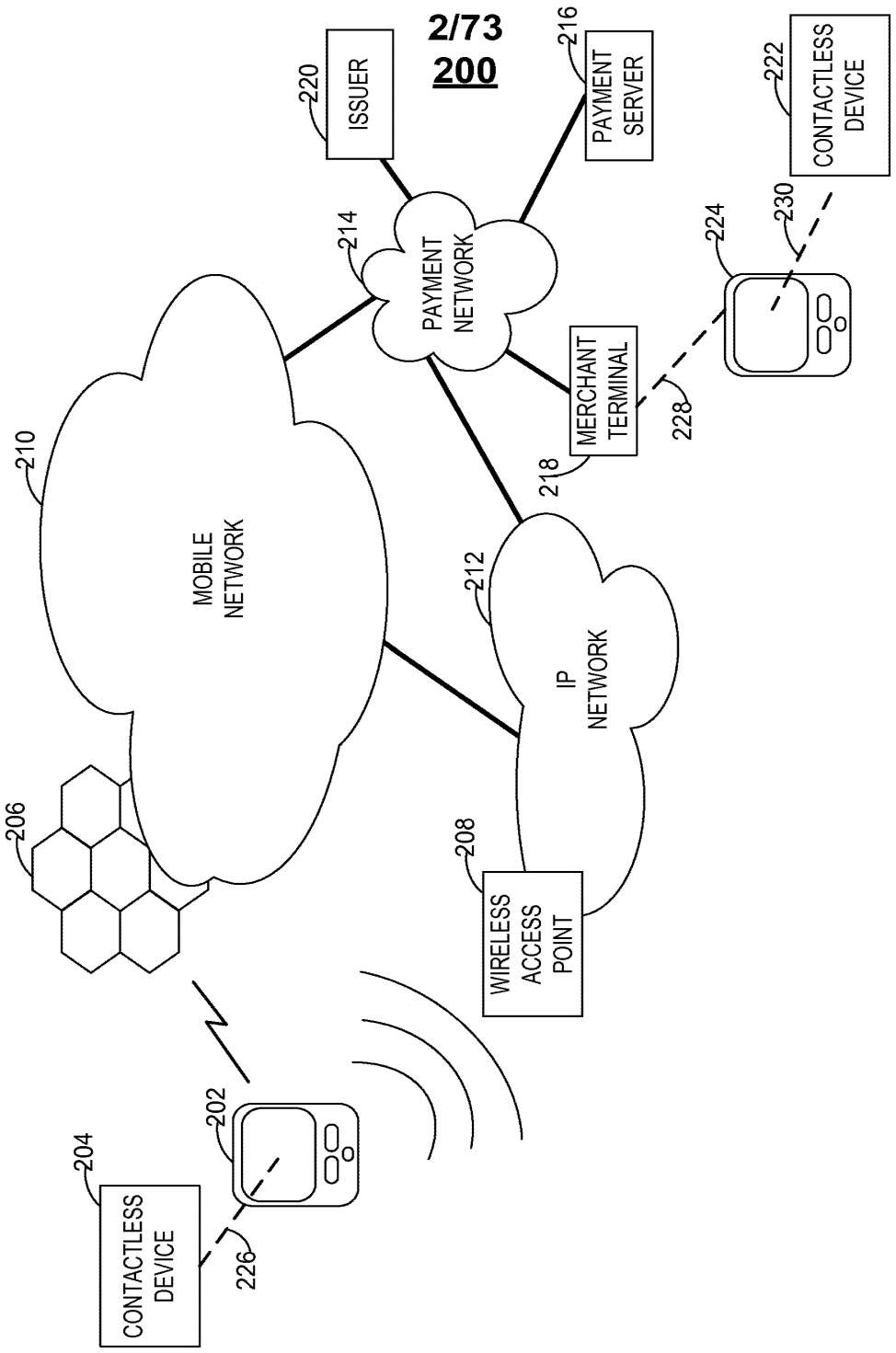

200
ISSUER
220
PAYMENT SERVER
216
CONTACTLESS DEVICE
222
PAYMENT NETWORK
214
MOBILE NETWORK
210
MERCHANT TERMINAL
218
228
224
230
IP NETWORK
212
206
WIRELESS ACCESS POINT
208
202
204
CONTACTLESS DEVICE
226

FIG. 2

300

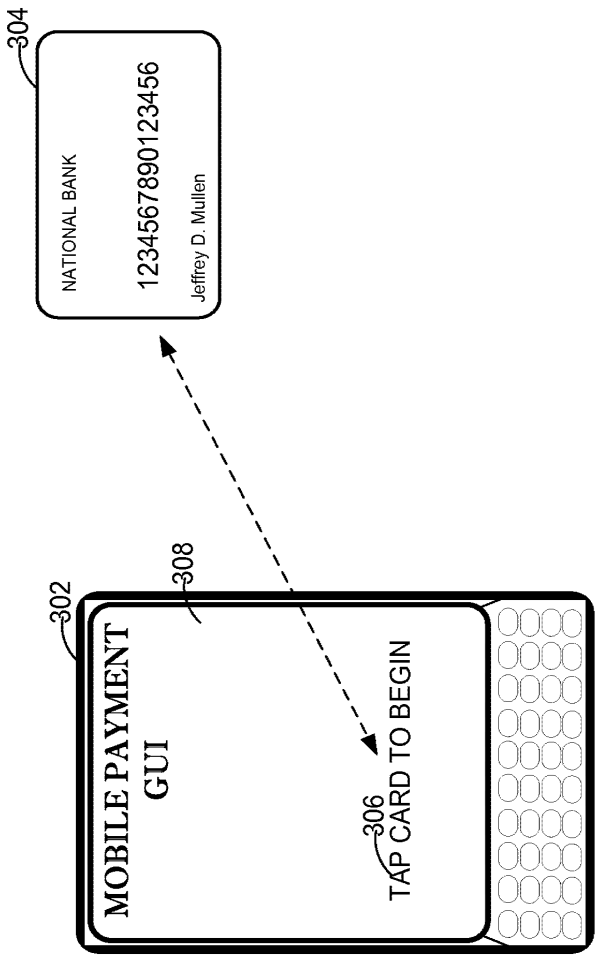

304
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
308
302
MOBILE PAYMENT
GUI
306
TAP CARD TO BEGIN

FIG. 3

400

CARD DETECTION
AIRLINE CARD
TRAVEL CARD
BANK CARD
404
HEALTHCARE CARD
IDENTIFICATION CARD
REWARDS CARD
CONTINUE
408
BACK
406

FIG. 4

500

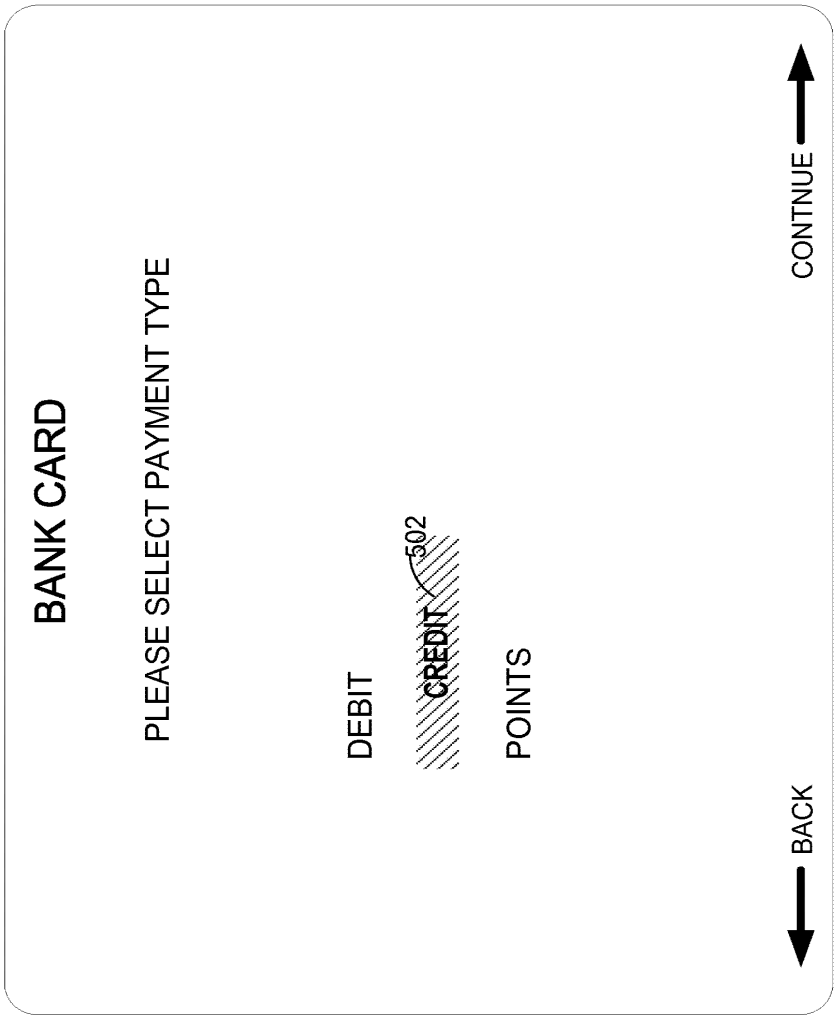

BANK CARD
PLEASE SELECT PAYMENT TYPE
DEBIT
CREDIT
502
POINTS
CONTNUE
BACK

FIG. 5

600

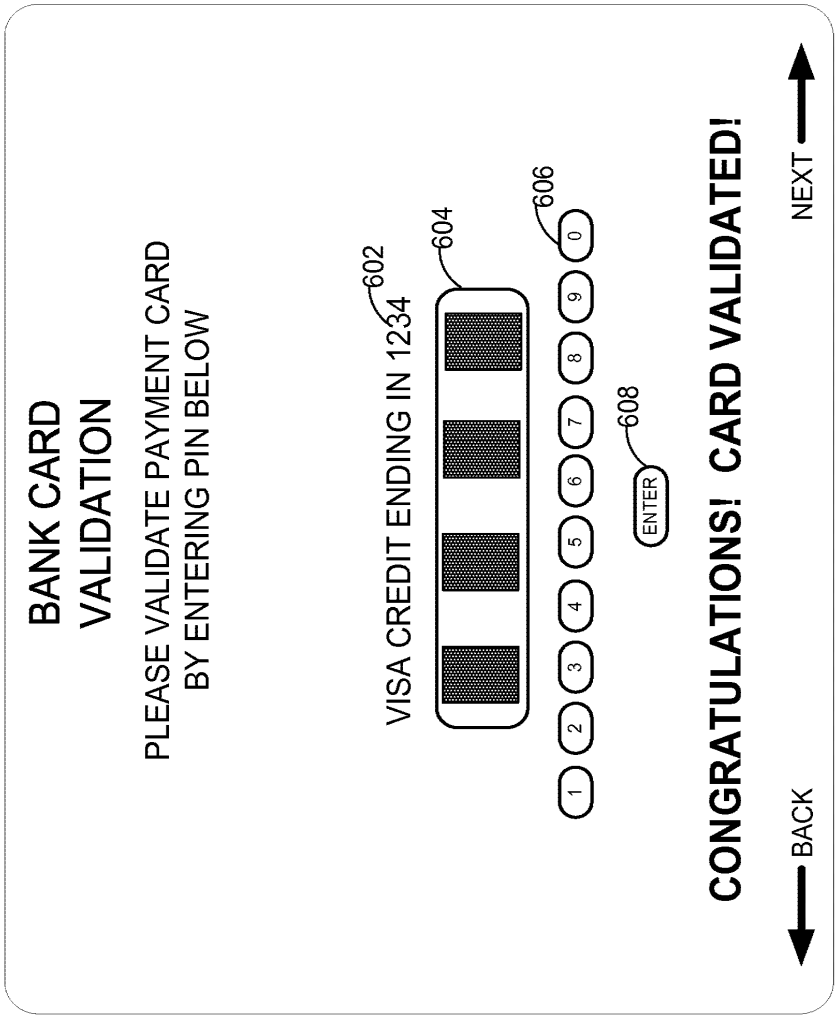

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING PIN BELOW
VISA CREDIT ENDING IN 1234
602
604
606
1
2
3
4
5
6
7
8
9
0
ENTER
608
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 6

700

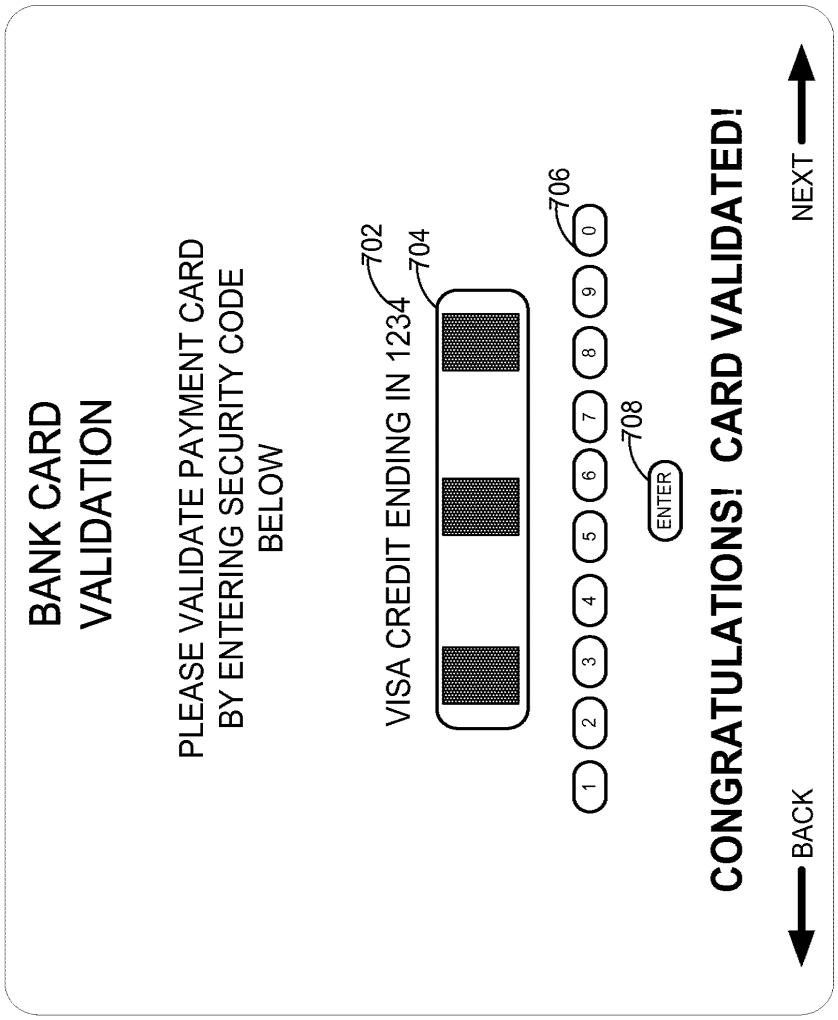

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING SECURITY CODE
BELOW
VISA CREDIT ENDING IN 1234
702
704
706
708
1
2
3
4
5
6
7
8
9
0
ENTER
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 7

800

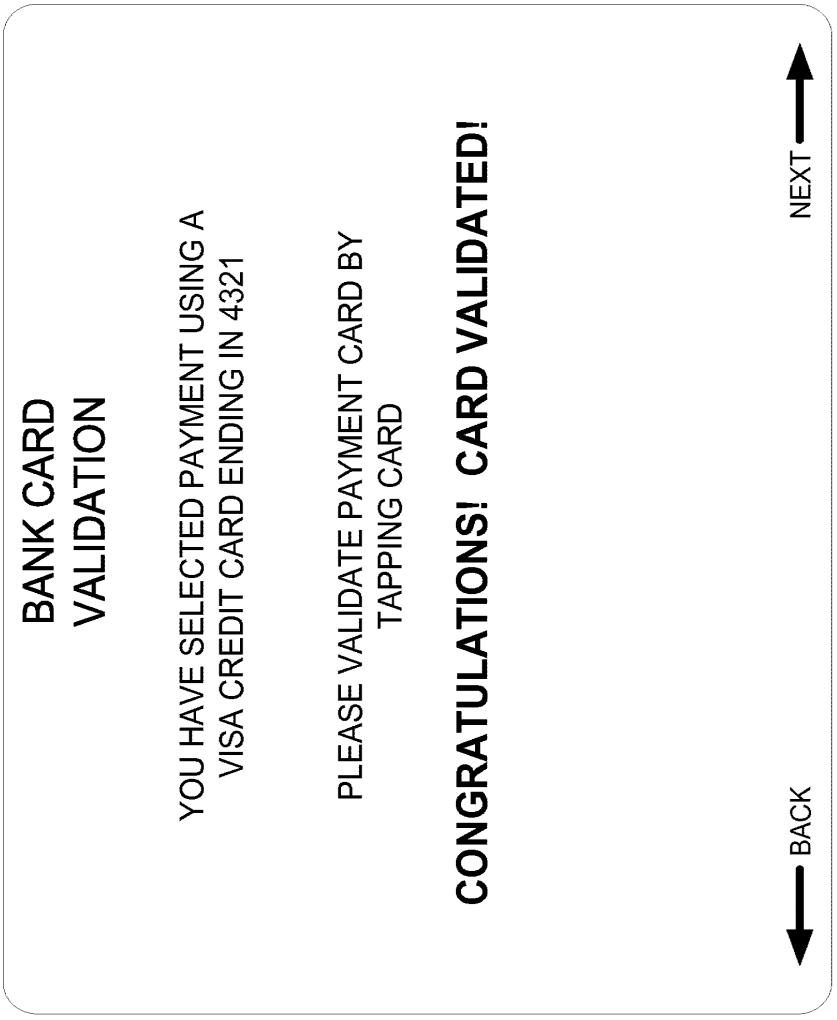

BANK CARD
VALIDATION
YOU HAVE SELECTED PAYMENT USING A
VISA CREDIT CARD ENDING IN 4321
PLEASE VALIDATE PAYMENT CARD BY
TAPPING CARD
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 8

900

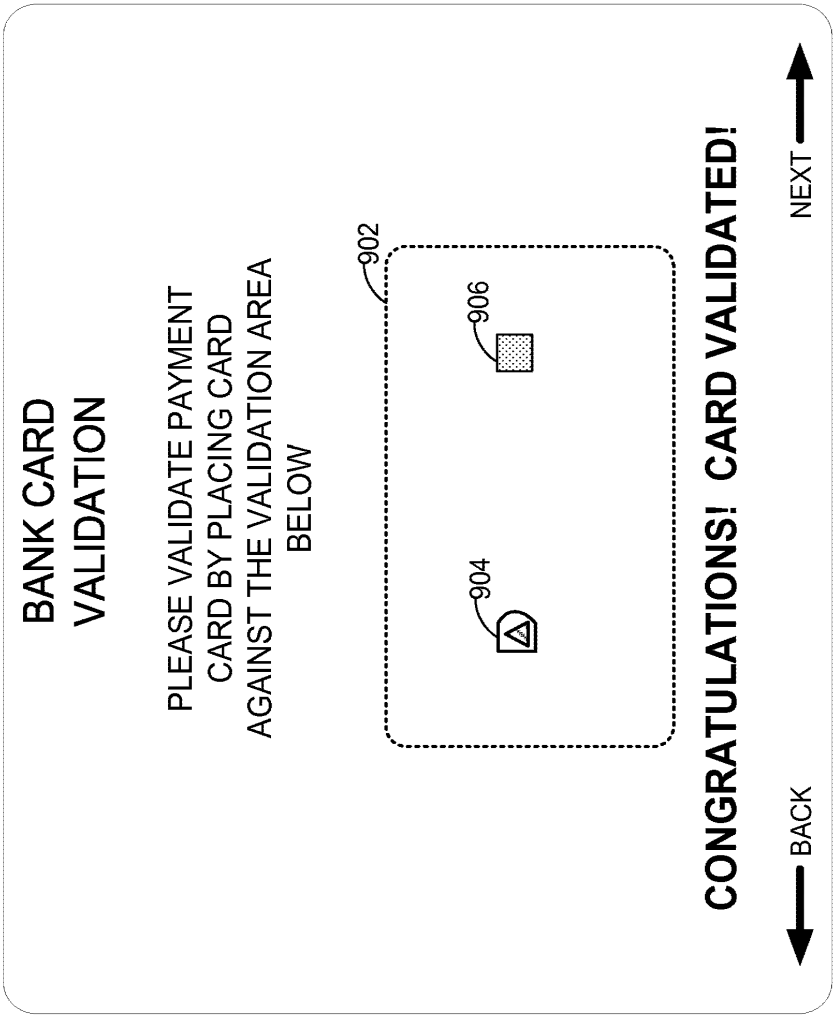

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT
CARD BY PLACING CARD
AGAINST THE VALIDATION AREA
BELOW
902
906
904
CONGRATULATIONS! CARD VALIDATED!
NEXT
BACK

FIG. 9

1000

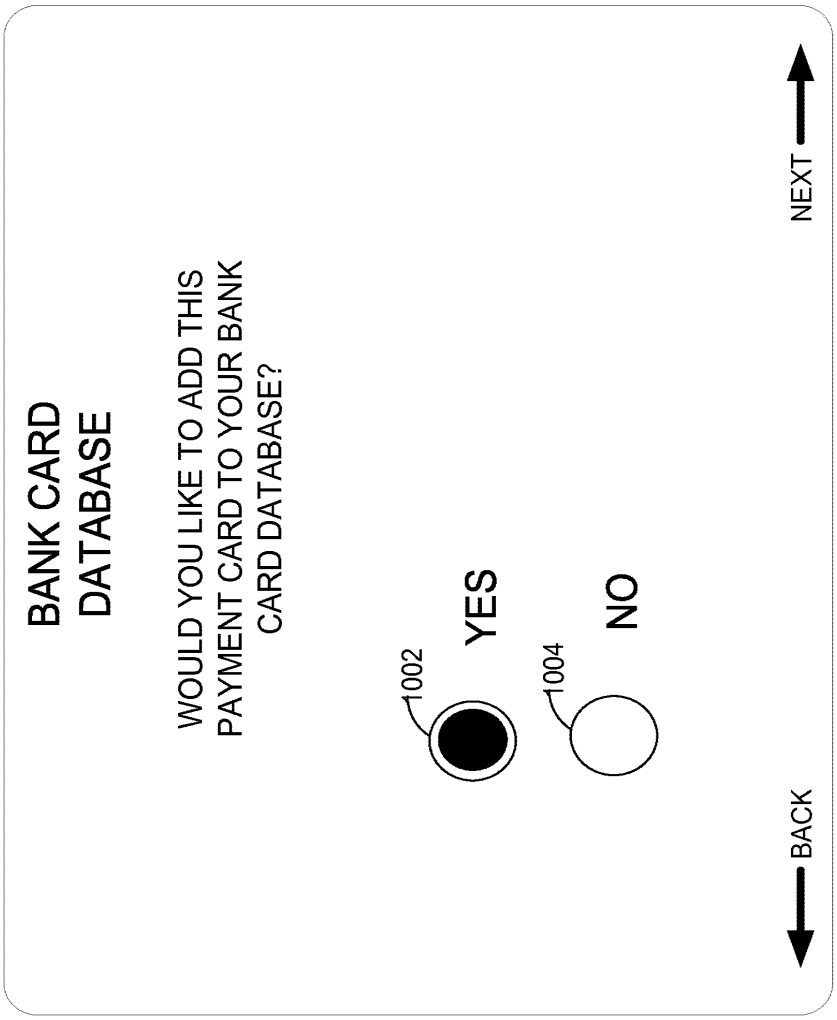

BANK CARD DATABASE
WOULD YOU LIKE TO ADD THIS PAYMENT CARD TO YOUR BANK CARD DATABASE?
YES
NO
1002
1004
NEXT
BACK

FIG. 10

1100

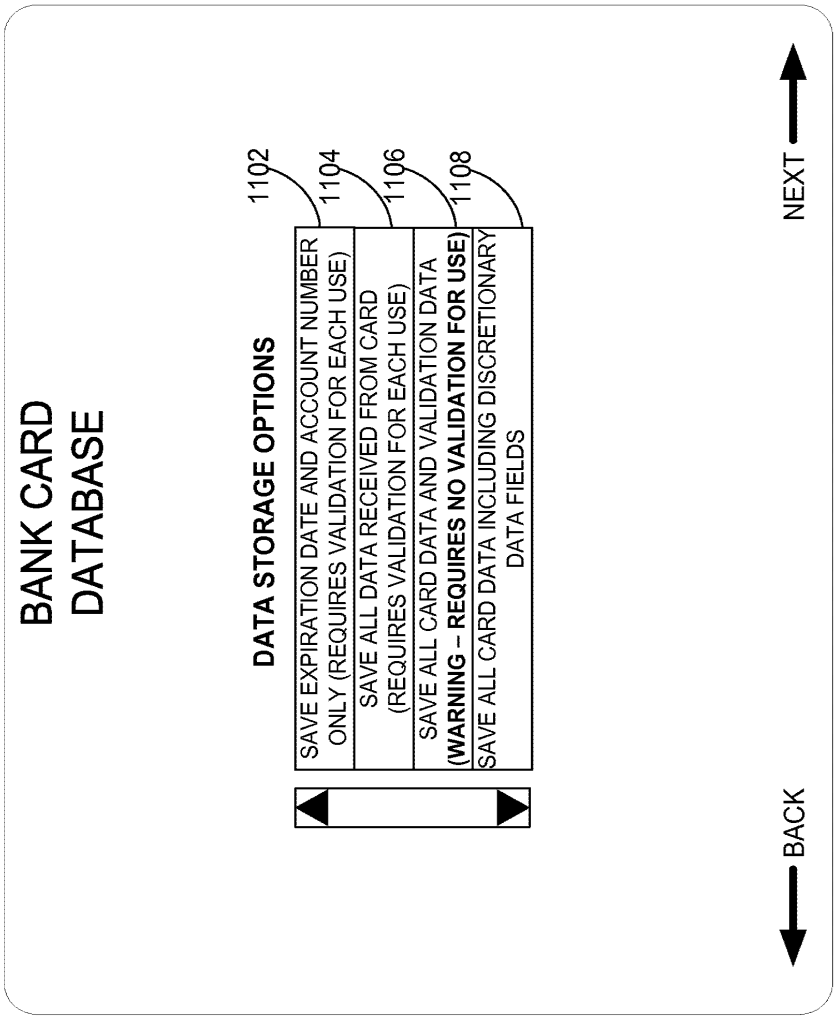

BANK CARD DATABASE
DATA STORAGE OPTIONS
1102
1104
1106
1108
SAVE EXPIRATION DATE AND ACCOUNT NUMBER ONLY (REQUIRES VALIDATION FOR EACH USE)
SAVE ALL DATA RECEIVED FROM CARD (REQUIRES VALIDATION FOR EACH USE)
SAVE ALL CARD DATA AND VALIDATION DATA (WARNING – REQUIRES NO VALIDATION FOR USE)
SAVE ALL CARD DATA INCLUDING DISCRETIONARY DATA FIELDS
NEXT
BACK

FIG. 11

12/73

1200

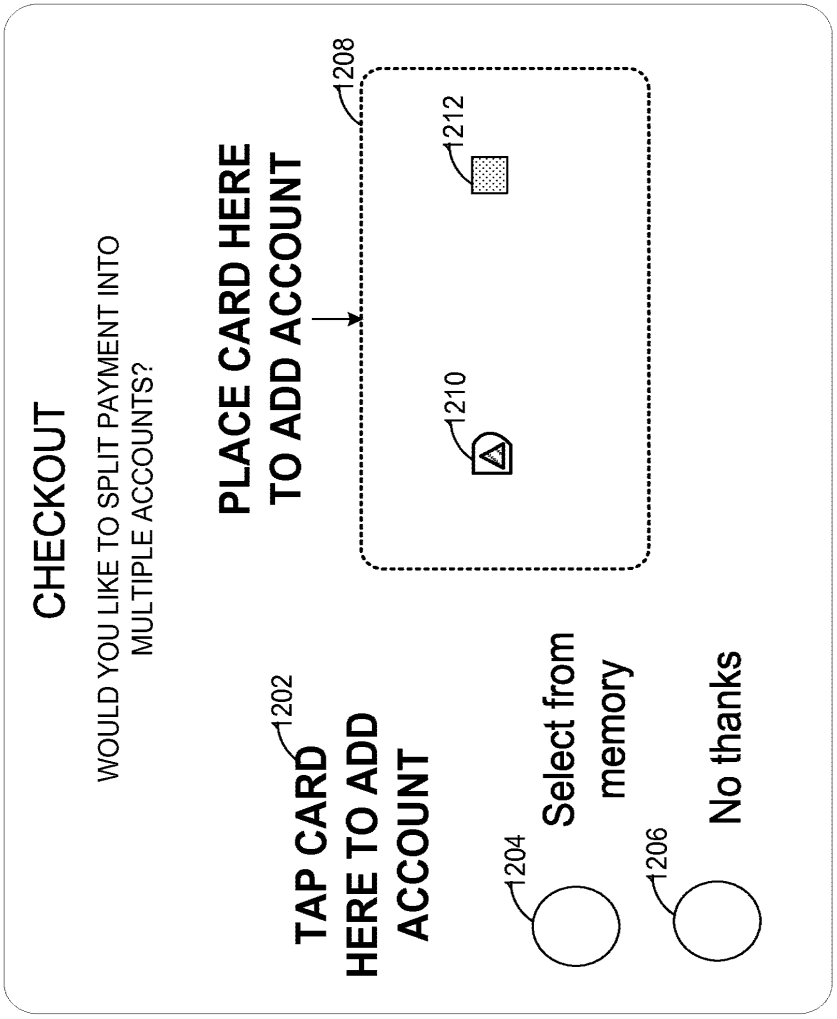


FIG. 12

13/73
1300

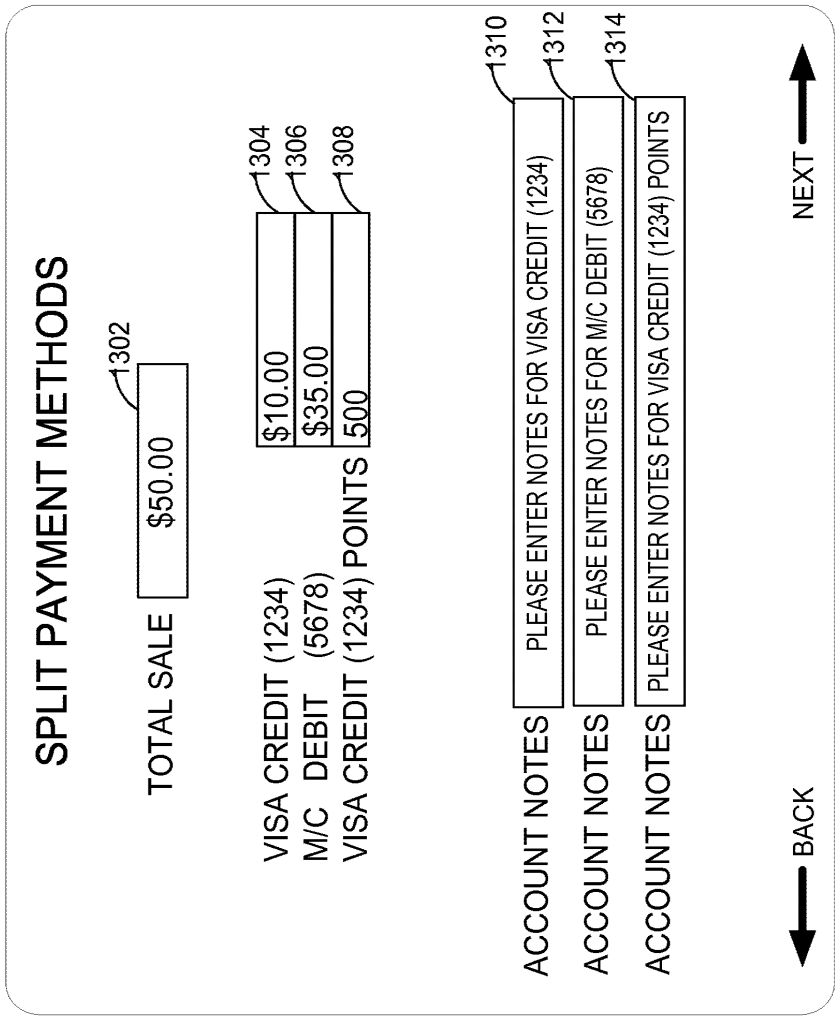


FIG. 13

14/73
1400

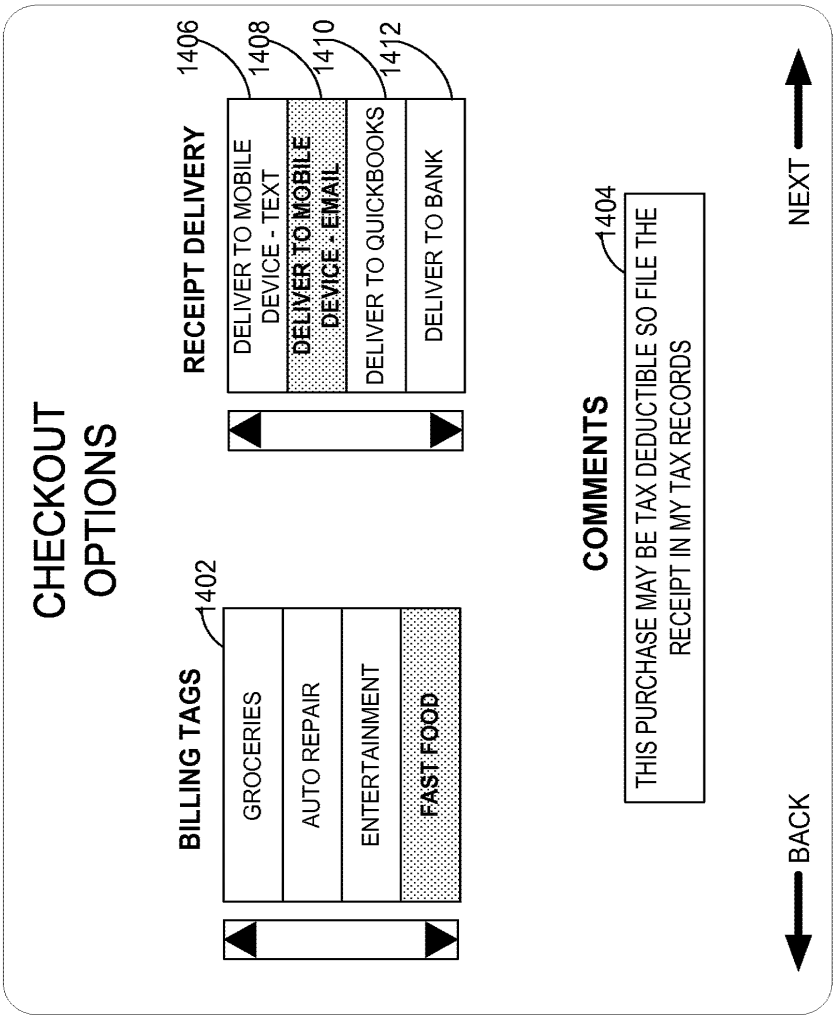


FIG. 14

15/73
1500

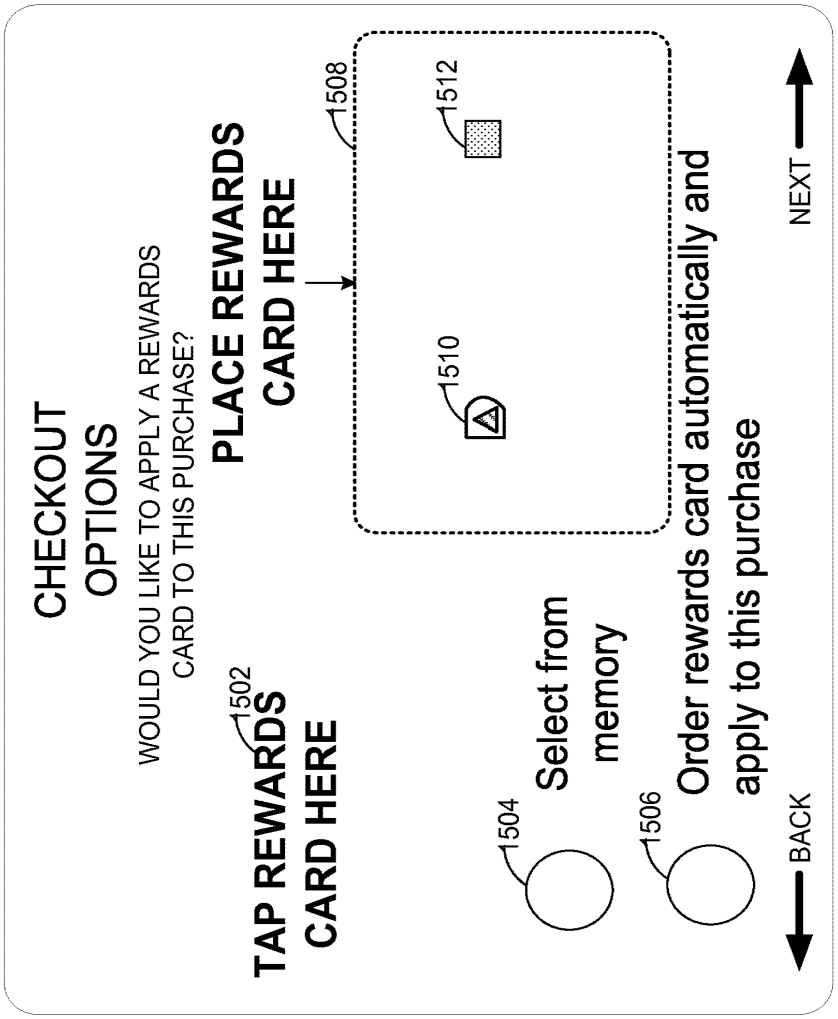


FIG. 15

1600

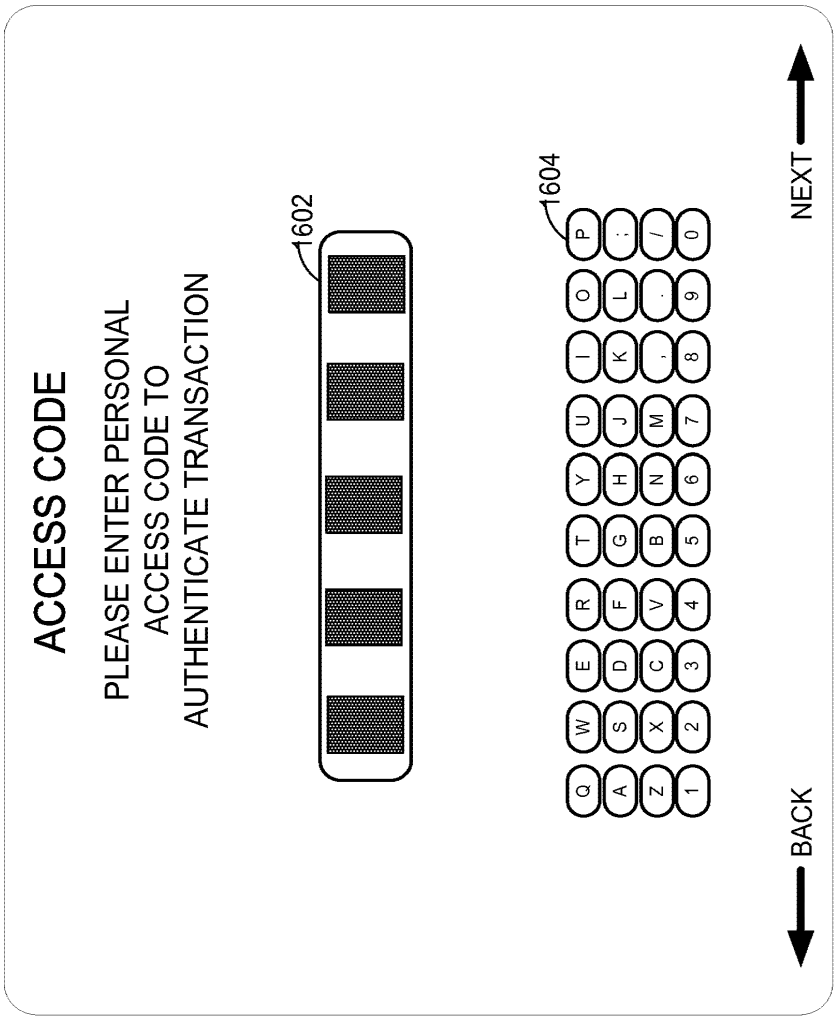

ACCESS CODE
PLEASE ENTER PERSONAL ACCESS CODE TO AUTHENTICATE TRANSACTION
1602
1604
NEXT
BACK

FIG. 16

1700

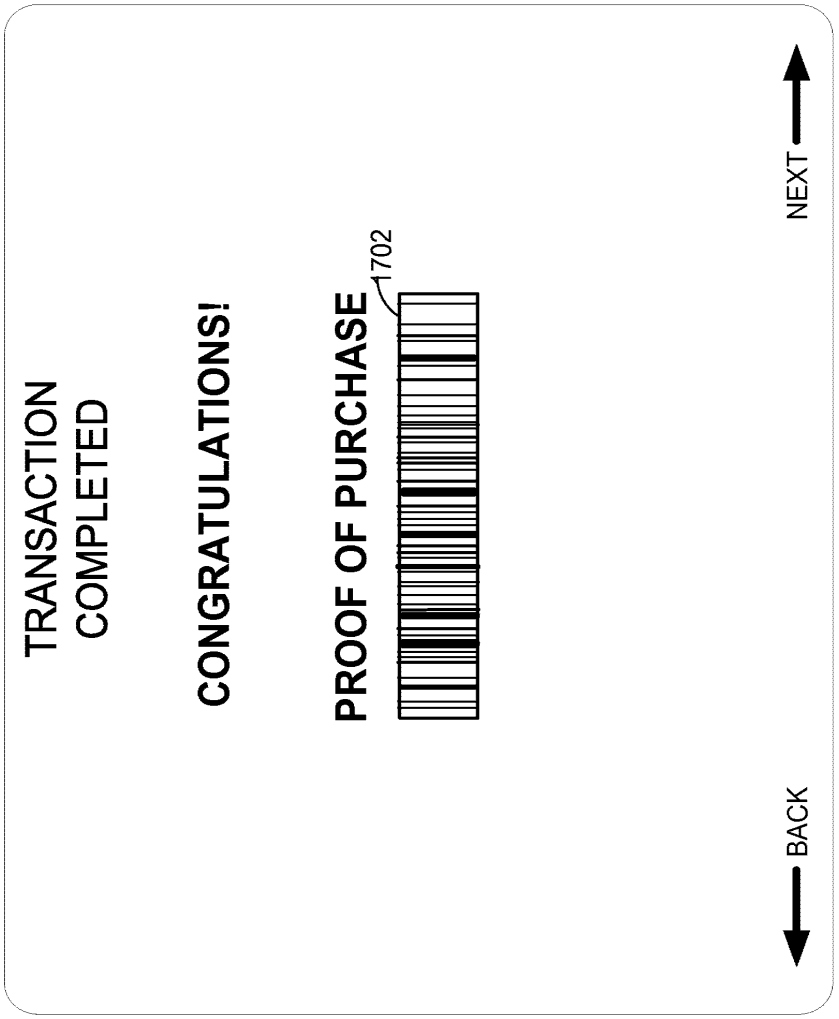

TRANSACTION COMPLETED
CONGRATULATIONS!
PROOF OF PURCHASE
1702
NEXT
BACK

FIG. 17

1800

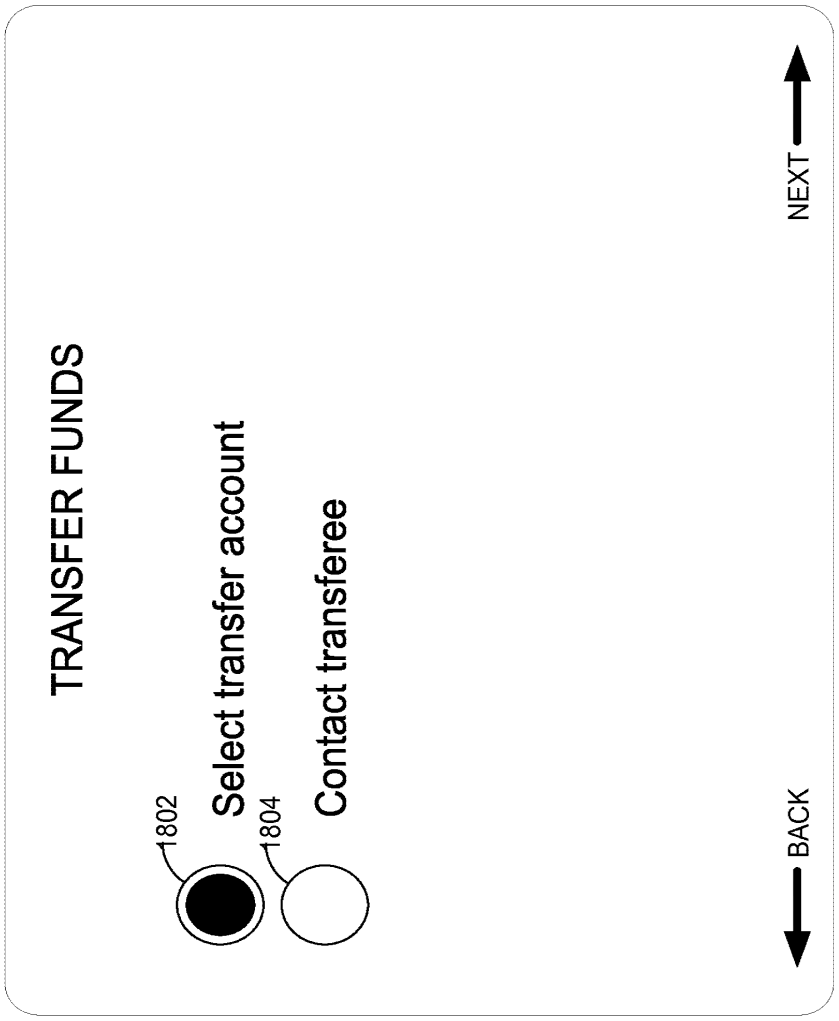

TRANSFER FUNDS
Select transfer account
Contact transferee
1802
1804
NEXT
BACK

FIG. 18

1900

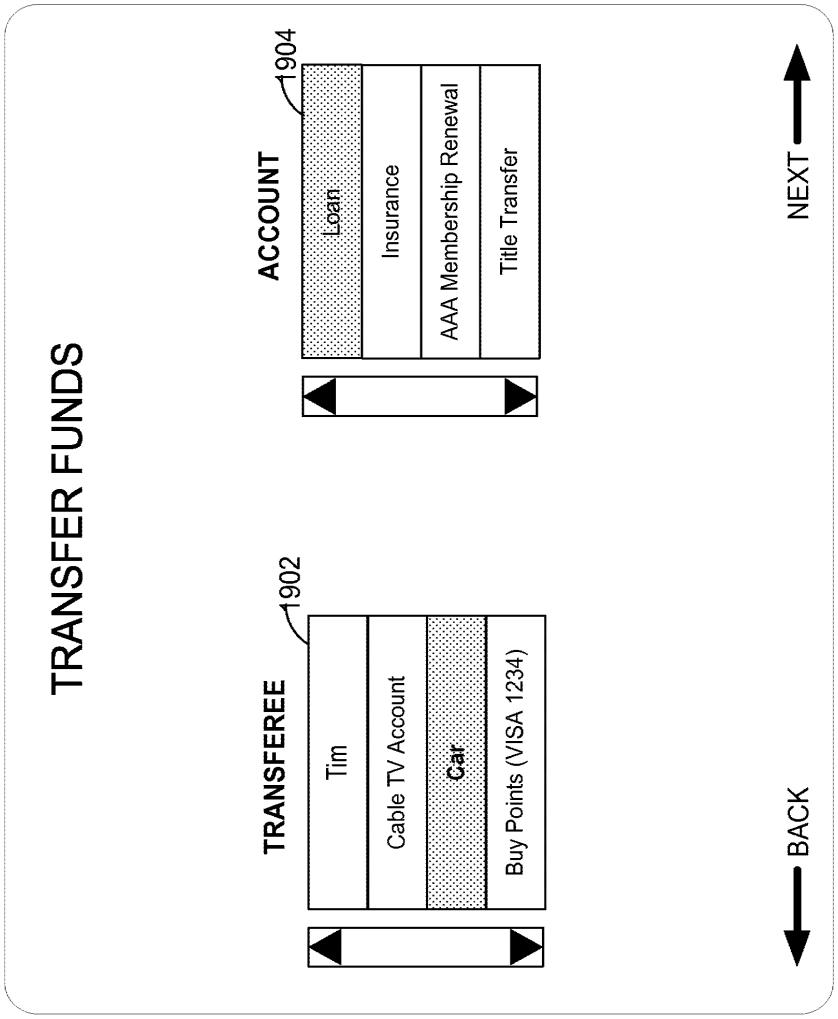

TRANSFER FUNDS
TRANSFEREE
1902
Tim
Cable TV Account
Car
Buy Points (VISA 1234)
ACCOUNT
1904
Loan
Insurance
AAA Membership Renewal
Title Transfer
NEXT
BACK

FIG. 19

2000

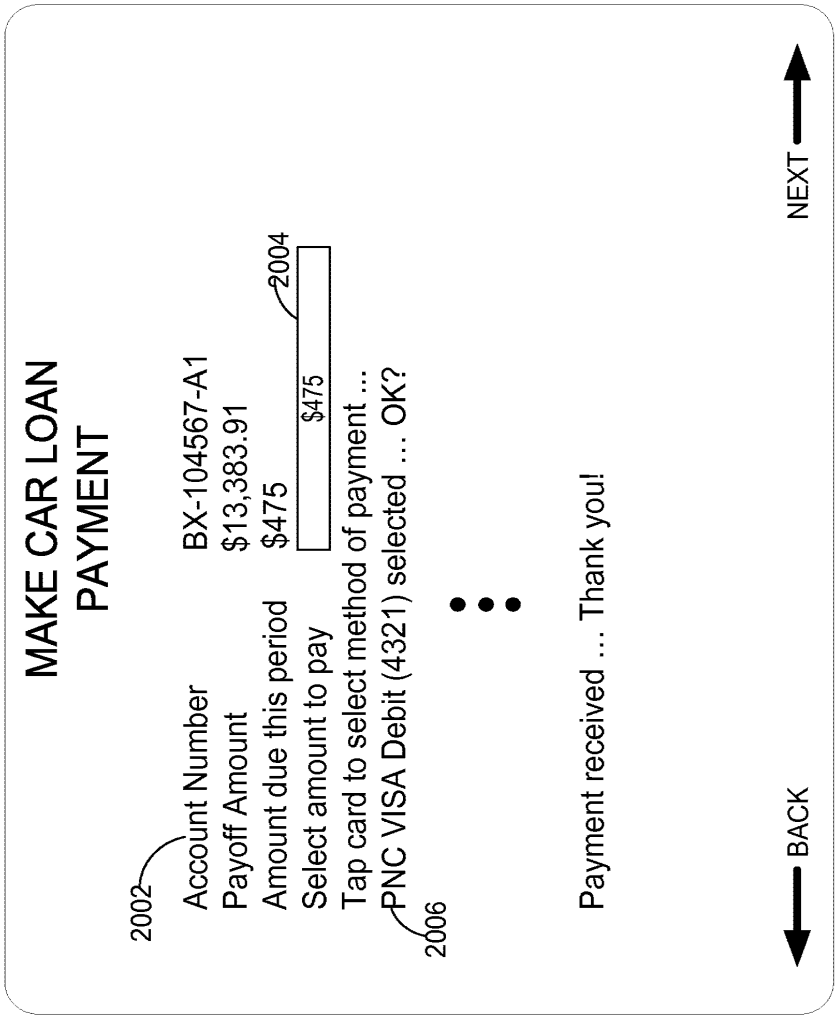

MAKE CAR LOAN PAYMENT
2002
Account Number
BX-104567-A1
Payoff Amount
$13,383.91
Amount due this period
$475
2004
Select amount to pay
$475
Tap card to select method of payment ...
PNC VISA Debit (4321) selected ... OK?
2006
Payment received ... Thank you!
BACK
NEXT

FIG. 20

2100

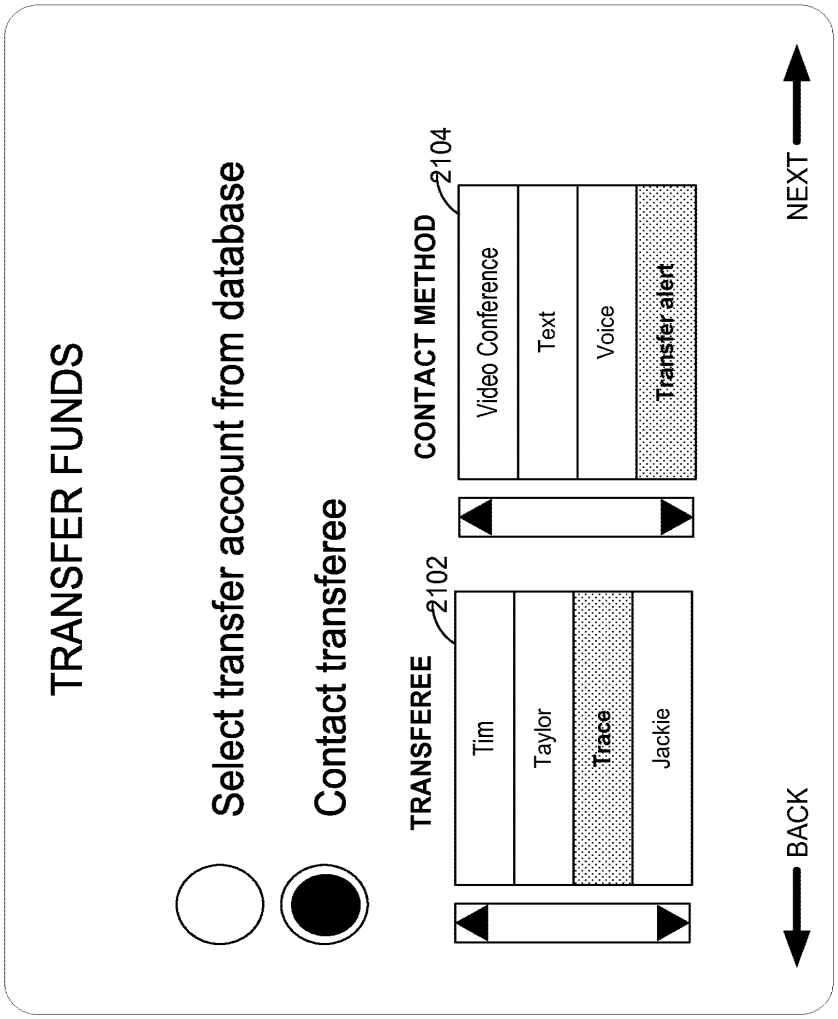

TRANSFER FUNDS
Select transfer account from database
Contact transferee
TRANSFEREE
2102
Tim
Taylor
Trace
Jackie
CONTACT METHOD
2104
Video Conference
Text
Voice
Transfer alert
BACK
NEXT

FIG. 21

2200

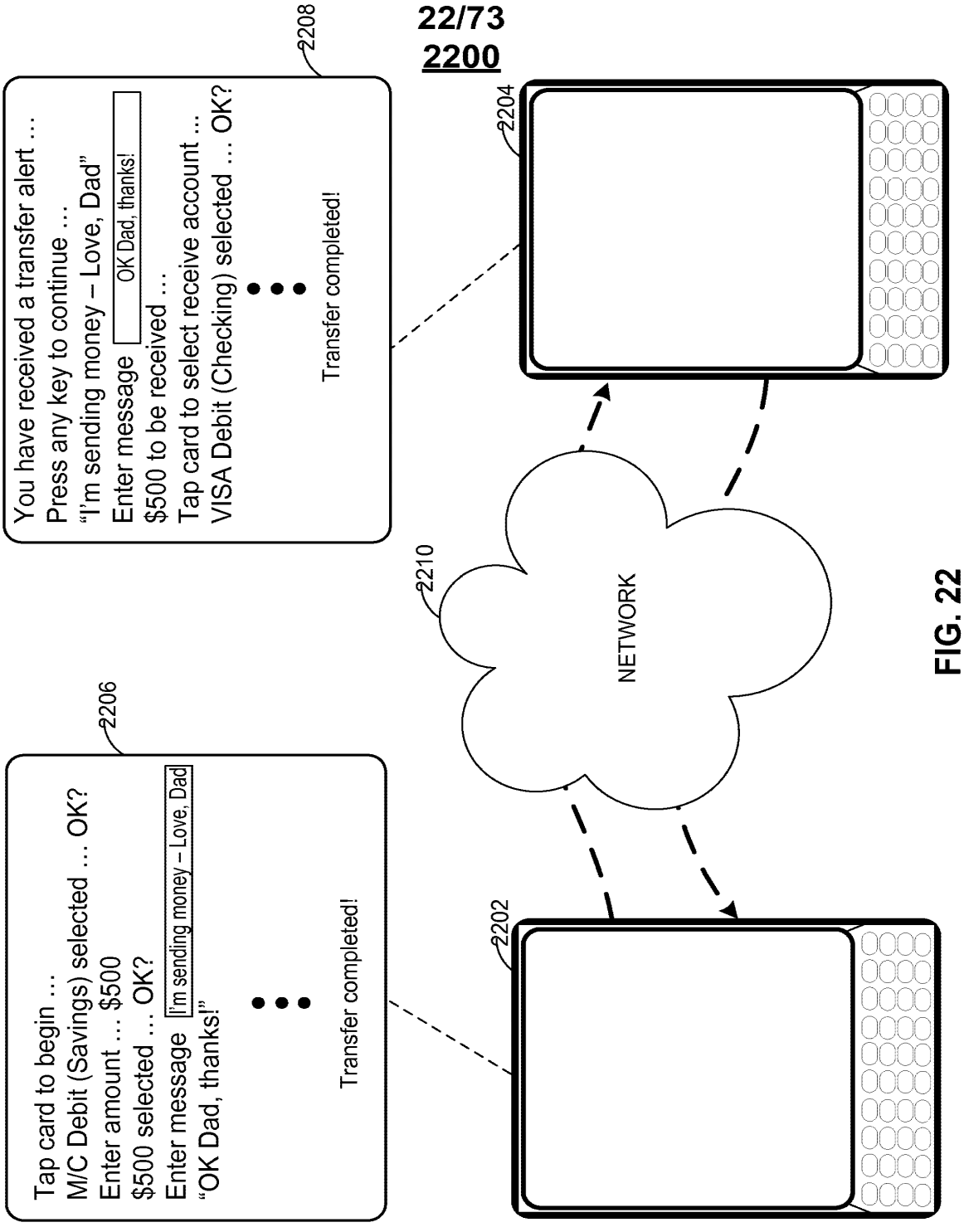

2208
You have received a transfer alert …
Press any key to continue …
"I'm sending money – Love, Dad"
Enter message OK Dad, thanks!
$500 to be received …
Tap card to select receive account …
VISA Debit (Checking) selected … OK?
• • •
Transfer completed!
2204
2210
NETWORK
2206
Tap card to begin …
M/C Debit (Savings) selected … OK?
Enter amount … $500
$500 selected … OK?
Enter message I'm sending money – Love, Dad
"OK Dad, thanks!"
• • •
Transfer completed!
2202

FIG. 22

2300

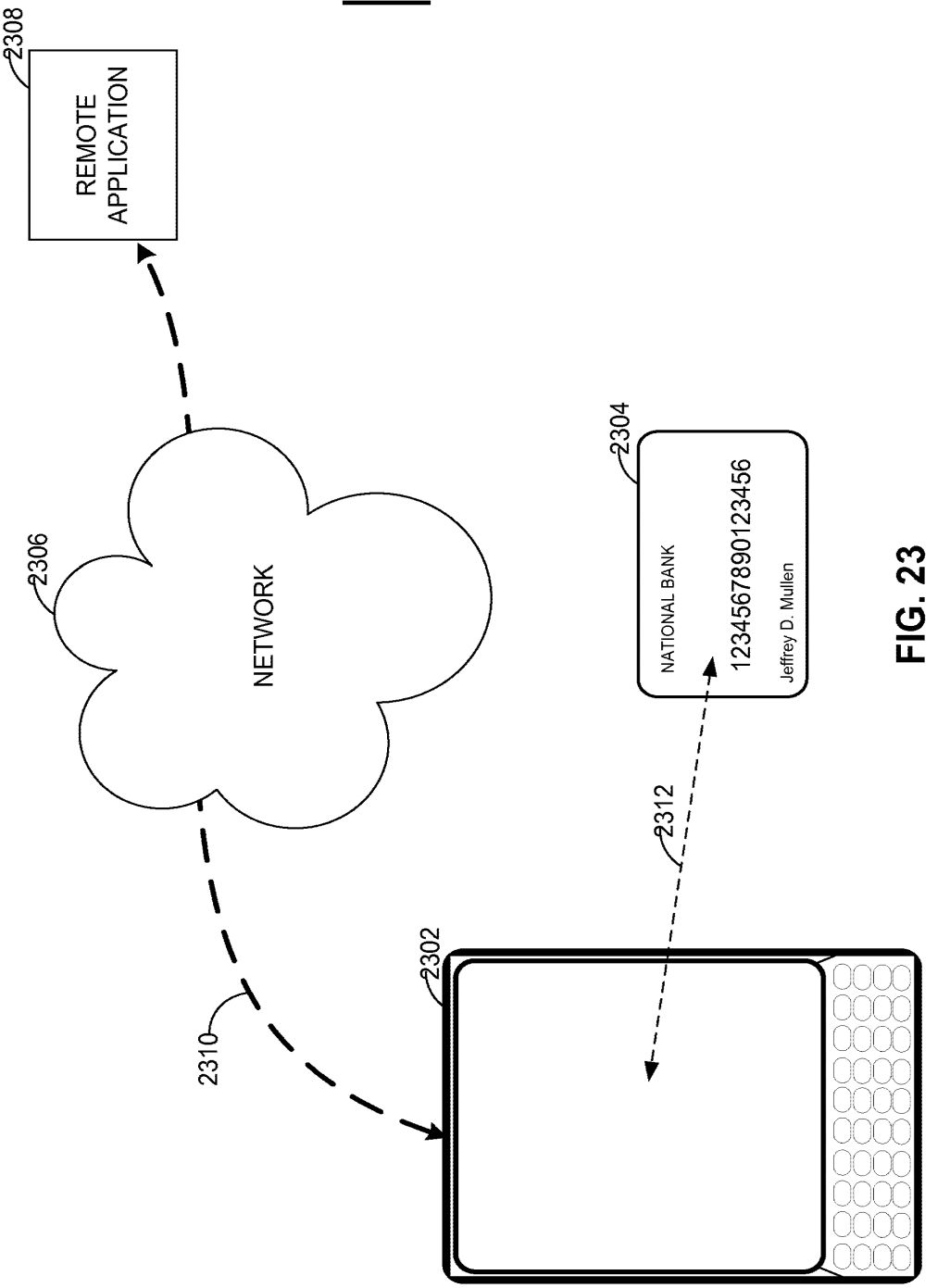

2308
REMOTE APPLICATION
2306
NETWORK
2304
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
2312
2302
2310

FIG. 23

24/73
2400

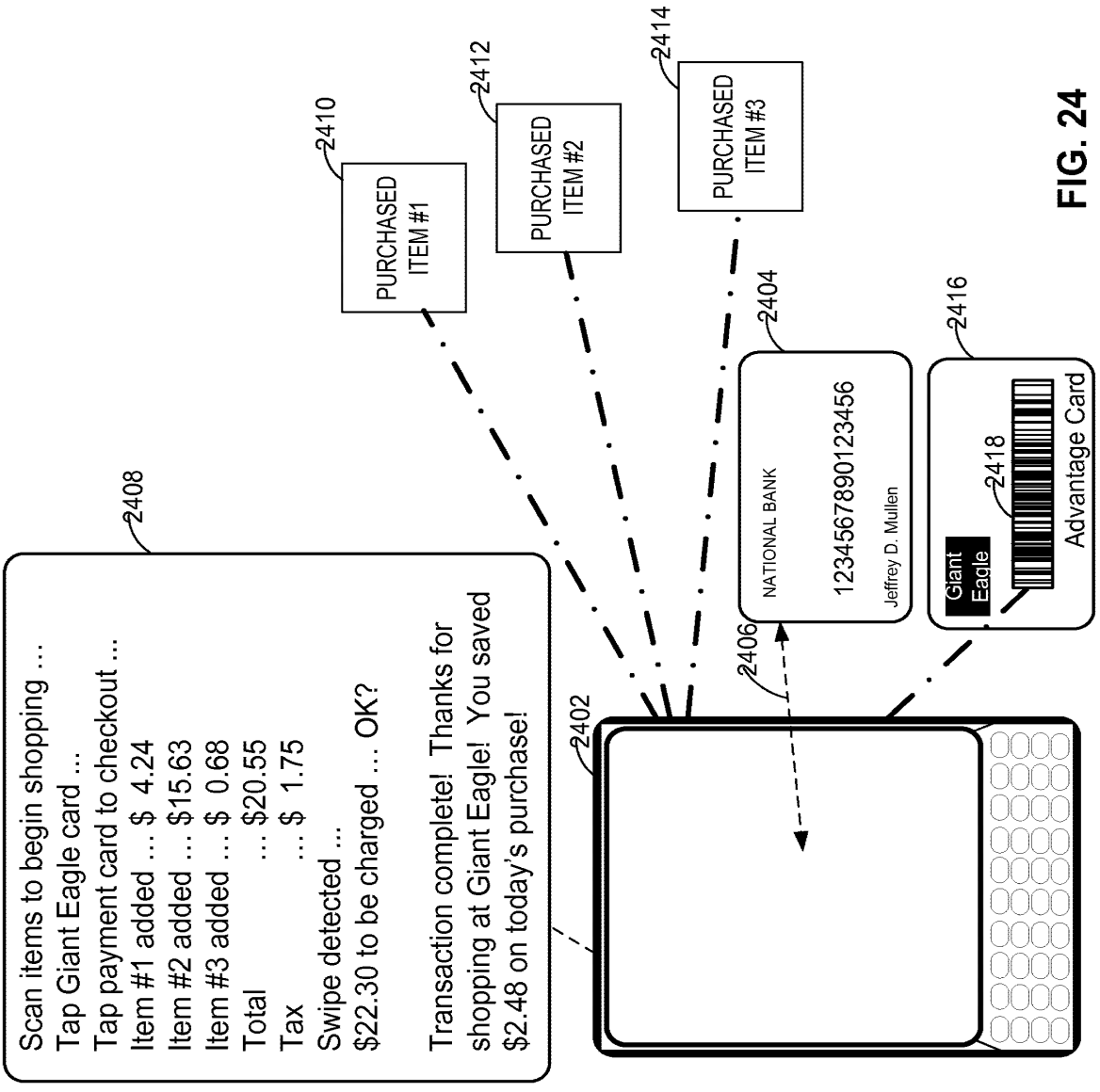


FIG. 24

25/73

2500

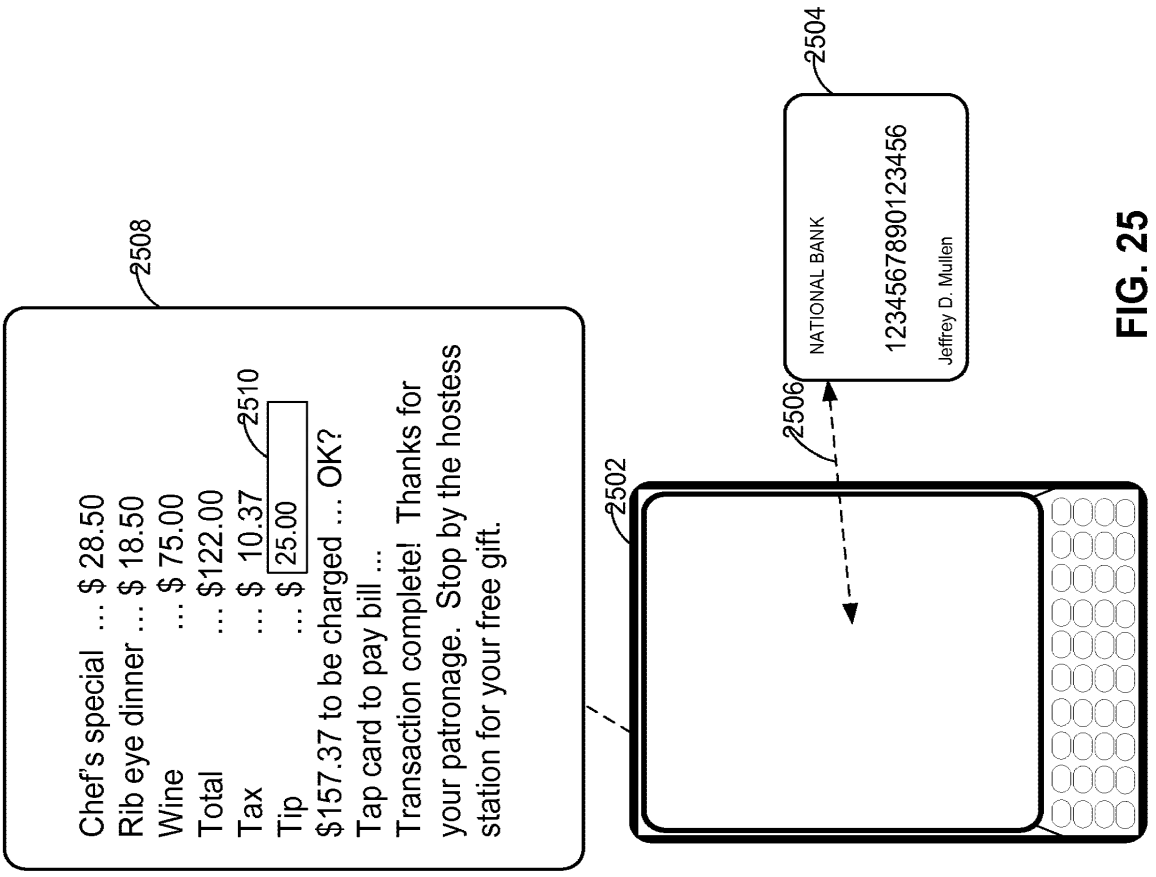


FIG. 25

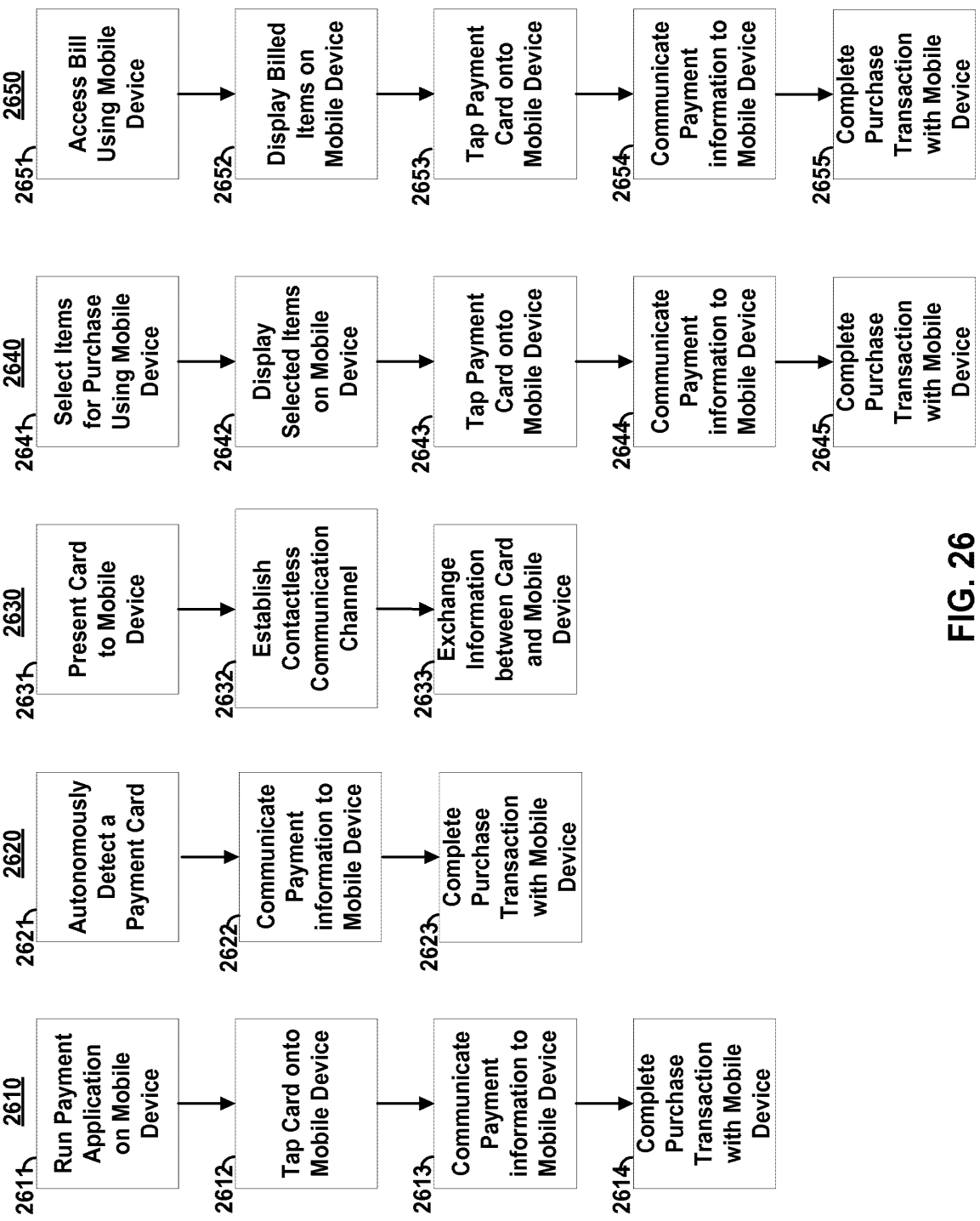

2610
2611
Run Payment Application on Mobile Device
2612
Tap Card onto Mobile Device
2613
Communicate Payment information to Mobile Device
2614
Complete Purchase Transaction with Mobile Device
2620
2621
Autonomously Detect a Payment Card
2622
Communicate Payment information to Mobile Device
2623
Complete Purchase Transaction with Mobile Device
2630
2631
Present Card to Mobile Device
2632
Establish Contactless Communication Channel
2633
Exchange Information between Card and Mobile Device
2640
2641
Select Items for Purchase Using Mobile Device
2642
Display Selected Items on Mobile Device
2643
Tap Payment Card onto Mobile Device
2644
Communicate Payment information to Mobile Device
2645
Complete Purchase Transaction with Mobile Device
2650
2651
Access Bill Using Mobile Device
2652
Display Billed Items on Mobile Device
2653
Tap Payment Card onto Mobile Device
2654
Communicate Payment information to Mobile Device
2655
Complete Purchase Transaction with Mobile Device

FIG. 26

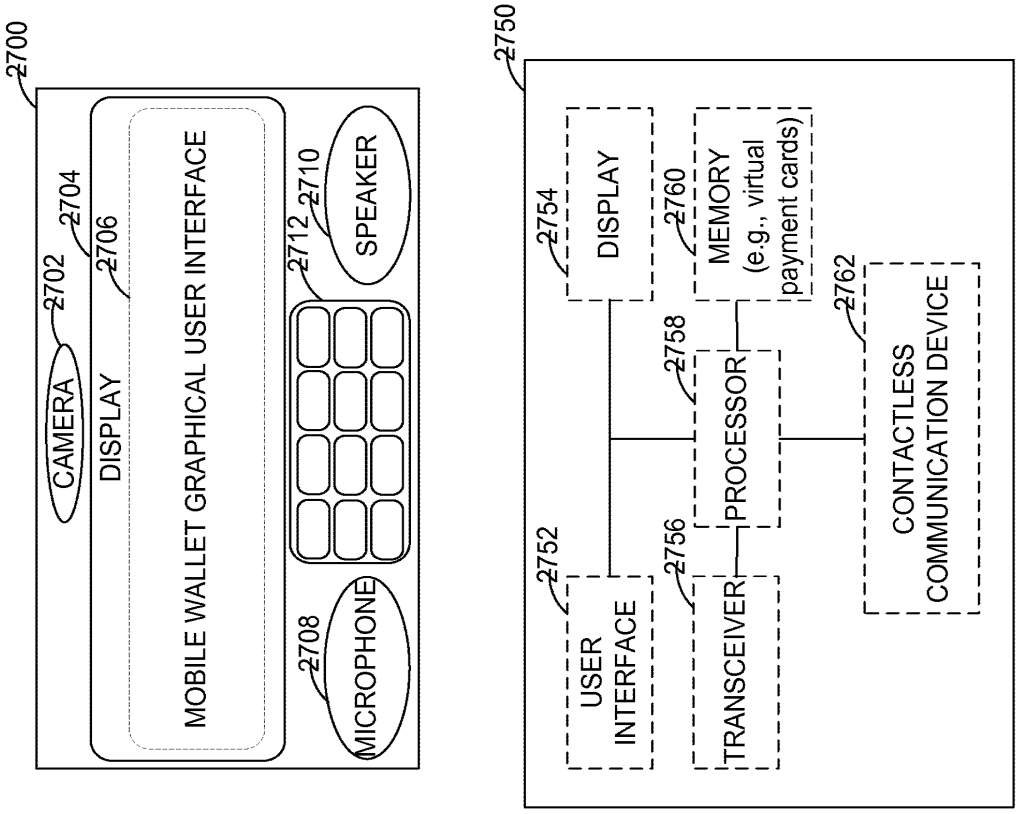

2700
CAMERA
2702
2704
DISPLAY
2706
MOBILE WALLET GRAPHICAL USER INTERFACE
2712
2710
SPEAKER
2708
MICROPHONE
2750
2754
DISPLAY
2760
MEMORY
(e.g., virtual
payment cards)
2758
PROCESSOR
2762
CONTACTLESS
COMMUNICATION DEVICE
2752
USER
INTERFACE
2756
TRANSCEIVER

FIG. 27

2800

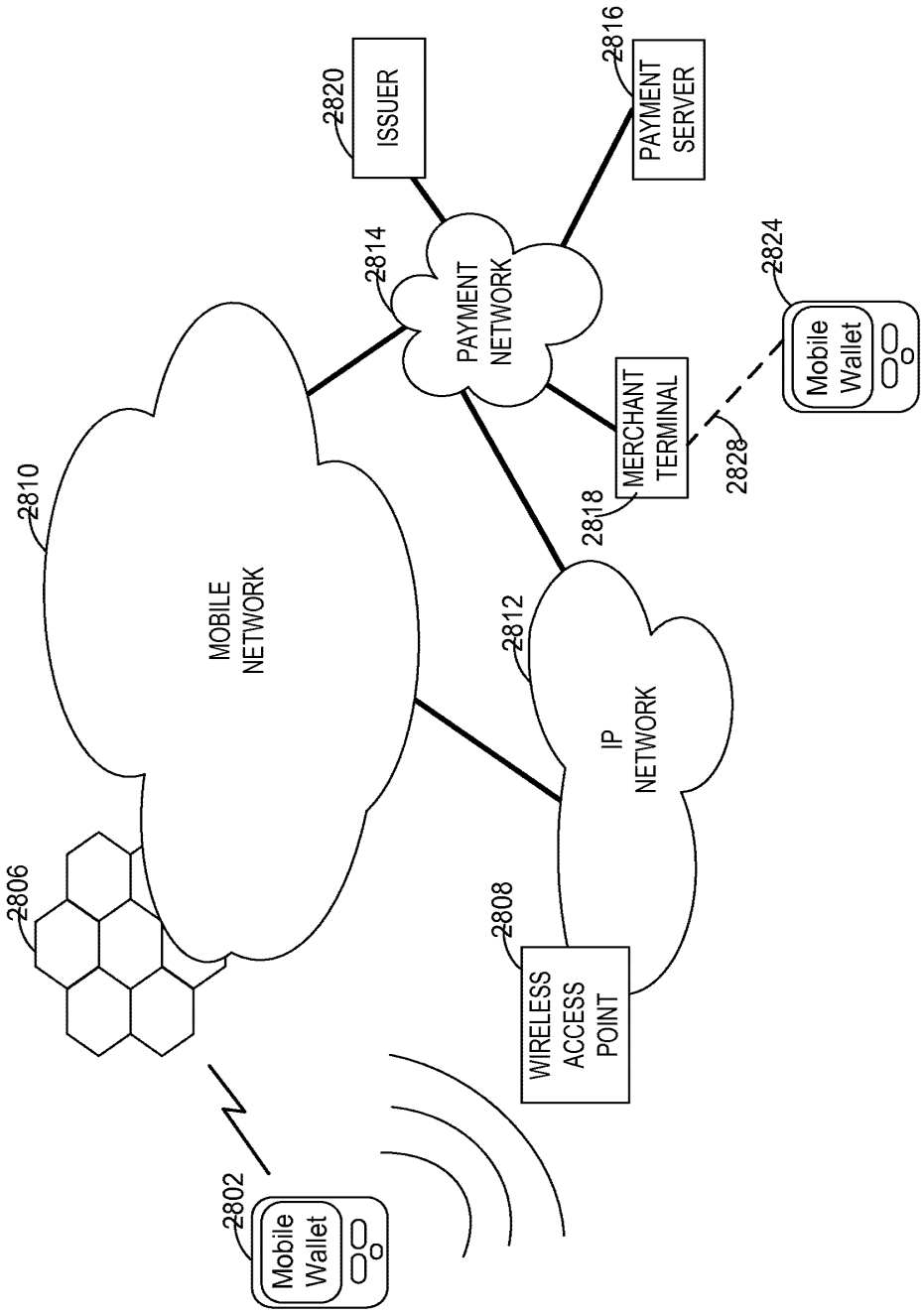

2820
ISSUER
2816
PAYMENT SERVER
2814
PAYMENT NETWORK
2824
Mobile Wallet
2828
MERCHANT TERMINAL
2818
2810
MOBILE NETWORK
2812
IP NETWORK
2806
2808
WIRELESS ACCESS POINT
2802
Mobile Wallet

FIG. 28

2900

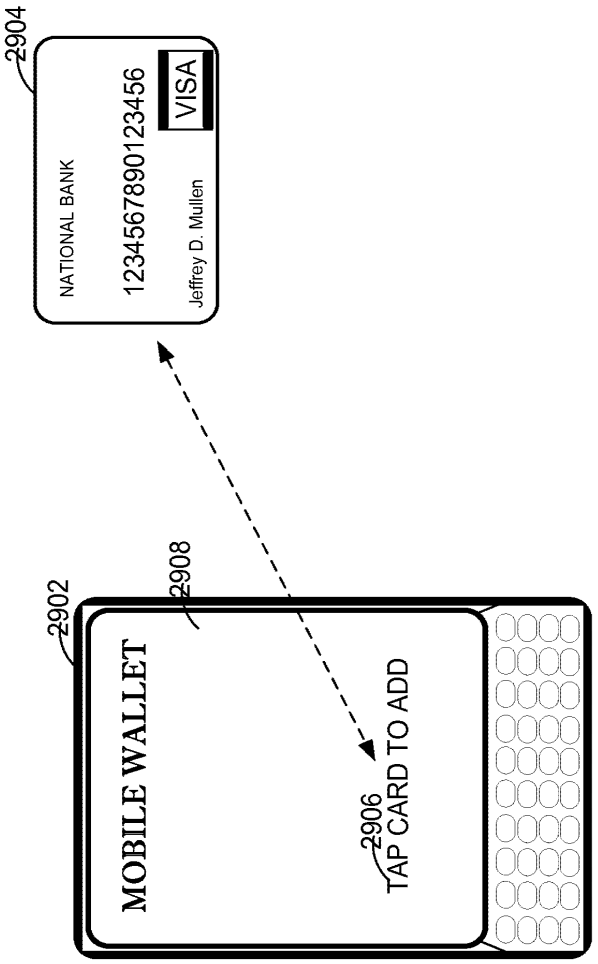

2904
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
2902
2908
MOBILE WALLET
2906
TAP CARD TO ADD

FIG. 29

3000

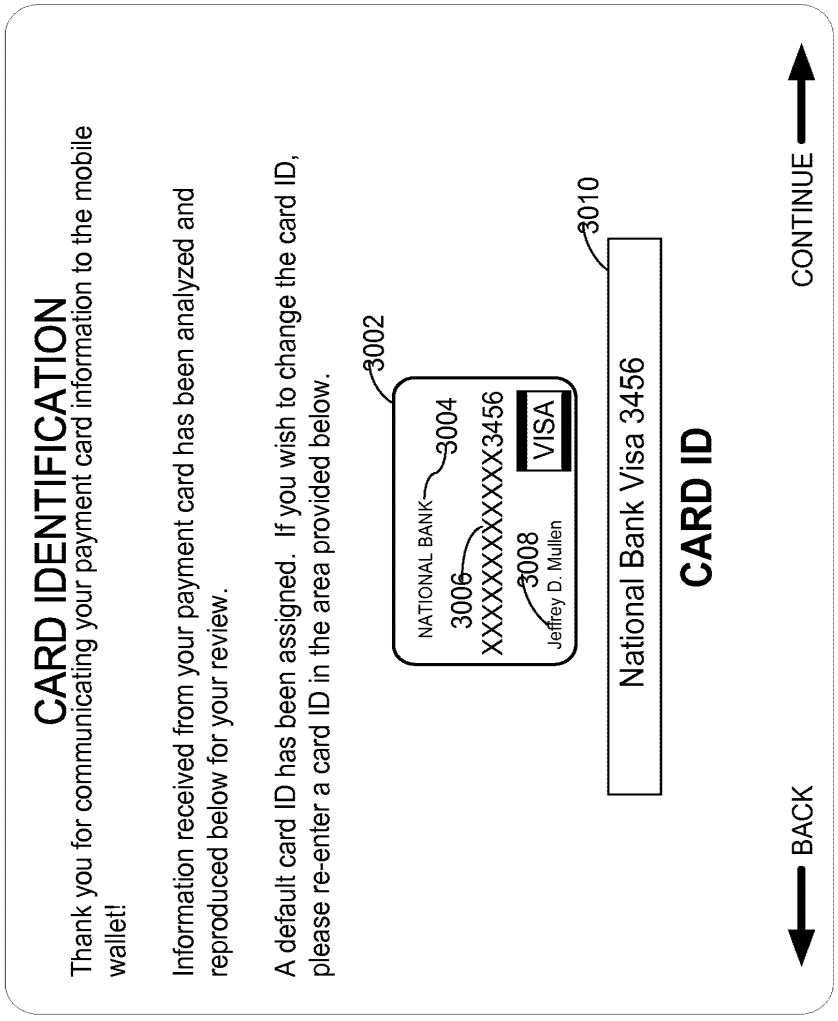

CARD IDENTIFICATION
Thank you for communicating your payment card information to the mobile wallet!
Information received from your payment card has been analyzed and reproduced below for your review.
A default card ID has been assigned. If you wish to change the card ID, please re-enter a card ID in the area provided below.
3002
NATIONAL BANK
3004
3006
XXXXXXXXXXXX3456
VISA
3008
Jeffrey D. Mullen
3010
National Bank Visa 3456
CARD ID
BACK
CONTINUE

FIG. 30

3100

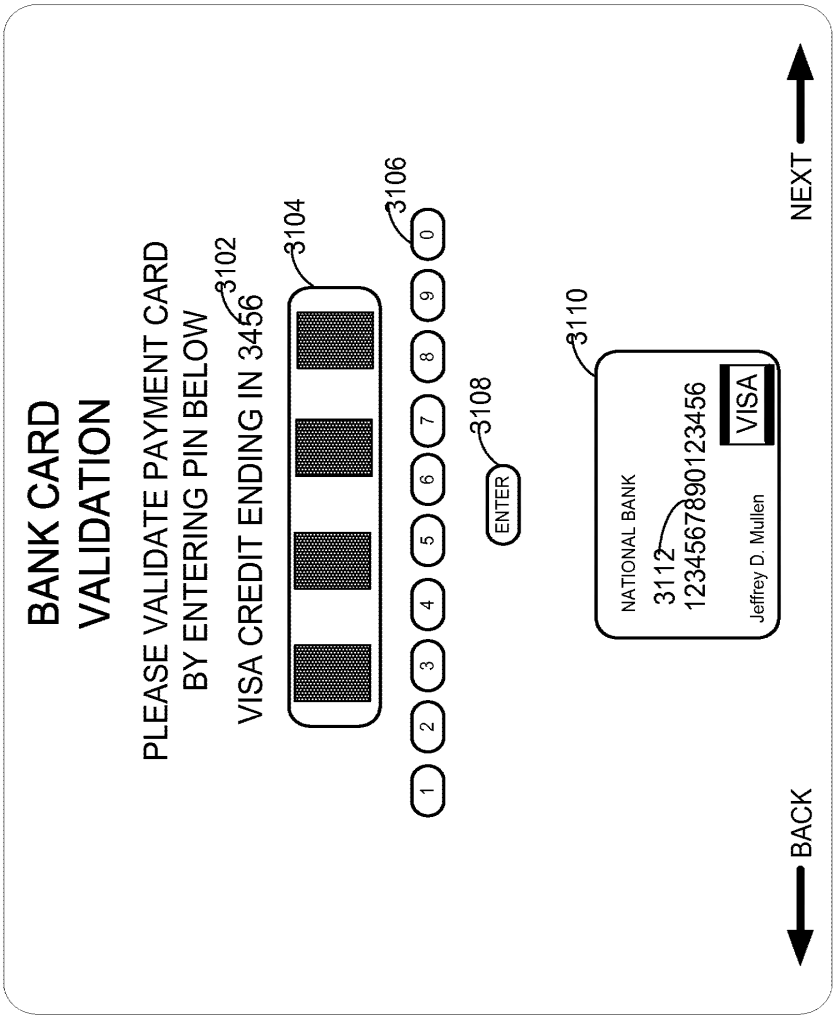

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING PIN BELOW
VISA CREDIT ENDING IN 3456
3102
3104
3106
1
2
3
4
5
6
7
8
9
0
ENTER
3108
3110
NATIONAL BANK
3112
1234567890123456
Jeffrey D. Mullen
VISA
BACK
NEXT

FIG. 31

3200

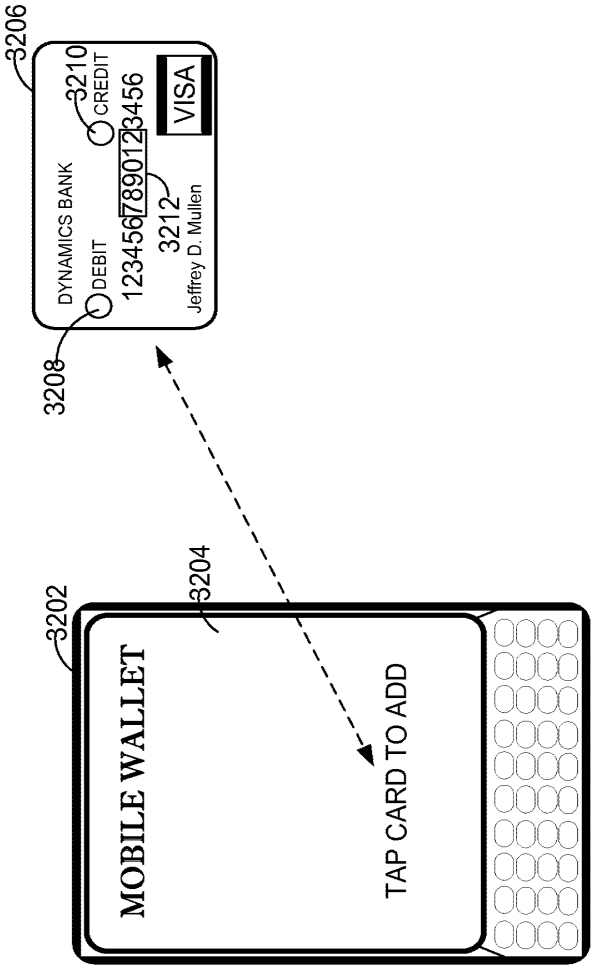

3206
3210
CREDIT
VISA
DYNAMICS BANK
DEBIT
1234567890123456
3212
Jeffrey D. Mullen
3208
3204
3202
MOBILE WALLET
TAP CARD TO ADD

FIG. 32

3300

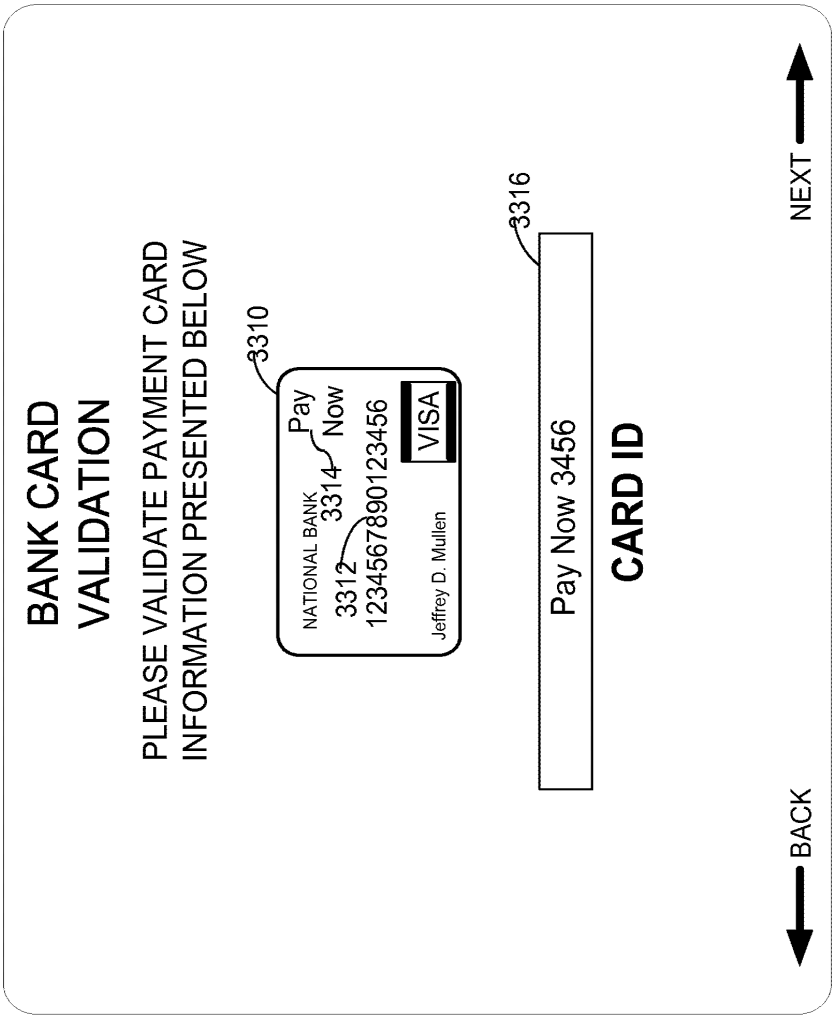

BANK CARD VALIDATION
PLEASE VALIDATE PAYMENT CARD INFORMATION PRESENTED BELOW
3310
NATIONAL BANK
3314
Pay Now
3312
1234567890123456
VISA
Jeffrey D. Mullen
3316
Pay Now 3456
CARD ID
NEXT
BACK

FIG. 33

3400

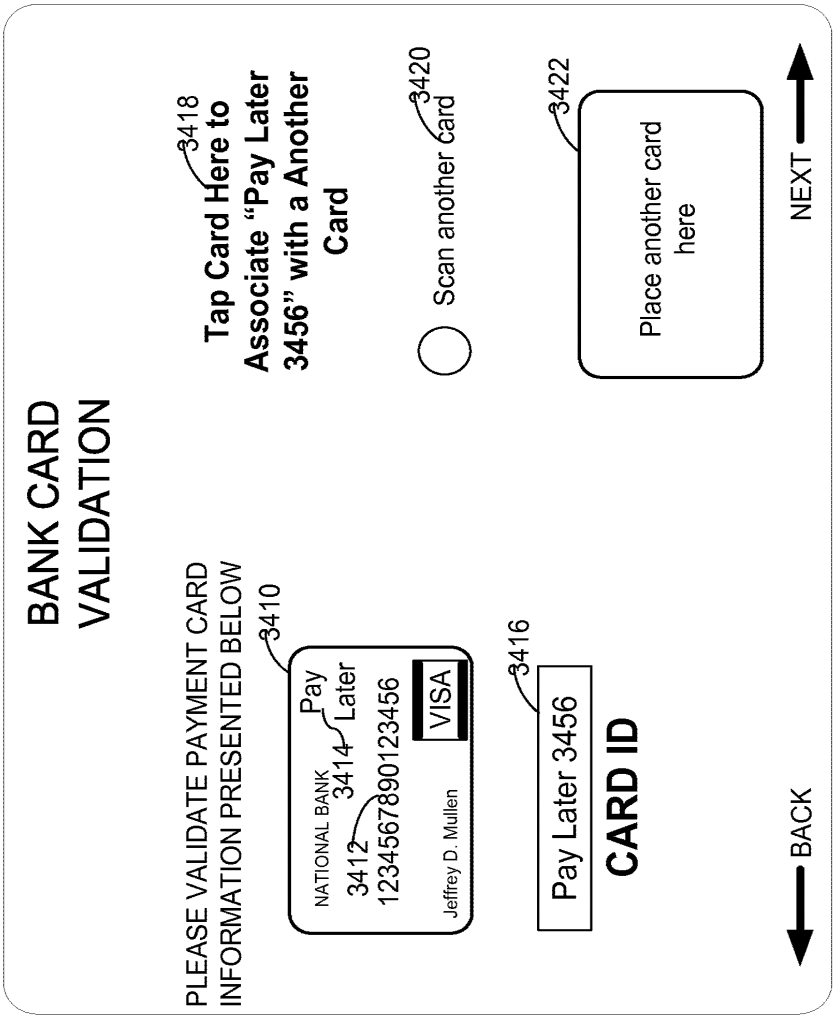

BANK CARD VALIDATION
PLEASE VALIDATE PAYMENT CARD INFORMATION PRESENTED BELOW
3410
NATIONAL BANK
Pay Later
3414
3412
1234567890123456
Jeffrey D. Mullen
VISA
3416
Pay Later 3456
CARD ID
3418
Tap Card Here to Associate "Pay Later 3456" with a Another Card
3420
Scan another card
3422
Place another card here
BACK
NEXT

FIG. 34

3500

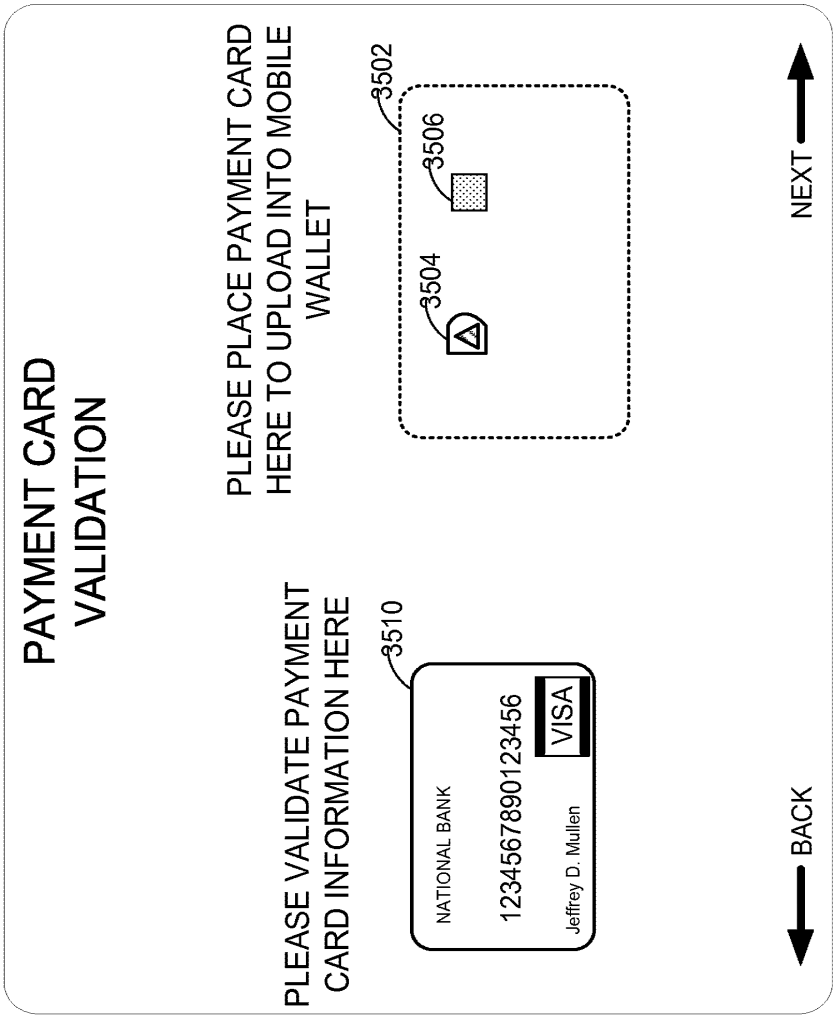

PAYMENT CARD VALIDATION
PLEASE PLACE PAYMENT CARD HERE TO UPLOAD INTO MOBILE WALLET
3502
3506
3504
PLEASE VALIDATE PAYMENT CARD INFORMATION HERE
3510
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
BACK
NEXT

FIG. 35

3600

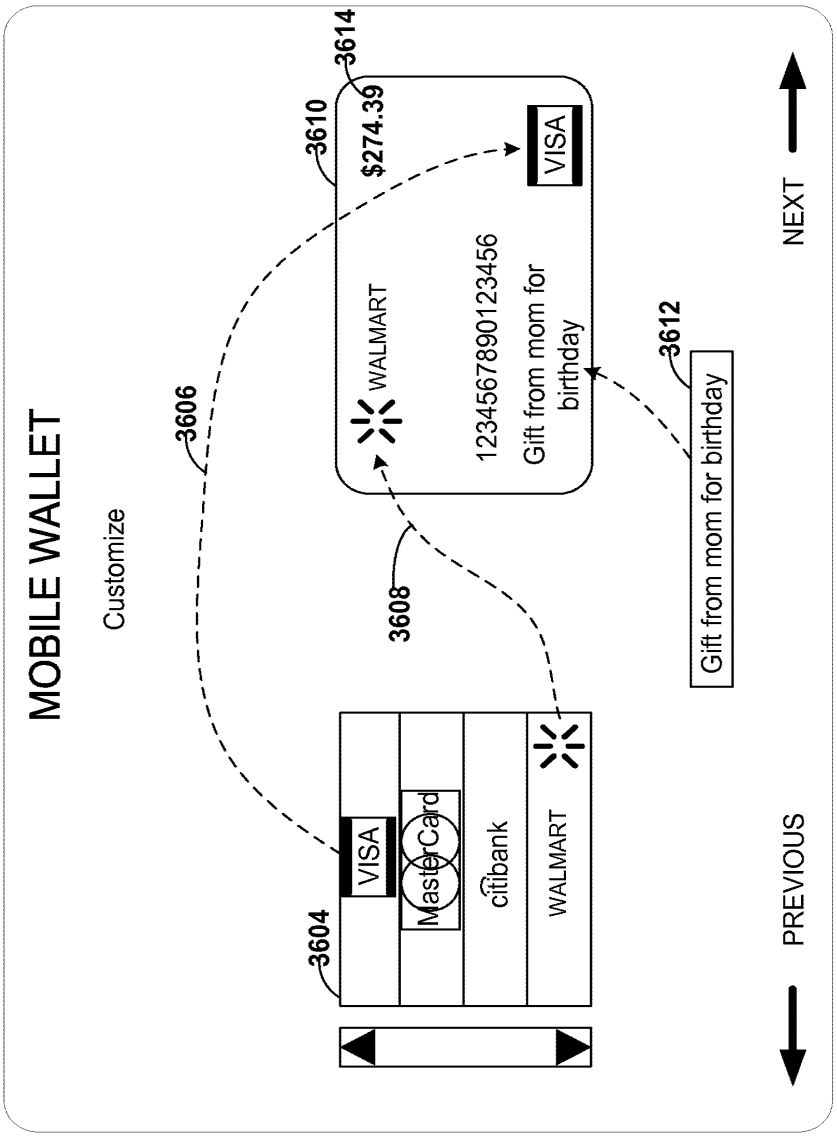

MOBILE WALLET
Customize
3606
3614
3610
$274.39
VISA
WALMART
1234567890123456
Gift from mom for birthday
3612
Gift from mom for birthday
3608
NEXT
PREVIOUS
3604
VISA
MasterCard
citibank
WALMART

FIG. 36

3700

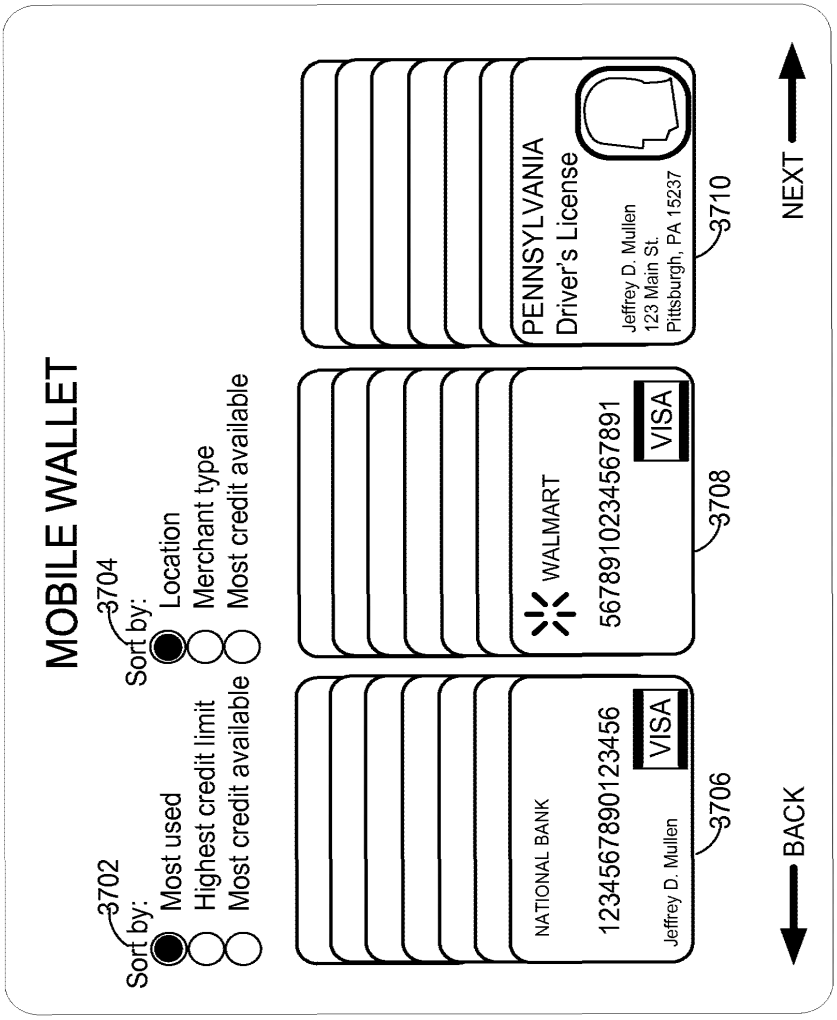

MOBILE WALLET
3702
Sort by:
Most used
Highest credit limit
Most credit available
3704
Sort by:
Location
Merchant type
Most credit available
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
3706
WALMART
5678910234567891
VISA
3708
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
3710
BACK
NEXT

FIG. 37

38/73
3800

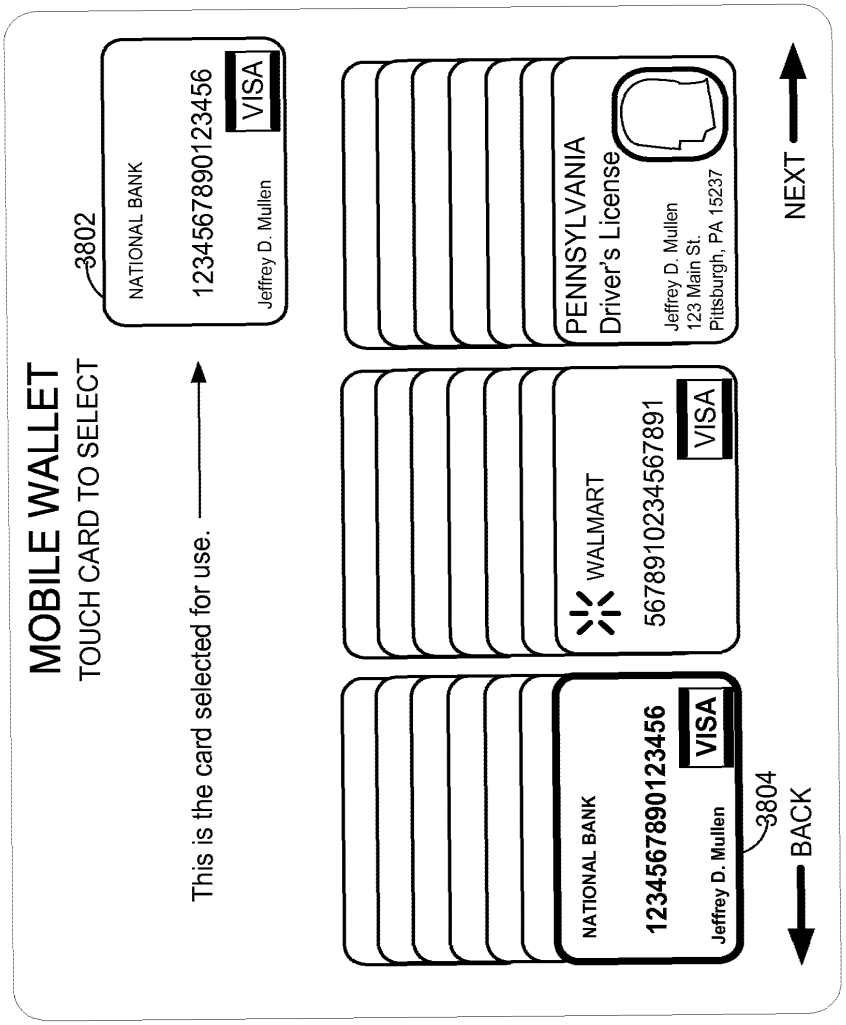


FIG. 38

3900

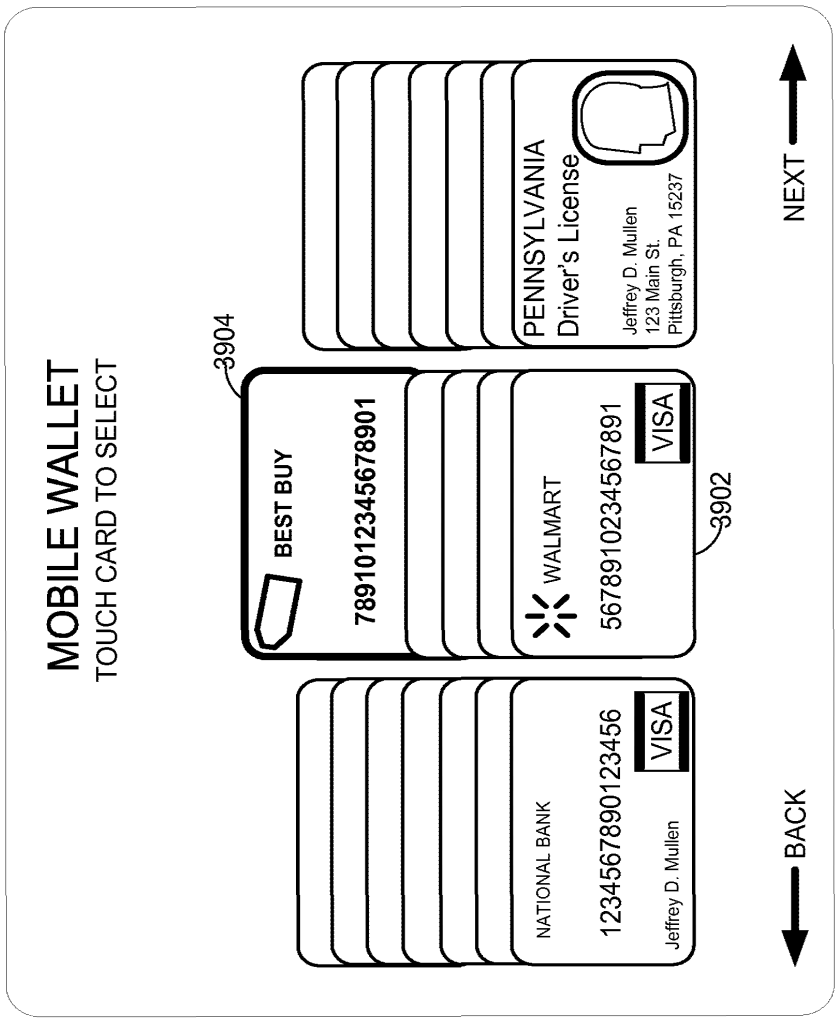

MOBILE WALLET
TOUCH CARD TO SELECT
3904
BEST BUY
7891012345678901
WALMART
5678910234567891
VISA
3902
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
BACK
NEXT

FIG. 39

4000

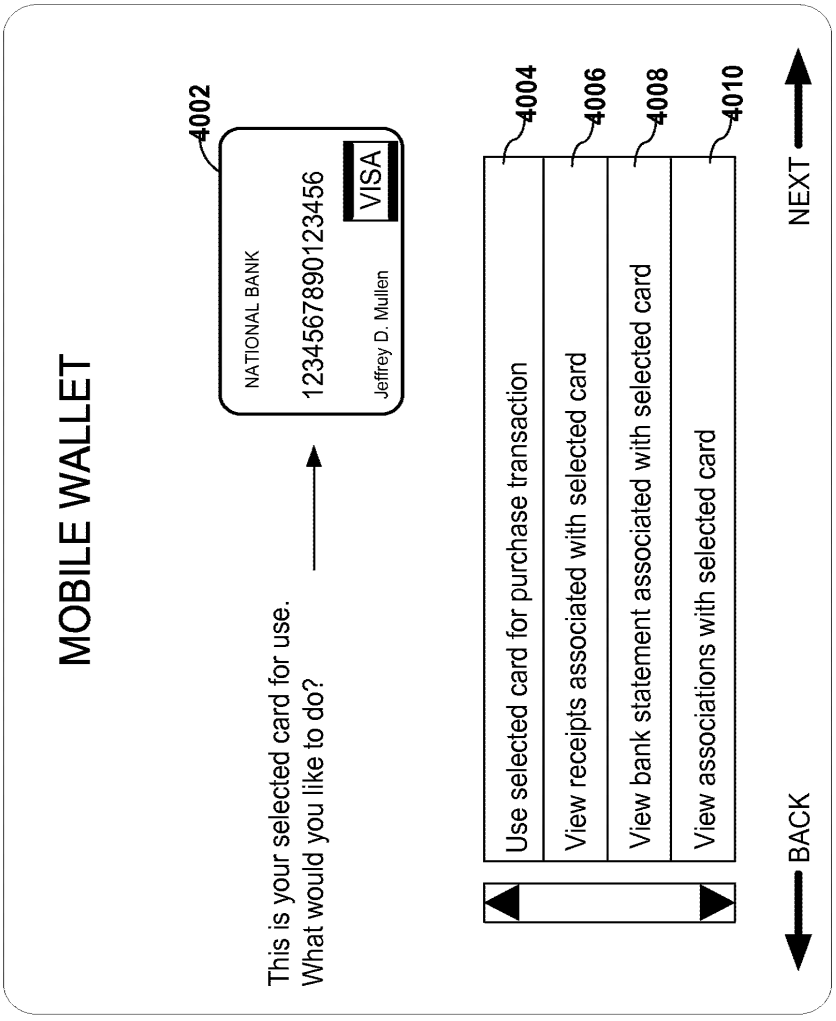

MOBILE WALLET
4002
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
This is your selected card for use.
What would you like to do?
4004
Use selected card for purchase transaction
4006
View receipts associated with selected card
4008
View bank statement associated with selected card
4010
View associations with selected card
BACK
NEXT

FIG. 40

4100

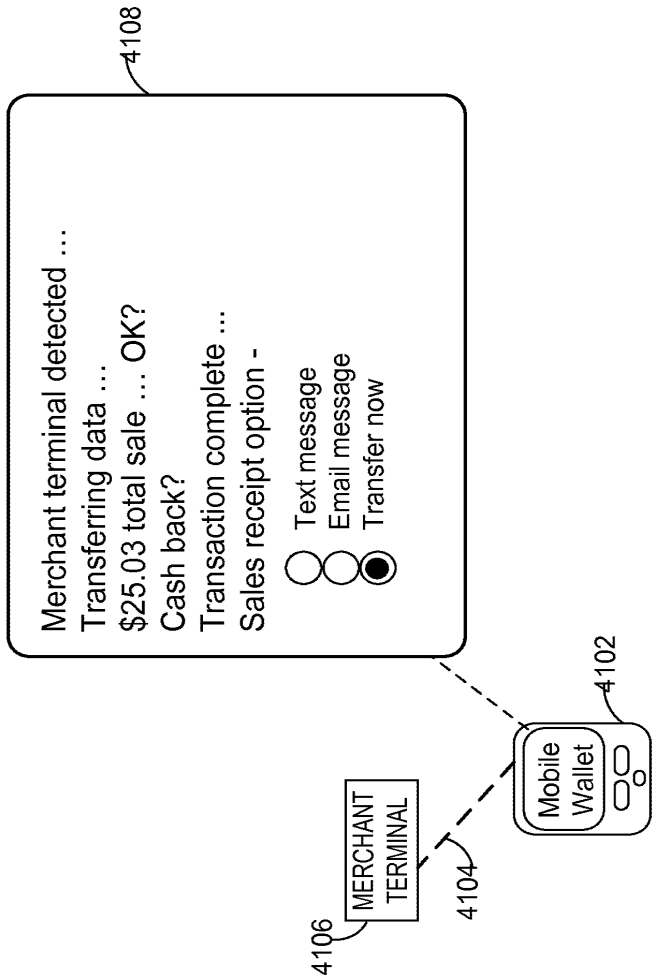

4108
Merchant terminal detected ...
Transferring data ...
$25.03 total sale ... OK?
Cash back?
Transaction complete ...
Sales receipt option -
Text message
Email message
Transfer now
4102
Mobile Wallet
4104
MERCHANT TERMINAL
4106

FIG. 41

4200

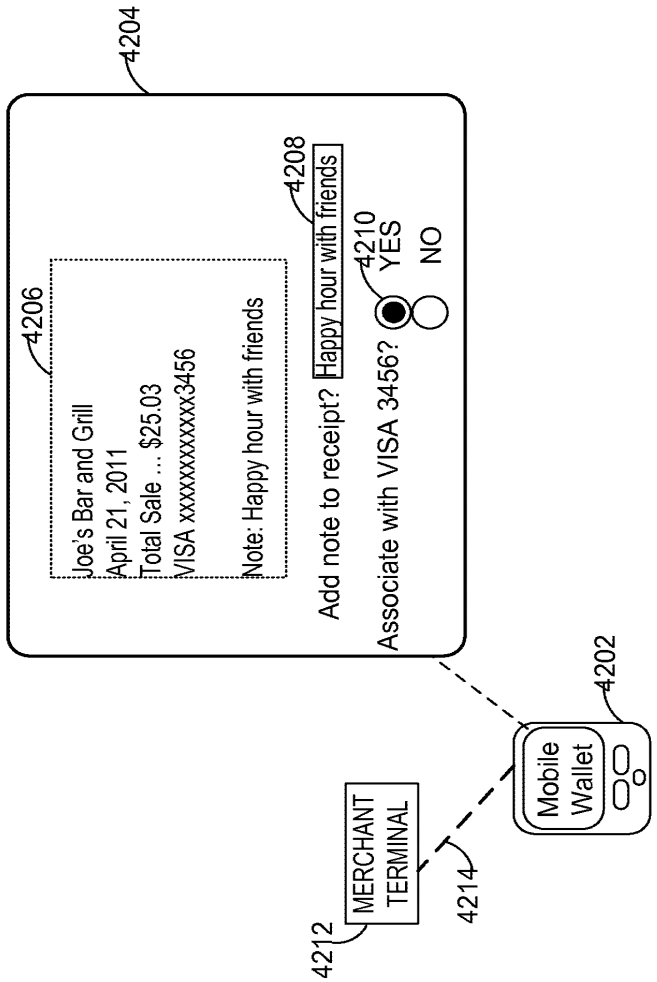

4204
4206
Joe's Bar and Grill
April 21, 2011
Total Sale ... $25.03
VISA xxxxxxxxxxx3456
Note: Happy hour with friends
4208
Add note to receipt? Happy hour with friends
4210
Associate with VISA 3456? YES NO
4202
Mobile Wallet
4212
MERCHANT TERMINAL
4214

FIG. 42

4300

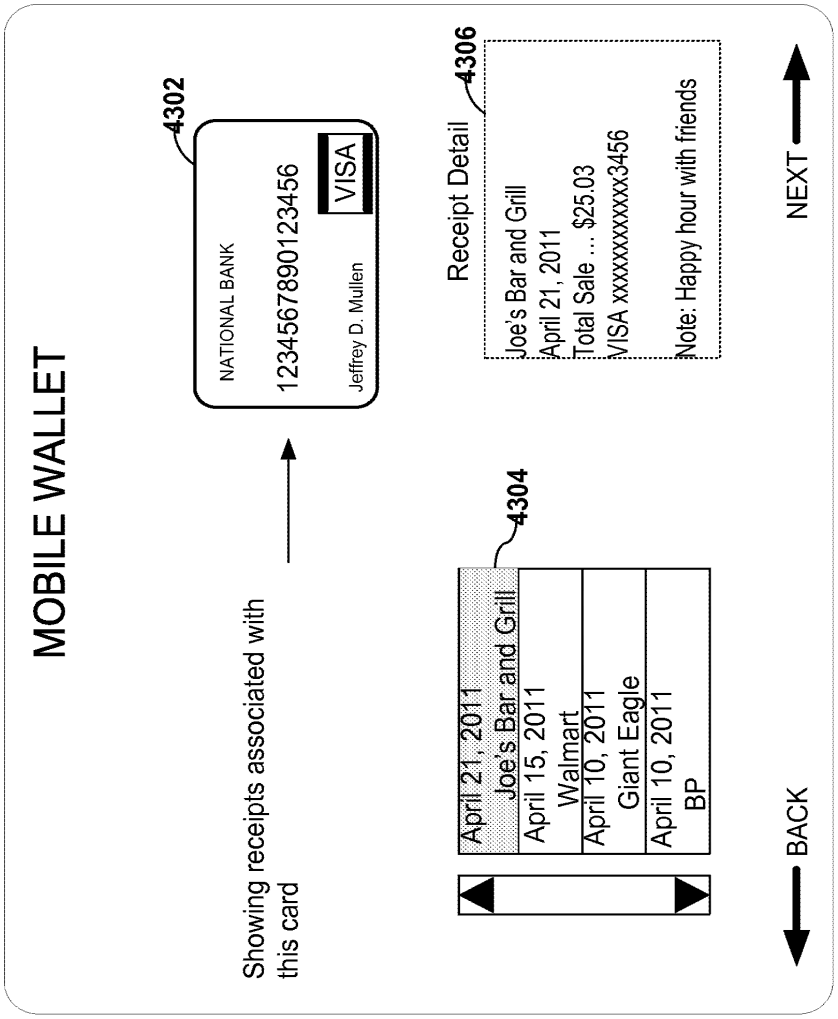

MOBILE WALLET
Showing receipts associated with this card
4302
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
4304
April 21, 2011
Joe's Bar and Grill
April 15, 2011
Walmart
April 10, 2011
Giant Eagle
April 10, 2011
BP
Receipt Detail
4306
Joe's Bar and Grill
April 21, 2011
Total Sale ... $25.03
VISA xxxxxxxxxxx3456
Note: Happy hour with friends
BACK
NEXT

FIG. 43

4400

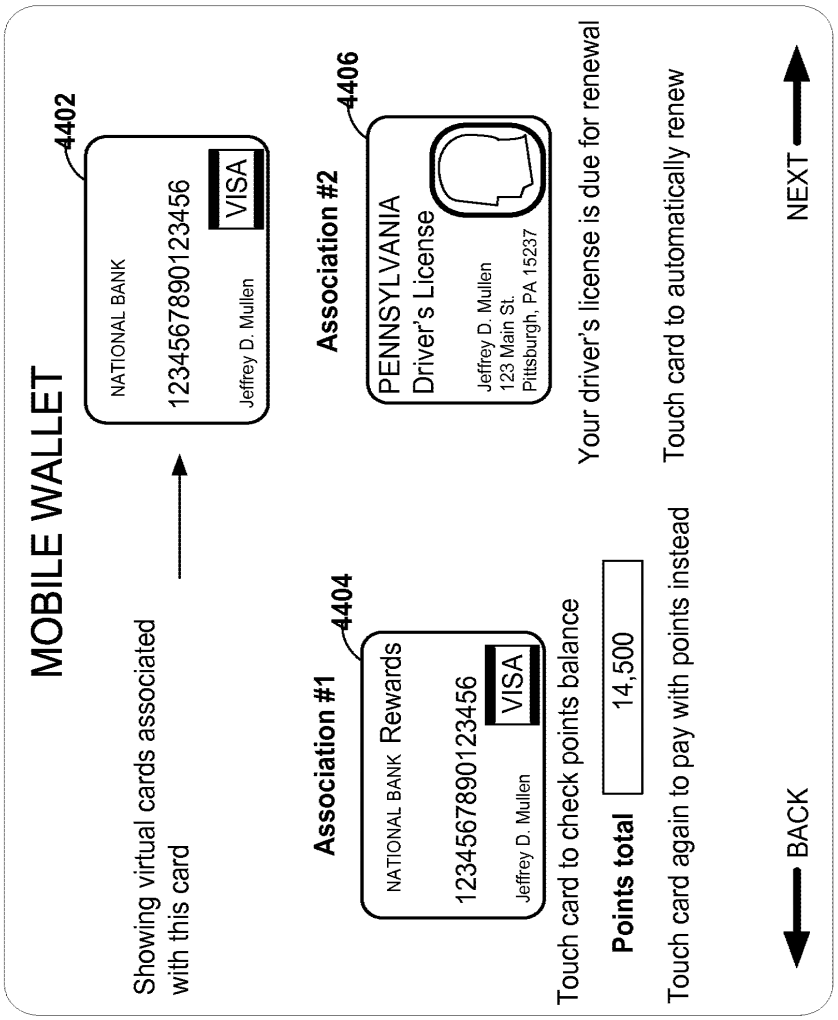

MOBILE WALLET
4402
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
Showing virtual cards associated with this card
Association #1
4404
NATIONAL BANK Rewards
1234567890123456
Jeffrey D. Mullen
VISA
Touch card to check points balance
Points total
14,500
Touch card again to pay with points instead
Association #2
4406
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
Your driver's license is due for renewal
Touch card to automatically renew
BACK
NEXT

FIG. 44

4500

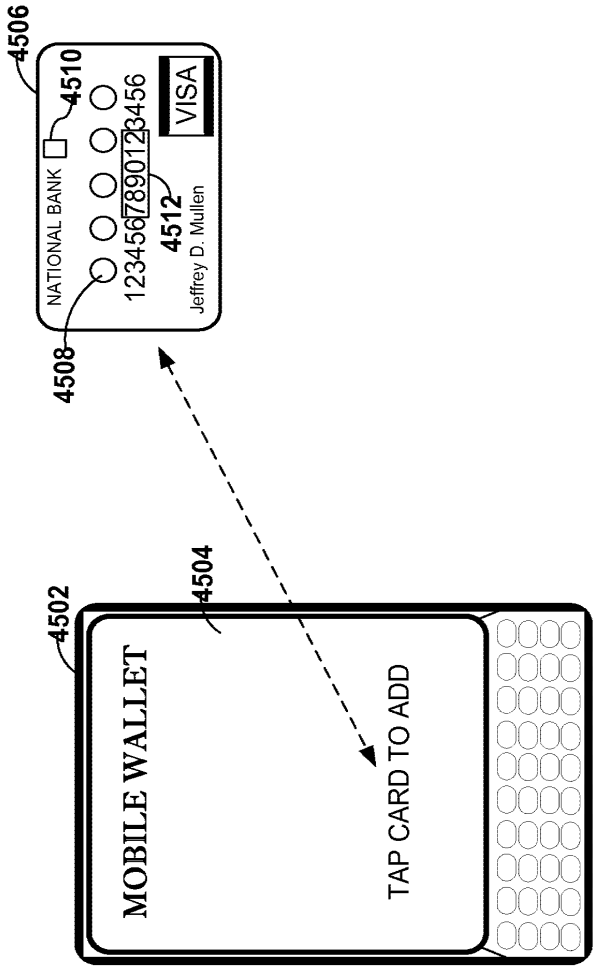

4506
4510
NATIONAL BANK
123456789012 3456
VISA
4512
Jeffrey D. Mullen
4508
4502
4504
MOBILE WALLET
TAP CARD TO ADD

FIG. 45

4600

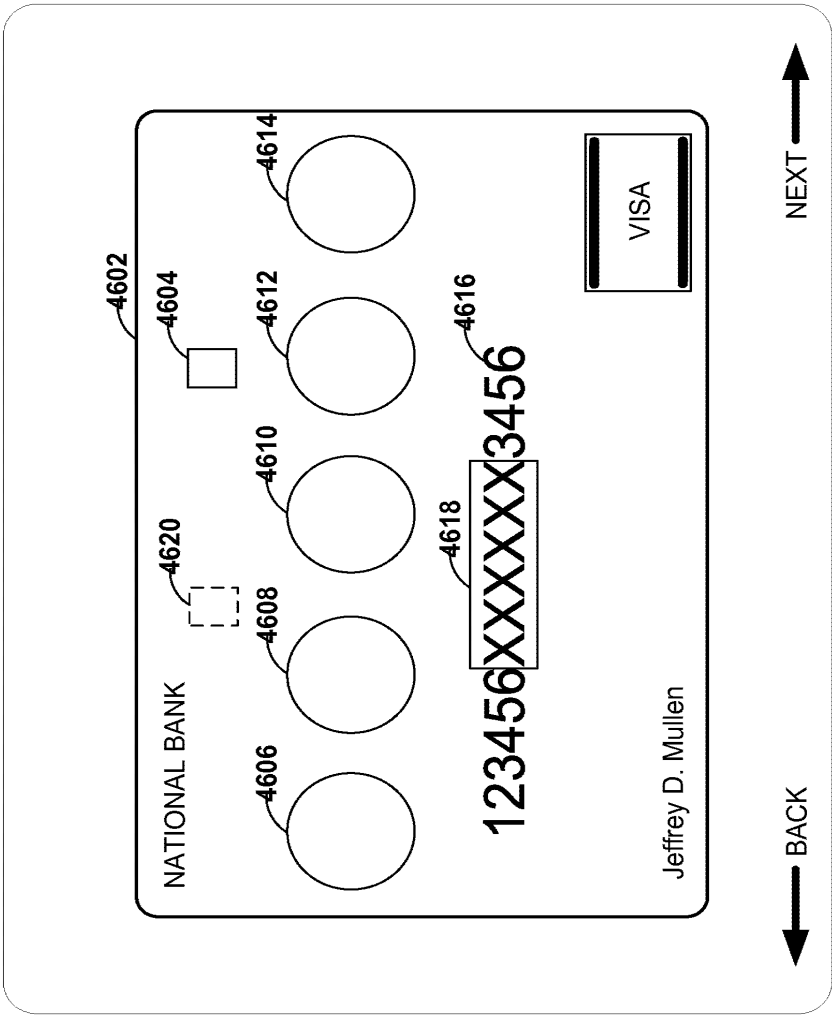

4602
4604
4606
4608
4610
4612
4614
4616
4618
4620
NATIONAL BANK
123456XXXXXX3456
Jeffrey D. Mullen
VISA
NEXT
BACK

FIG. 46

47/73
4700

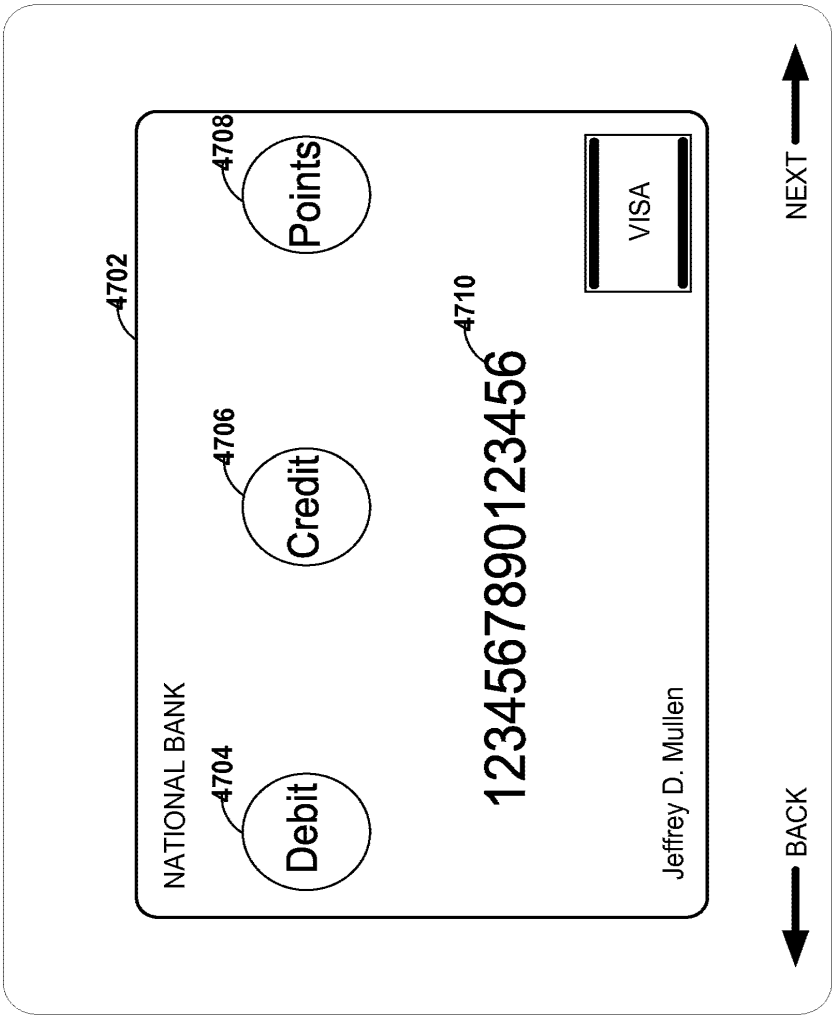


FIG. 47

48/73
4800

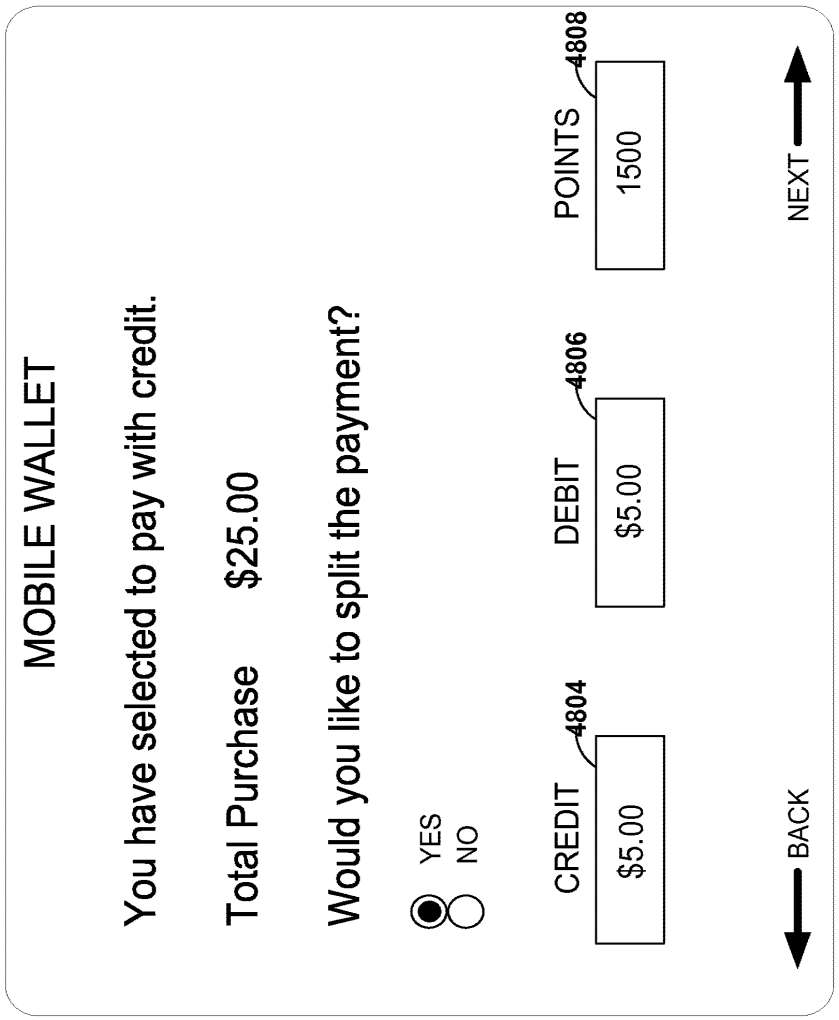


FIG. 48

4900

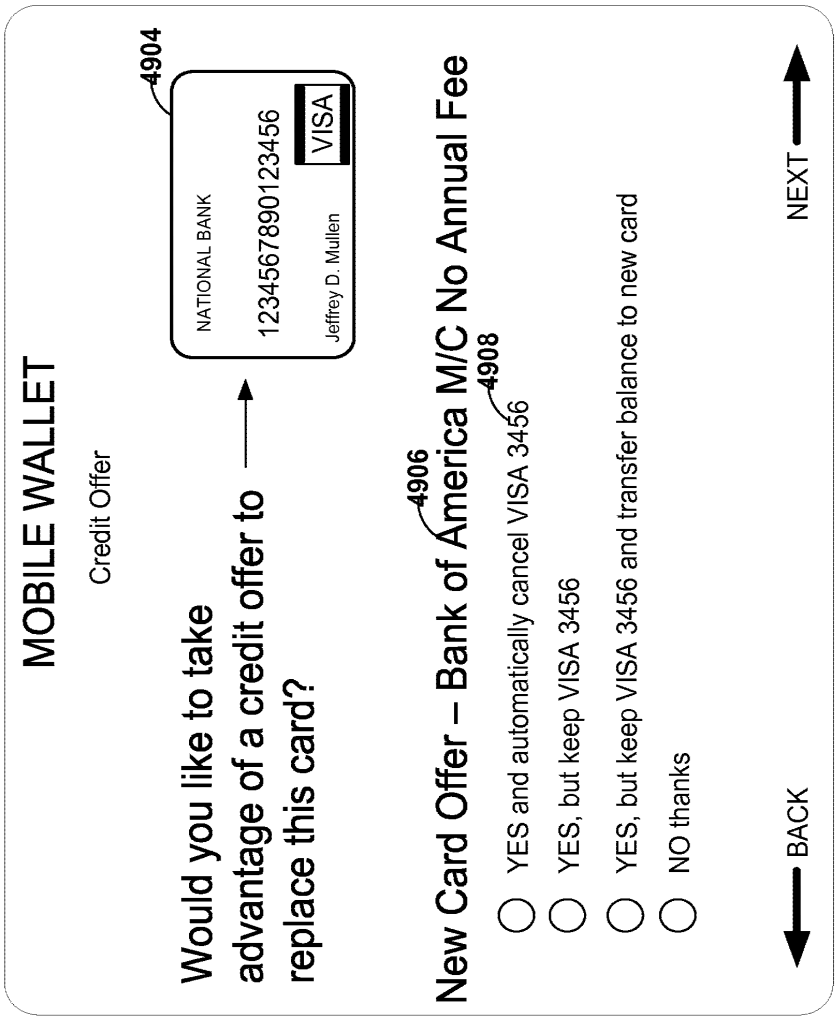

MOBILE WALLET
Credit Offer
Would you like to take advantage of a credit offer to replace this card?
4904
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
New Card Offer – Bank of America M/C No Annual Fee
4906
4908
YES and automatically cancel VISA 3456
YES, but keep VISA 3456
YES, but keep VISA 3456 and transfer balance to new card
NO thanks
BACK
NEXT

FIG. 49

50/73
5000

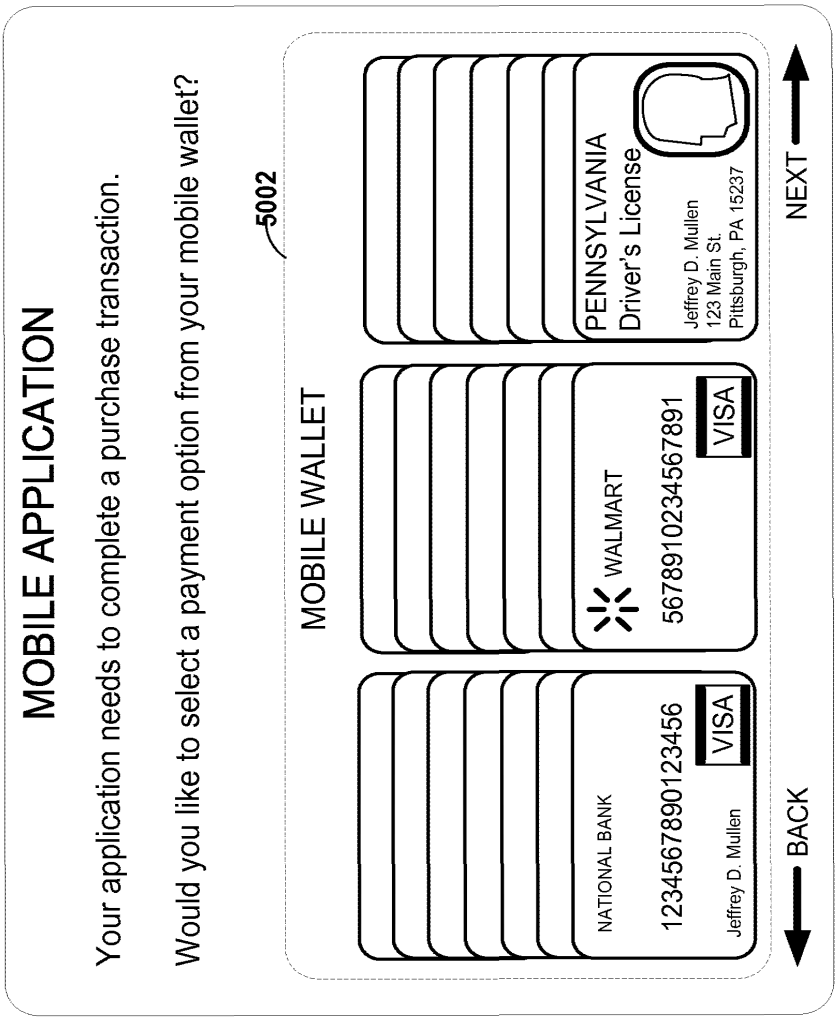


FIG. 50

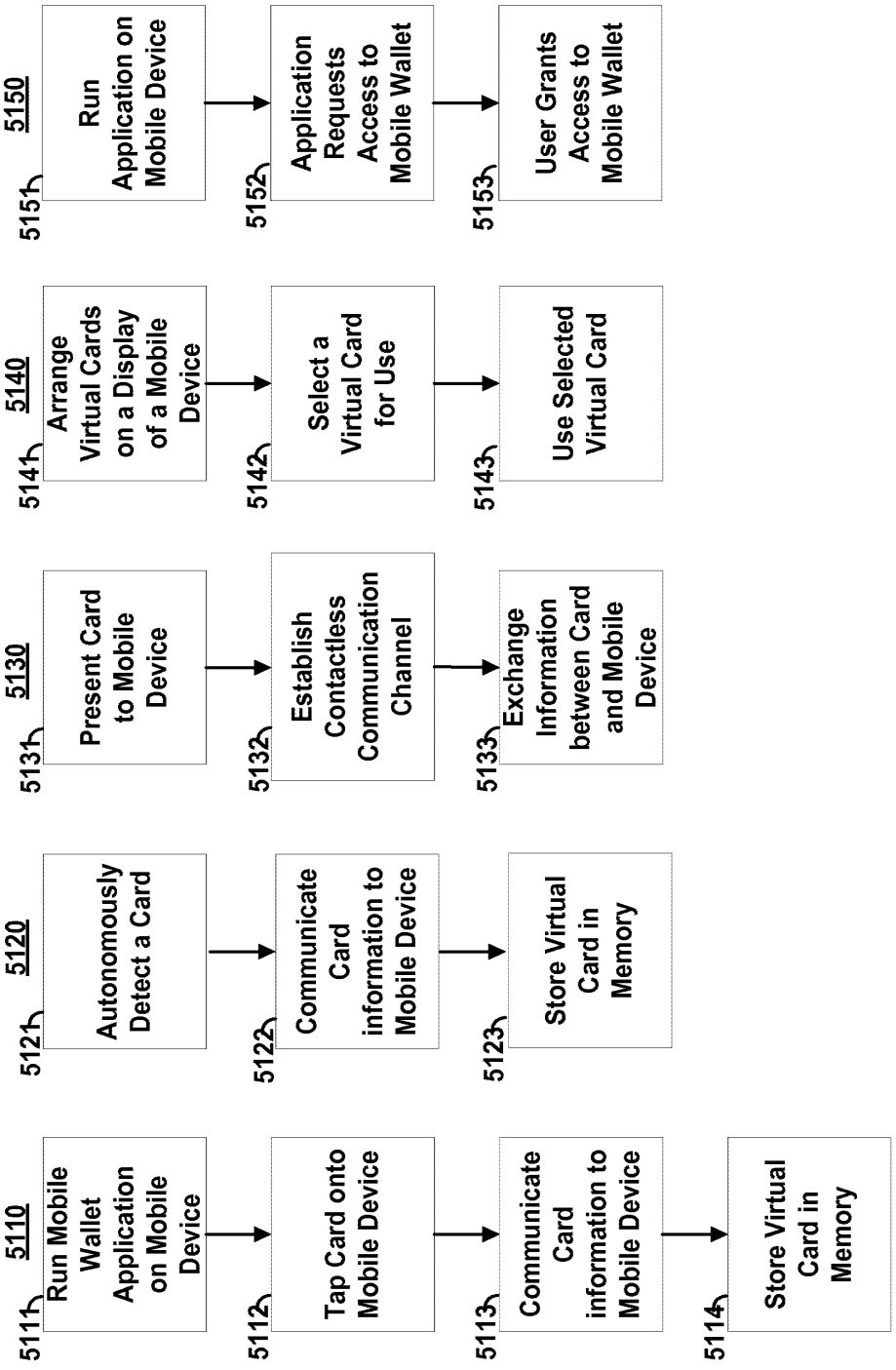

5110
Run Mobile Wallet Application on Mobile Device
5111
Tap Card onto Mobile Device
5112
Communicate Card information to Mobile Device
5113
Store Virtual Card in Memory
5114
5120
Autonomously Detect a Card
5121
Communicate Card information to Mobile Device
5122
Store Virtual Card in Memory
5123
5130
Present Card to Mobile Device
5131
Establish Contactless Communication Channel
5132
Exchange Information between Card and Mobile Device
5133
5140
Arrange Virtual Cards on a Display of a Mobile Device
5141
Select a Virtual Card for Use
5142
Use Selected Virtual Card
5143
5150
Run Application on Mobile Device
5151
Application Requests Access to Mobile Wallet
5152
User Grants Access to Mobile Wallet
5153

FIG. 51

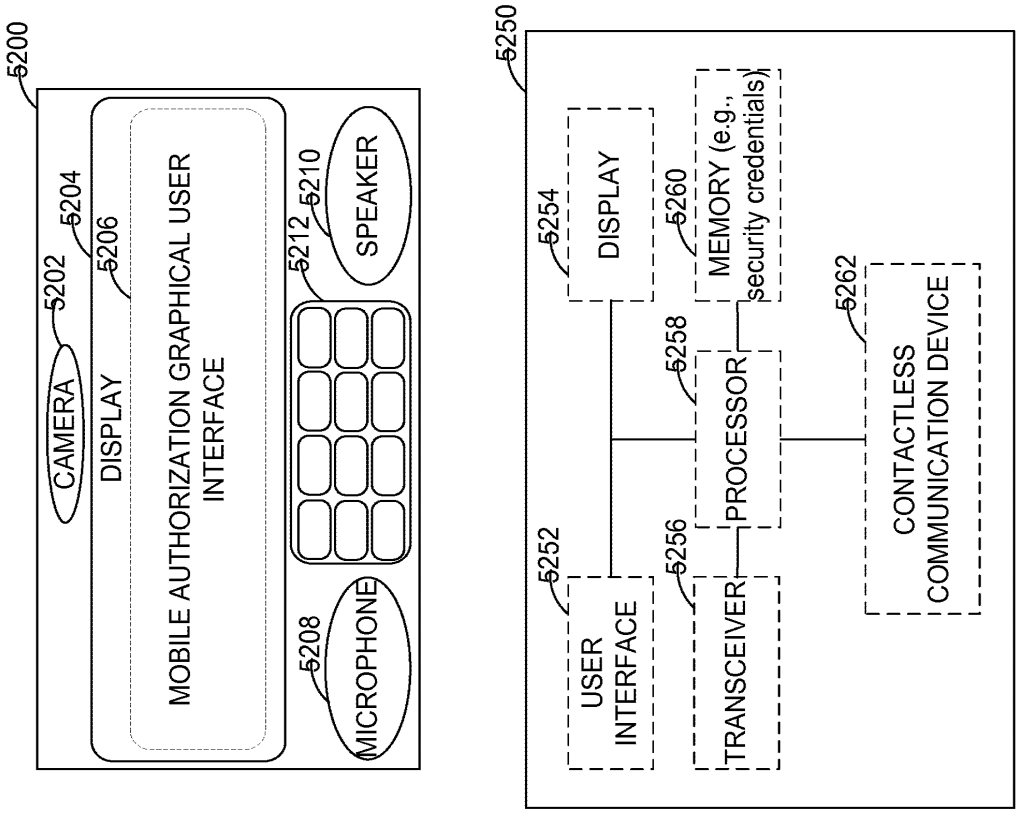

5200
CAMERA
5202
DISPLAY
5204
MOBILE AUTHORIZATION GRAPHICAL USER INTERFACE
5206
5208
MICROPHONE
5210
SPEAKER
5212
5250
USER INTERFACE
5252
DISPLAY
5254
TRANSCEIVER
5256
PROCESSOR
5258
MEMORY (e.g., security credentials)
5260
CONTACTLESS COMMUNICATION DEVICE
5262

FIG. 52

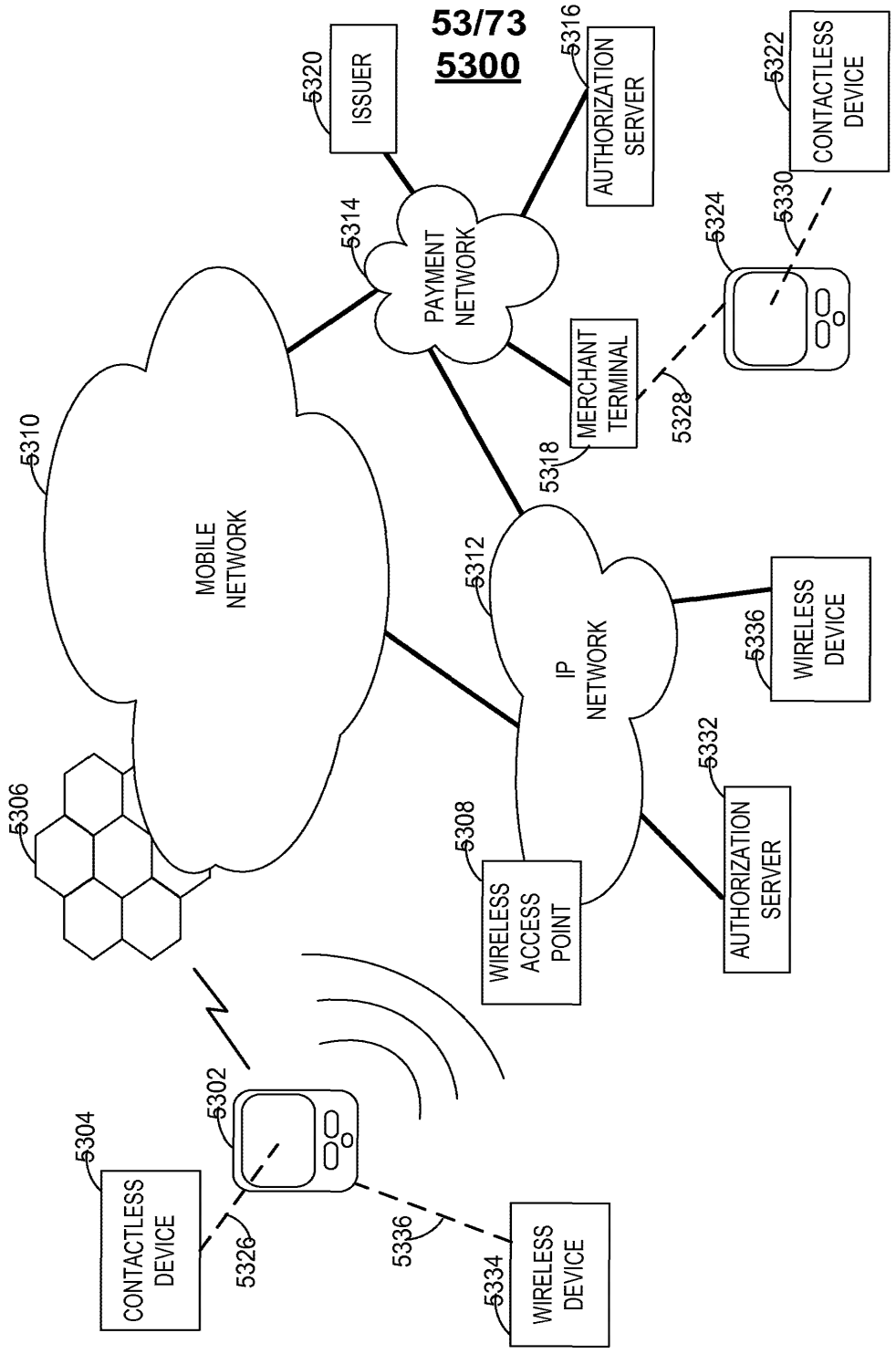

53/73
5300
5320
ISSUER
5316
AUTHORIZATION SERVER
5322
CONTACTLESS DEVICE
5314
PAYMENT NETWORK
5330
5324
5310
MOBILE NETWORK
MERCHANT TERMINAL
5328
5318
5312
IP NETWORK
5336
WIRELESS DEVICE
5306
5332
AUTHORIZATION SERVER
5308
WIRELESS ACCESS POINT
5302
5304
CONTACTLESS DEVICE
5326
5336
5334
WIRELESS DEVICE

FIG. 53

5400

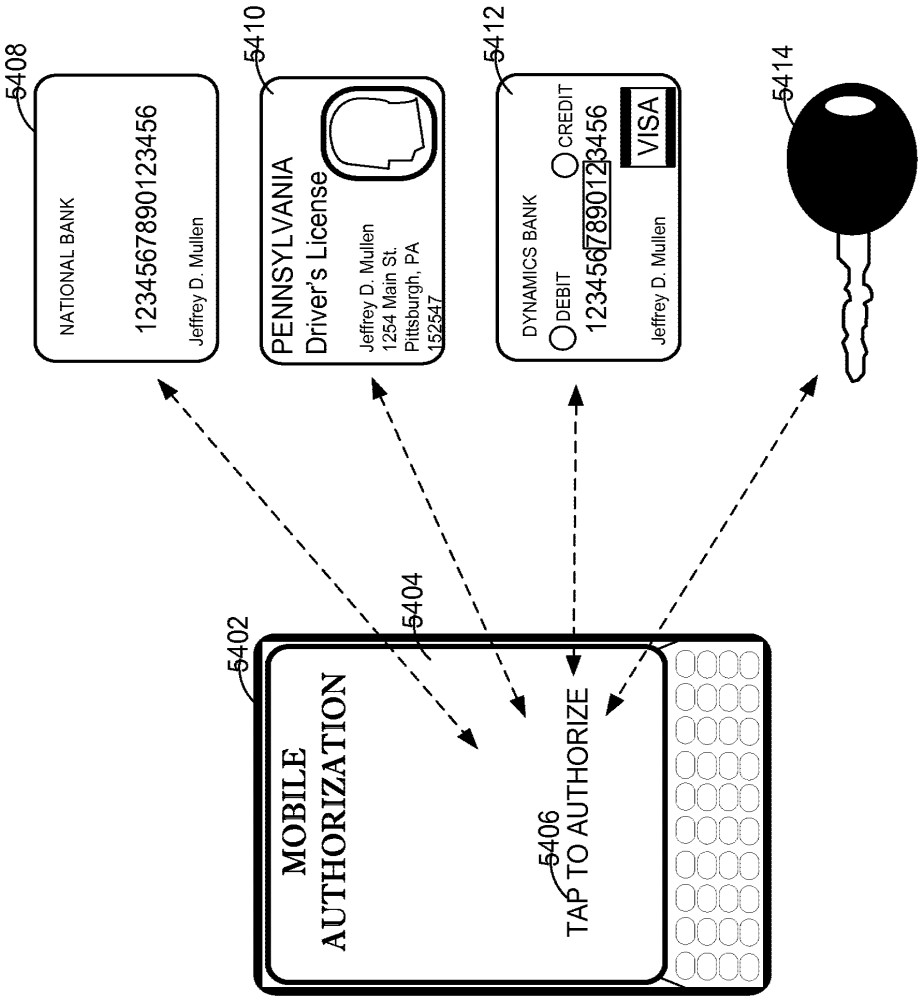

5408
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
5410
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
1254 Main St.
Pittsburgh, PA
152547
5412
DYNAMICS BANK
DEBIT
CREDIT
1234567890123456
VISA
Jeffrey D. Mullen
5414
5402
MOBILE
AUTHORIZATION
5404
5406
TAP TO AUTHORIZE

FIG. 54

5500

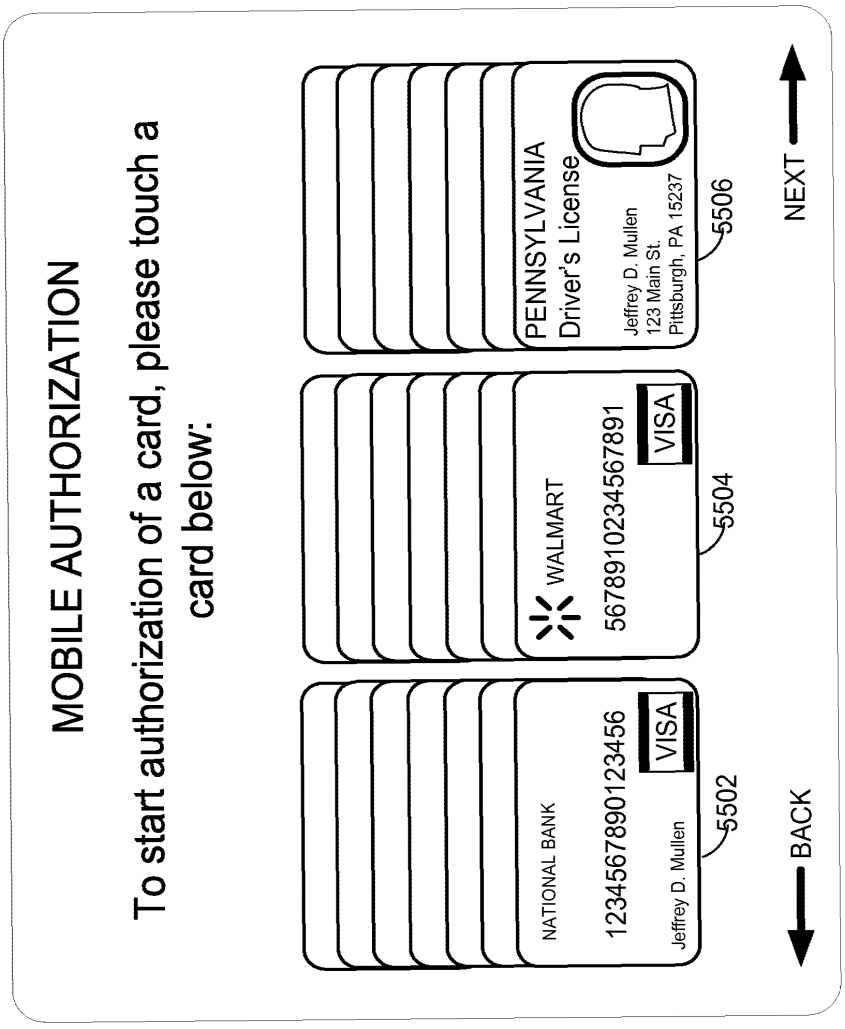

MOBILE AUTHORIZATION
To start authorization of a card, please touch a card below:
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
5502
WALMART
5678910234567891
VISA
5504
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
5506
BACK
NEXT

FIG. 55

5600

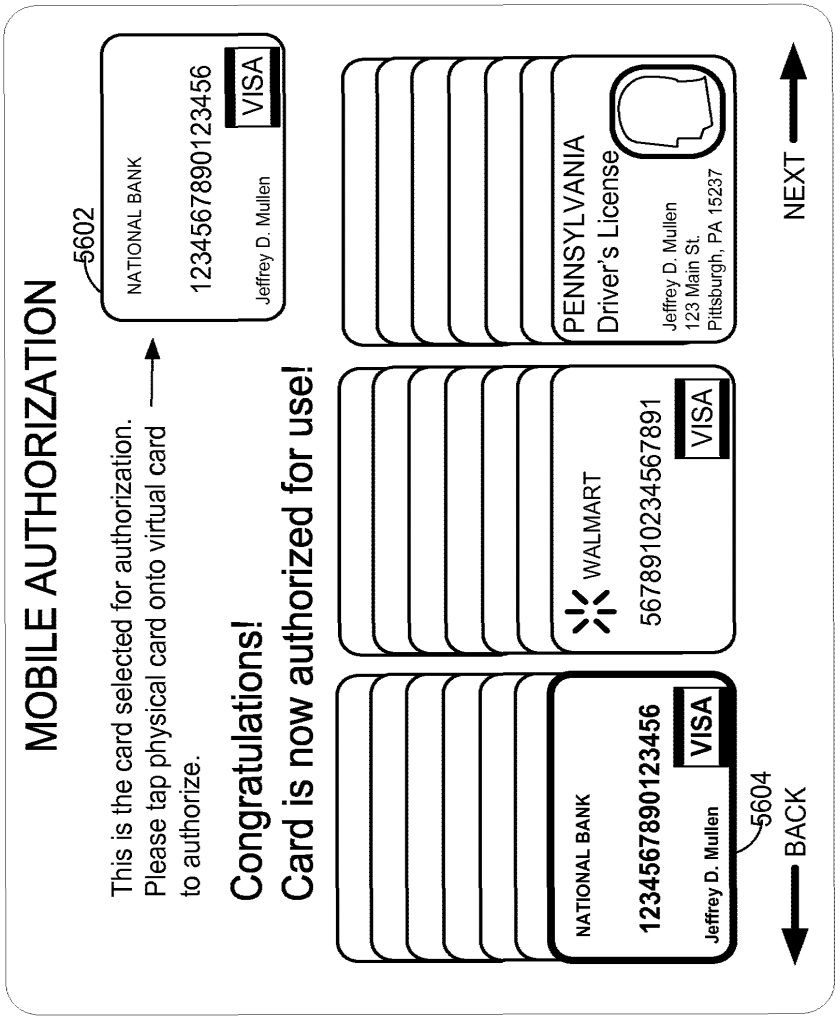

MOBILE AUTHORIZATION
This is the card selected for authorization.
Please tap physical card onto virtual card to authorize.
Congratulations!
Card is now authorized for use!
5602
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
WALMART
5678910234567891
VISA
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
5604
BACK
NEXT

FIG. 56

5700

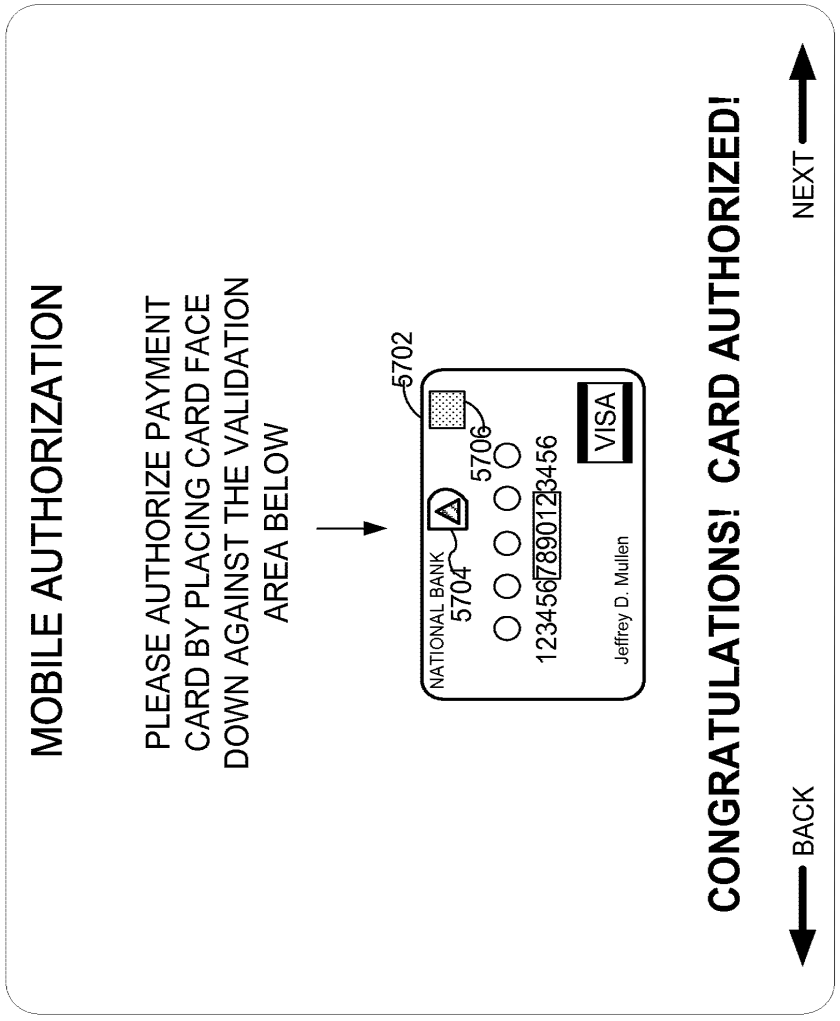

MOBILE AUTHORIZATION
PLEASE AUTHORIZE PAYMENT CARD BY PLACING CARD FACE DOWN AGAINST THE VALIDATION AREA BELOW
5702
NATIONAL BANK
5704
5706
1234567890123456
VISA
Jeffrey D. Mullen
CONGRATULATIONS! CARD AUTHORIZED!
BACK
NEXT

FIG. 57

5800

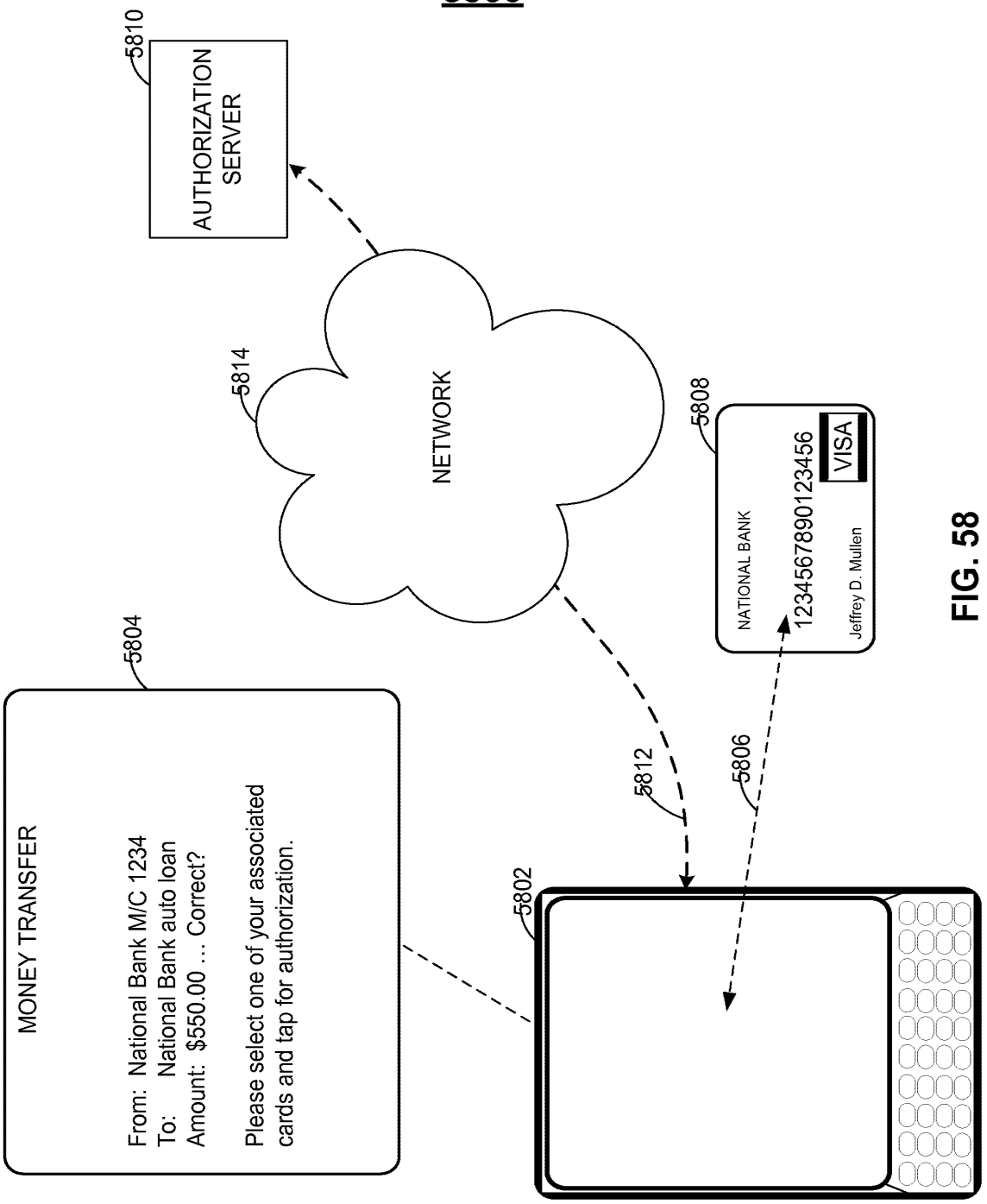

5810
AUTHORIZATION SERVER
5814
NETWORK
5808
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
5804
MONEY TRANSFER
From: National Bank M/C 1234
To: National Bank auto loan
Amount: $550.00 ... Correct?
Please select one of your associated cards and tap for authorization.
5812
5806
5802

FIG. 58

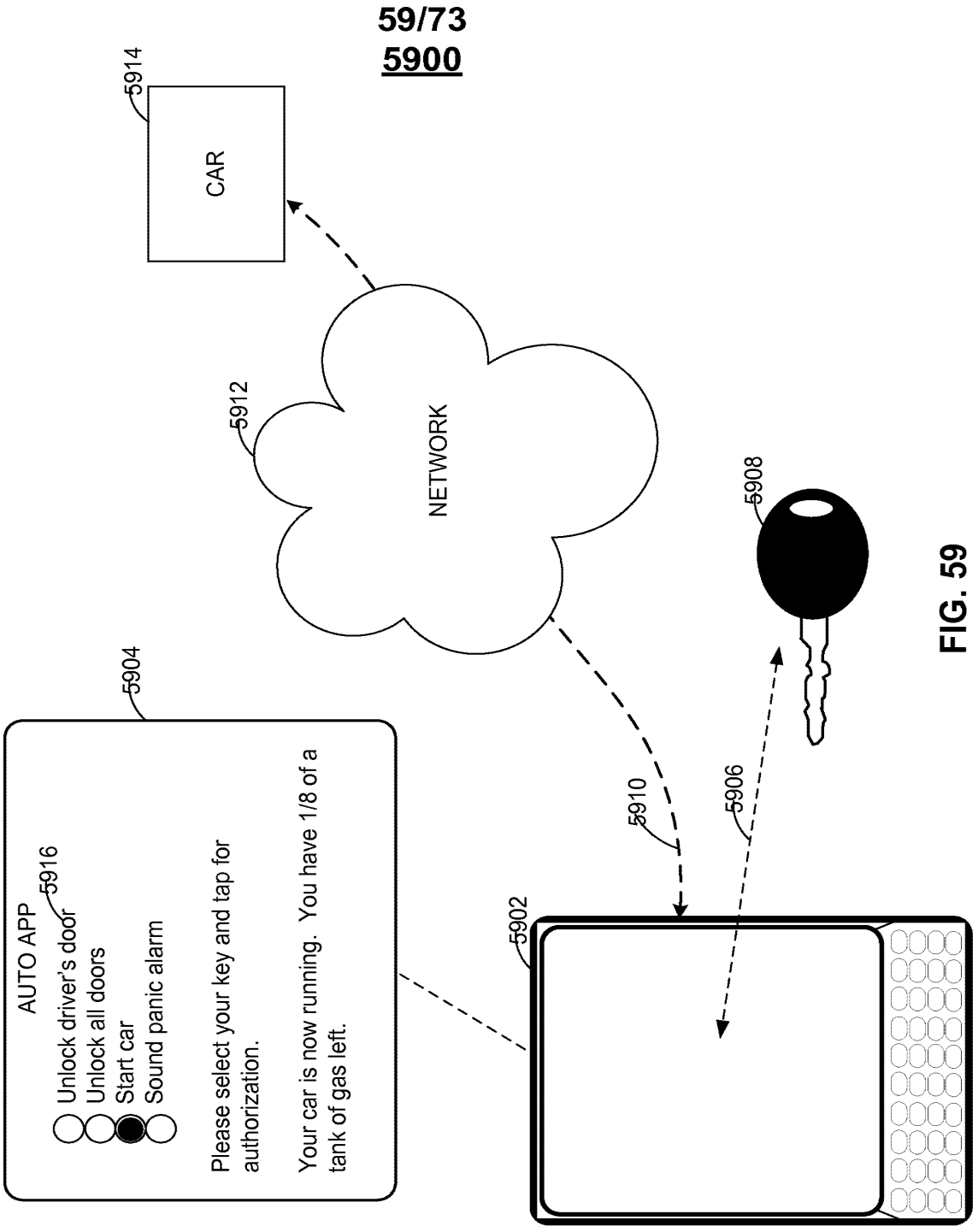

5900
5914
CAR
5912
NETWORK
5908
5904
AUTO APP
5916
Unlock driver's door
Unlock all doors
Start car
Sound panic alarm
Please select your key and tap for authorization.
Your car is now running. You have 1/8 of a tank of gas left.
5910
5906
5902

FIG. 59

60/73
6000

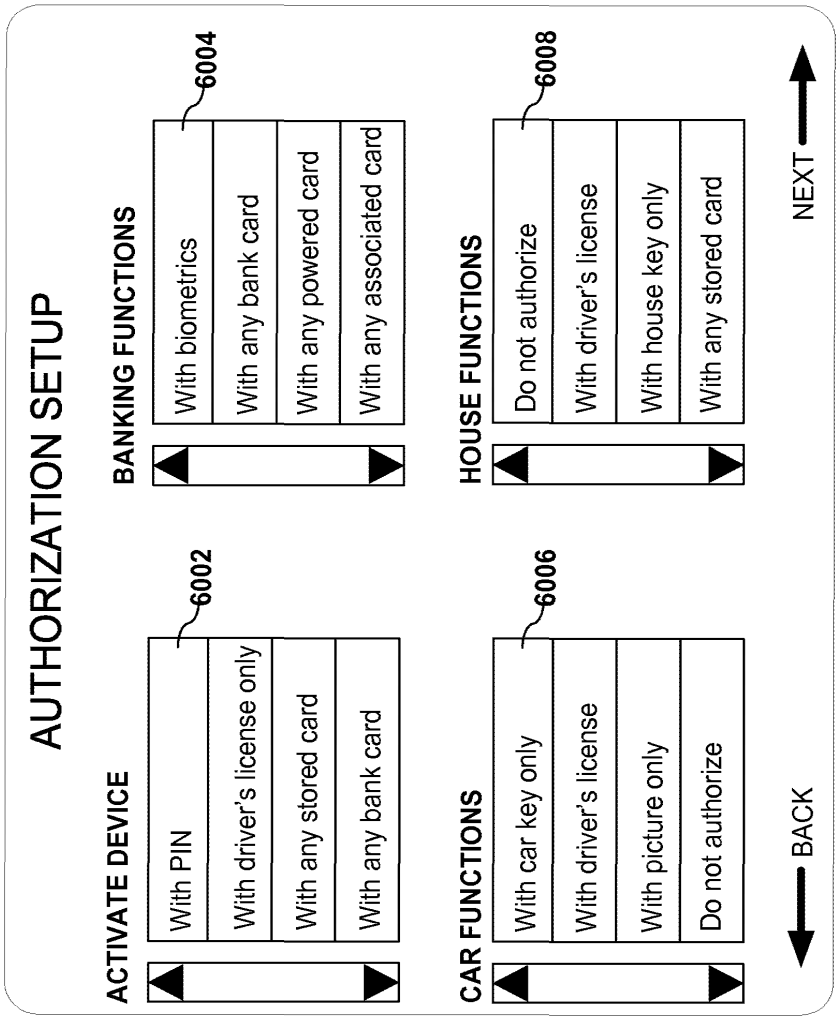


FIG. 60

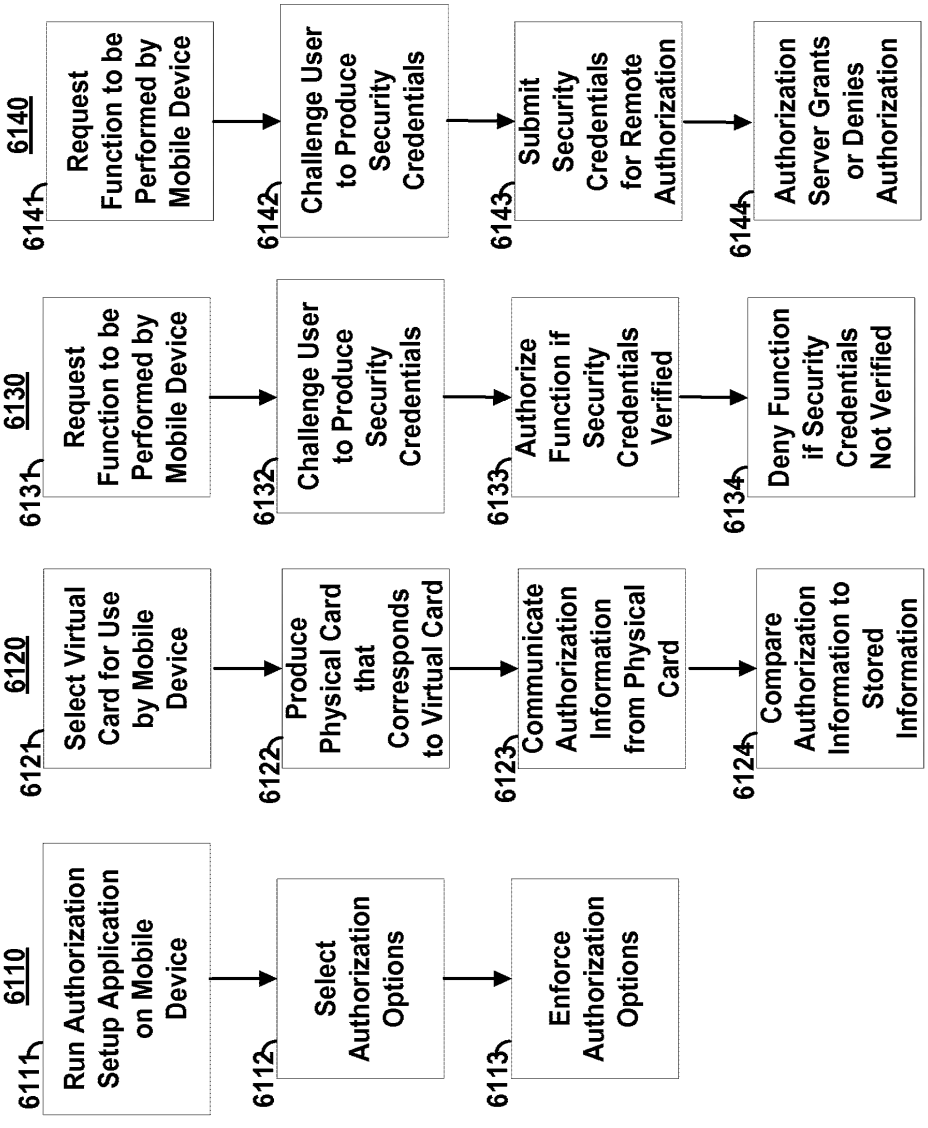

6110
6111
Run Authorization Setup Application on Mobile Device
6112
Select Authorization Options
6113
Enforce Authorization Options
6120
6121
Select Virtual Card for Use by Mobile Device
6122
Produce Physical Card that Corresponds to Virtual Card
6123
Communicate Authorization Information from Physical Card
6124
Compare Authorization Information to Stored Information
6130
6131
Request Function to be Performed by Mobile Device
6132
Challenge User to Produce Security Credentials
6133
Authorize Function if Security Credentials Verified
6134
Deny Function if Security Credentials Not Verified
6140
6141
Request Function to be Performed by Mobile Device
6142
Challenge User to Produce Security Credentials
6143
Submit Security Credentials for Remote Authorization
6144
Authorization Server Grants or Denies Authorization

FIG. 61

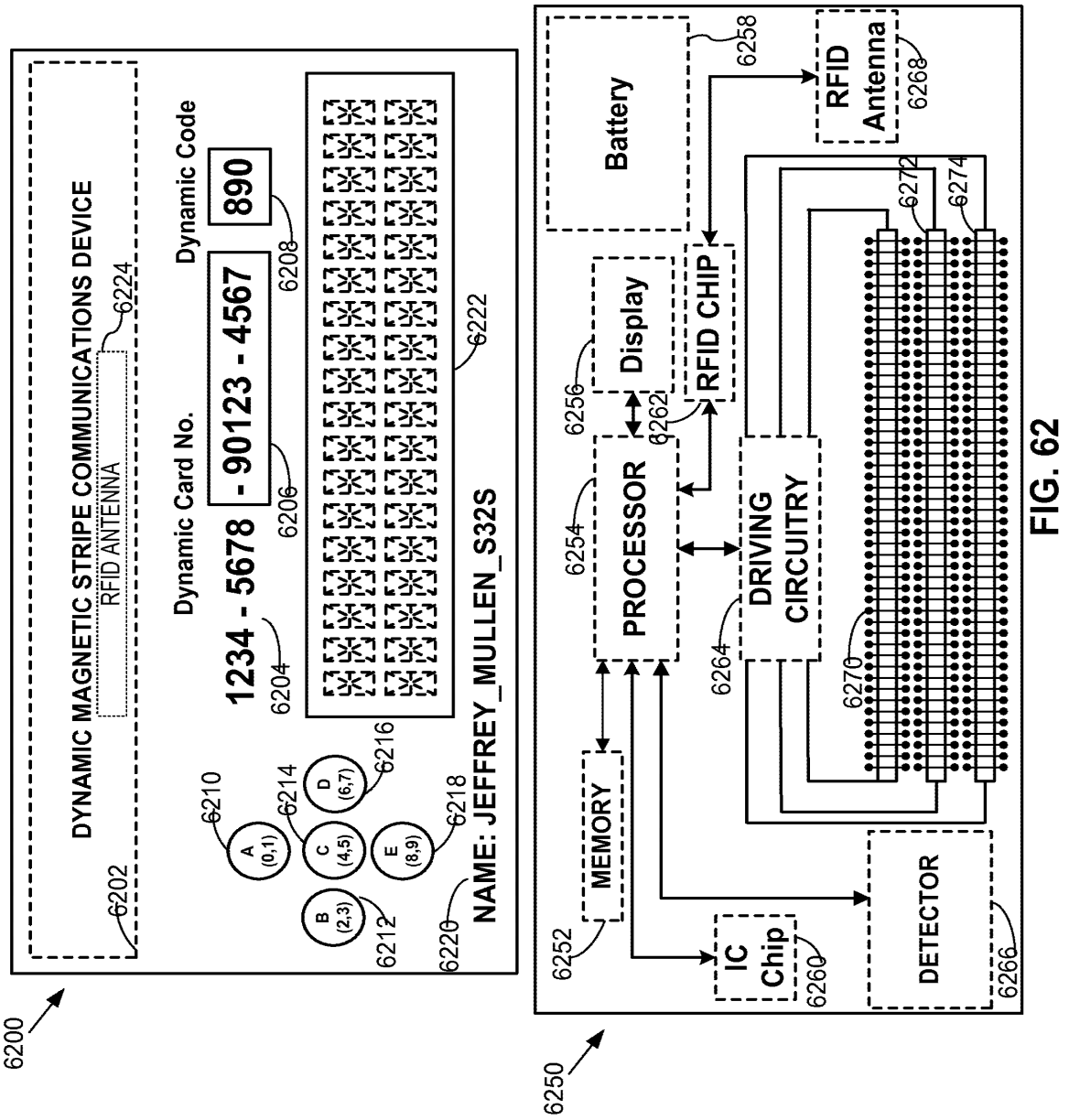

6200
DYNAMIC MAGNETIC STRIPE COMMUNICATIONS DEVICE
RFID ANTENNA
6224
6202
Dynamic Card No.
1234 - 5678 - 90123 - 4567
6204
6206
Dynamic Code
890
6208
6222
A (0,1)
B (2,3)
C (4,5)
D (6,7)
E (8,9)
6210
6212
6214
6216
6218
6220
NAME: JEFFREY_MULLEN_S32S
6250
Battery
6258
RFID Antenna
6268
6272
6274
Display
6256
RFID CHIP
6262
PROCESSOR
6254
DRIVING CIRCUITRY
6264
6270
MEMORY
6252
IC Chip
6260
DETECTOR
6266

FIG. 62

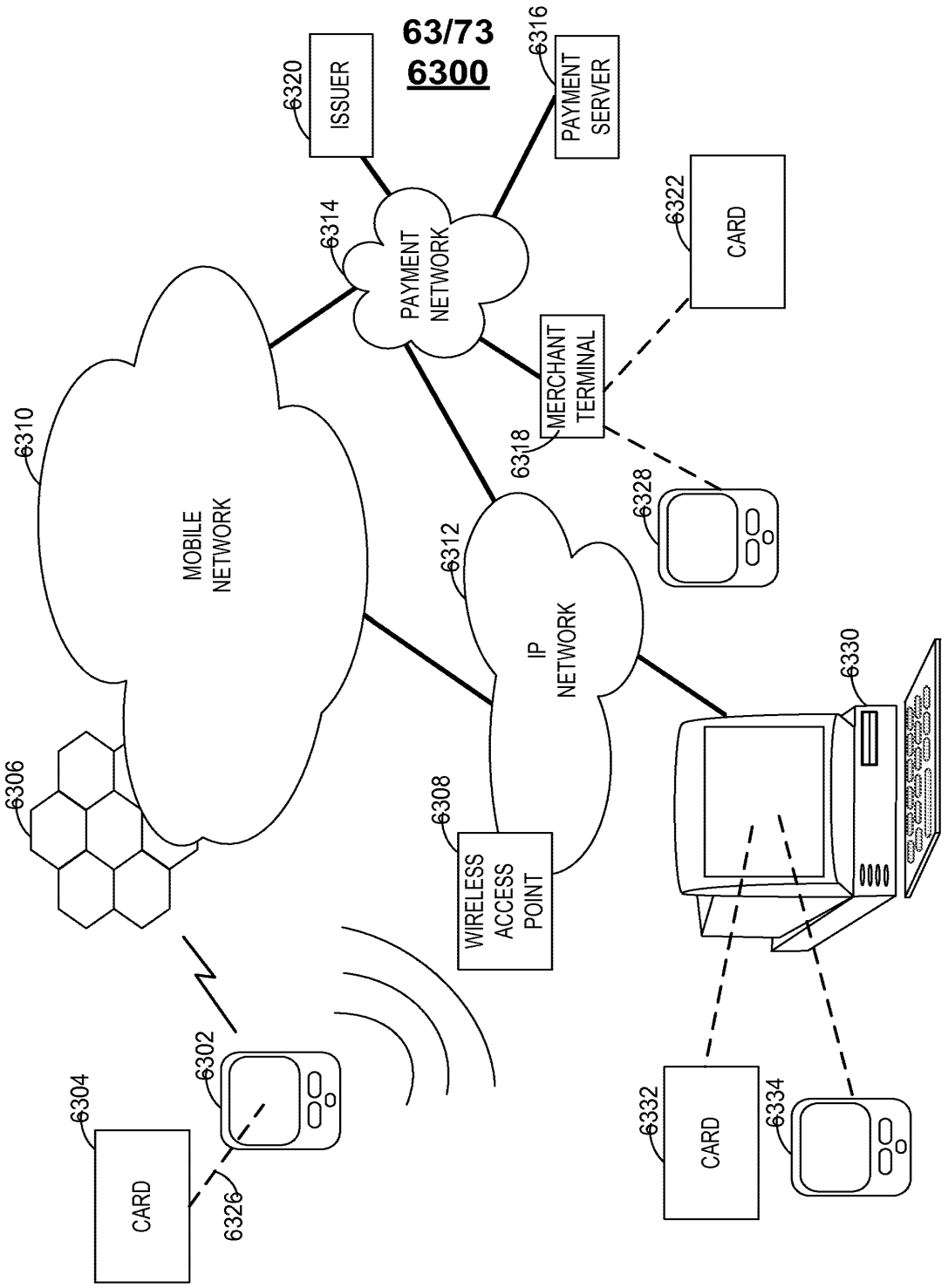

63/73
6300
6320
ISSUER
6316
PAYMENT SERVER
6314
PAYMENT NETWORK
6322
CARD
6310
MOBILE NETWORK
MERCHANT TERMINAL
6318
6328
6312
IP NETWORK
6330
6306
6308
WIRELESS ACCESS POINT
6302
6304
CARD
6326
6332
CARD
6334

FIG. 63

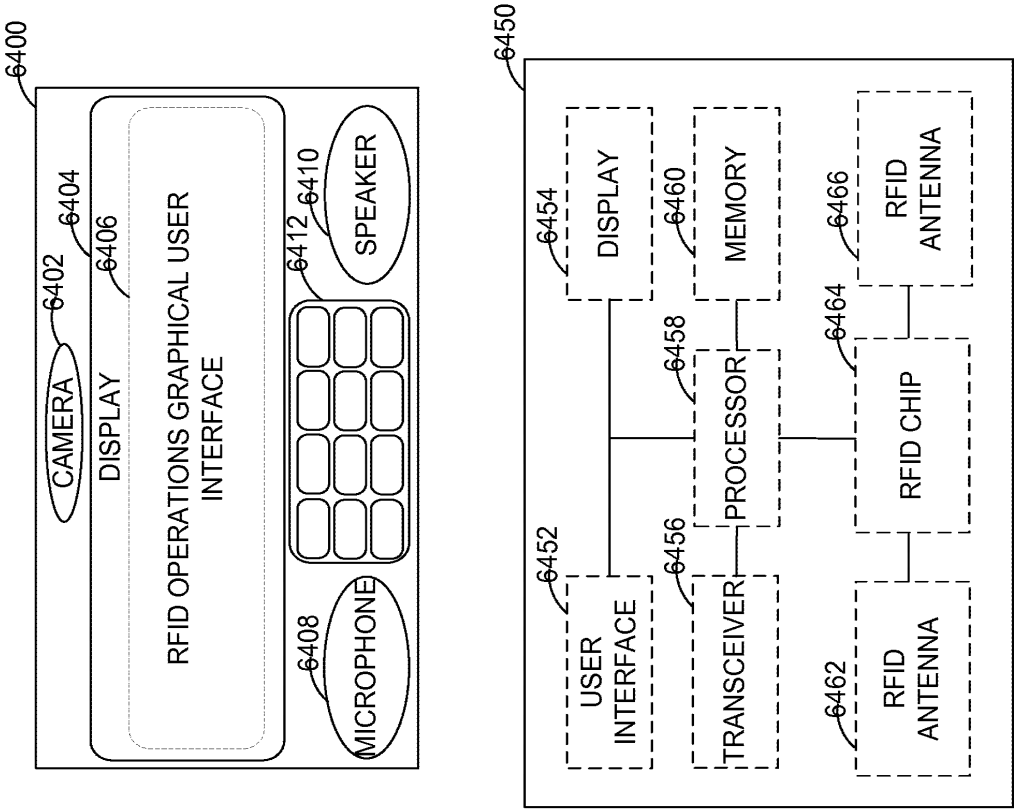

6400
CAMERA
6402
DISPLAY
6404
RFID OPERATIONS GRAPHICAL USER INTERFACE
6406
6408
MICROPHONE
6410
SPEAKER
6412
6450
USER INTERFACE
6452
DISPLAY
6454
TRANSCEIVER
6456
PROCESSOR
6458
MEMORY
6460
RFID ANTENNA
6462
RFID CHIP
6464
RFID ANTENNA
6466

FIG. 64

6500

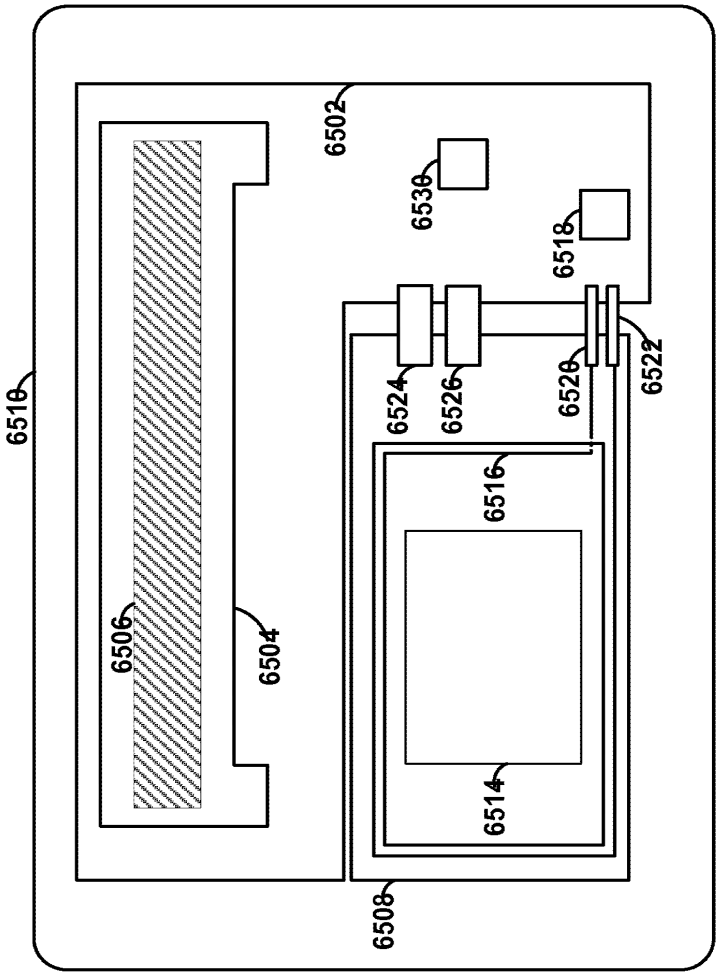

6502
6530
6518
6510
6524
6526
6528
6522
6516
6506
6504
6514
6508

FIG. 65

6600

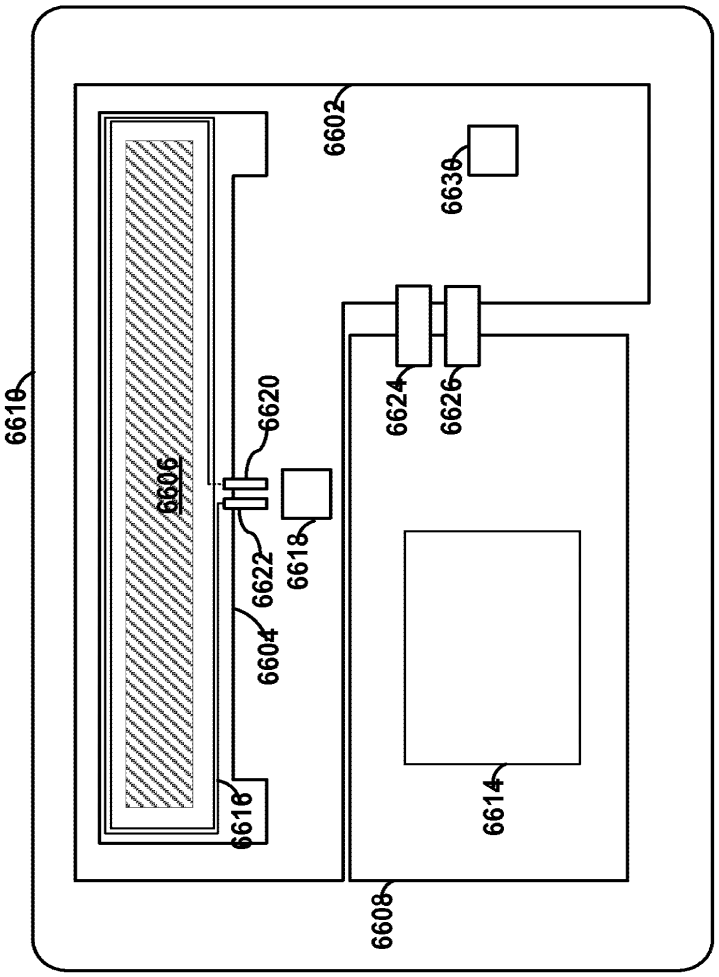

6602
6638
6610
6620
6624
6626
6606
6618
6622
6604
6616
6614
6608

FIG. 66

67/73
6700

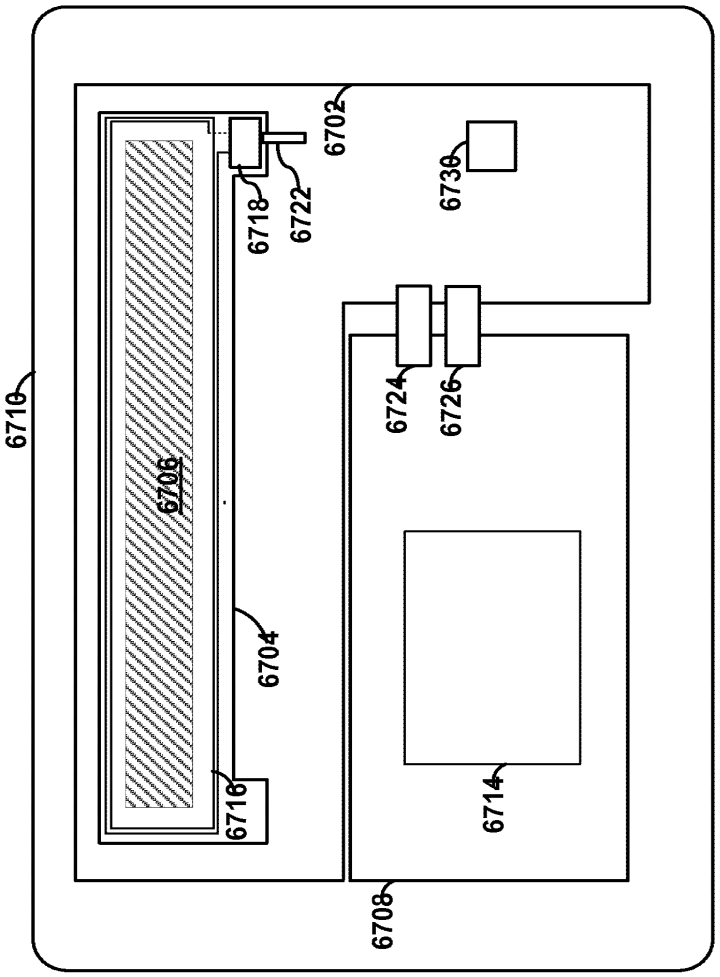


FIG. 67

68/73
6800

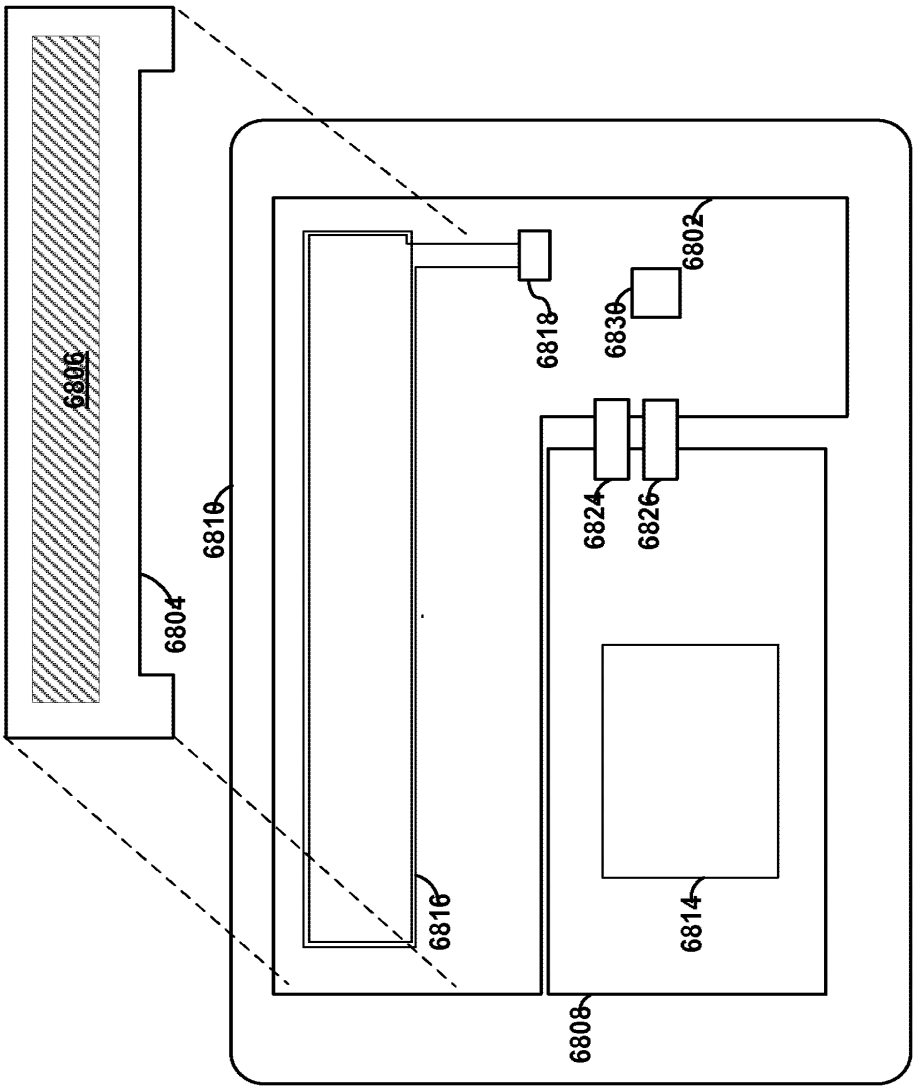


FIG. 68

69/73
6900

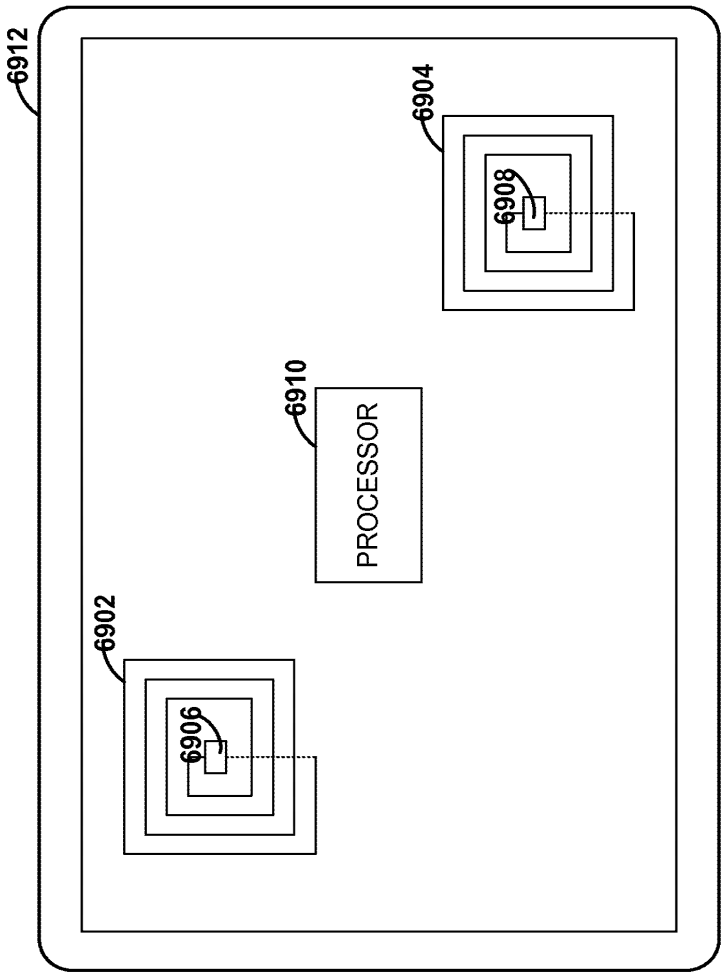


FIG. 69

70/73
7000

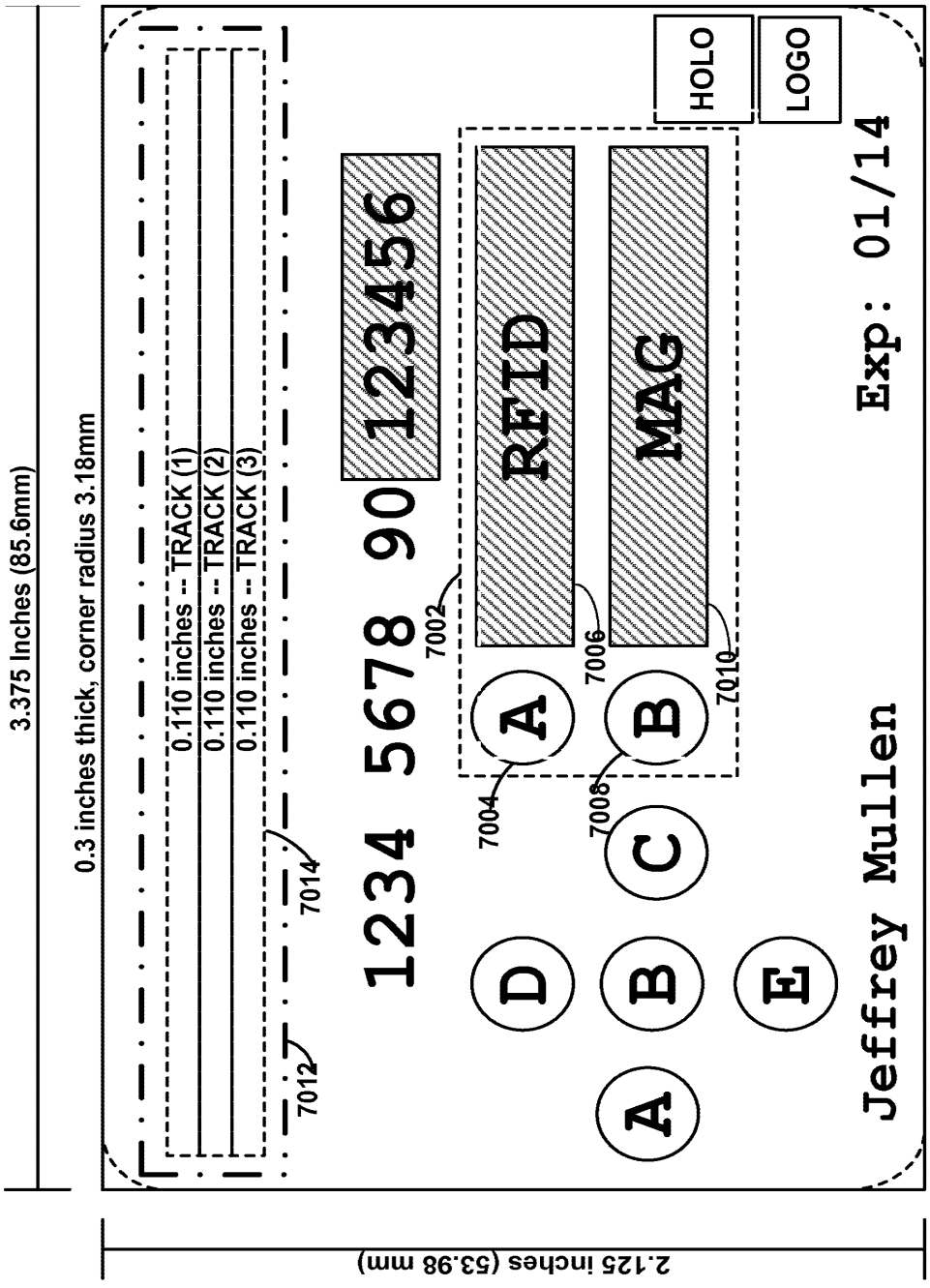


FIG. 70

71/73
7100

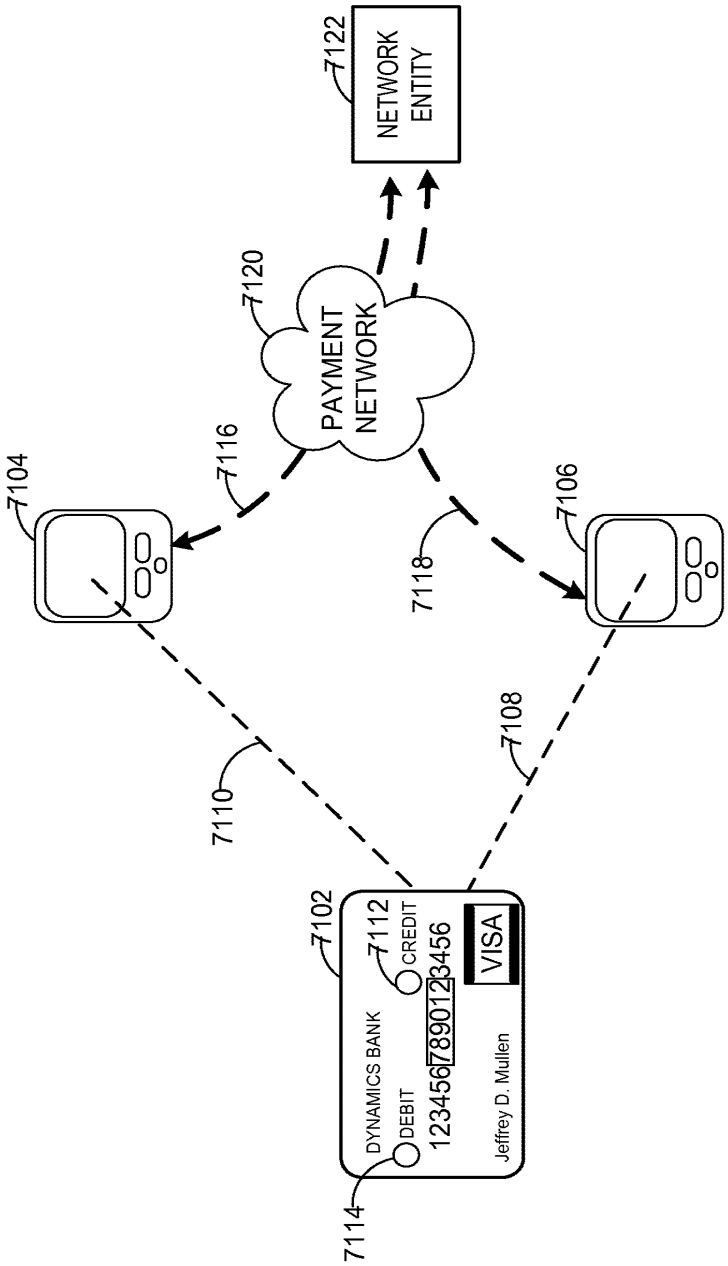


FIG. 71

72/73
7200

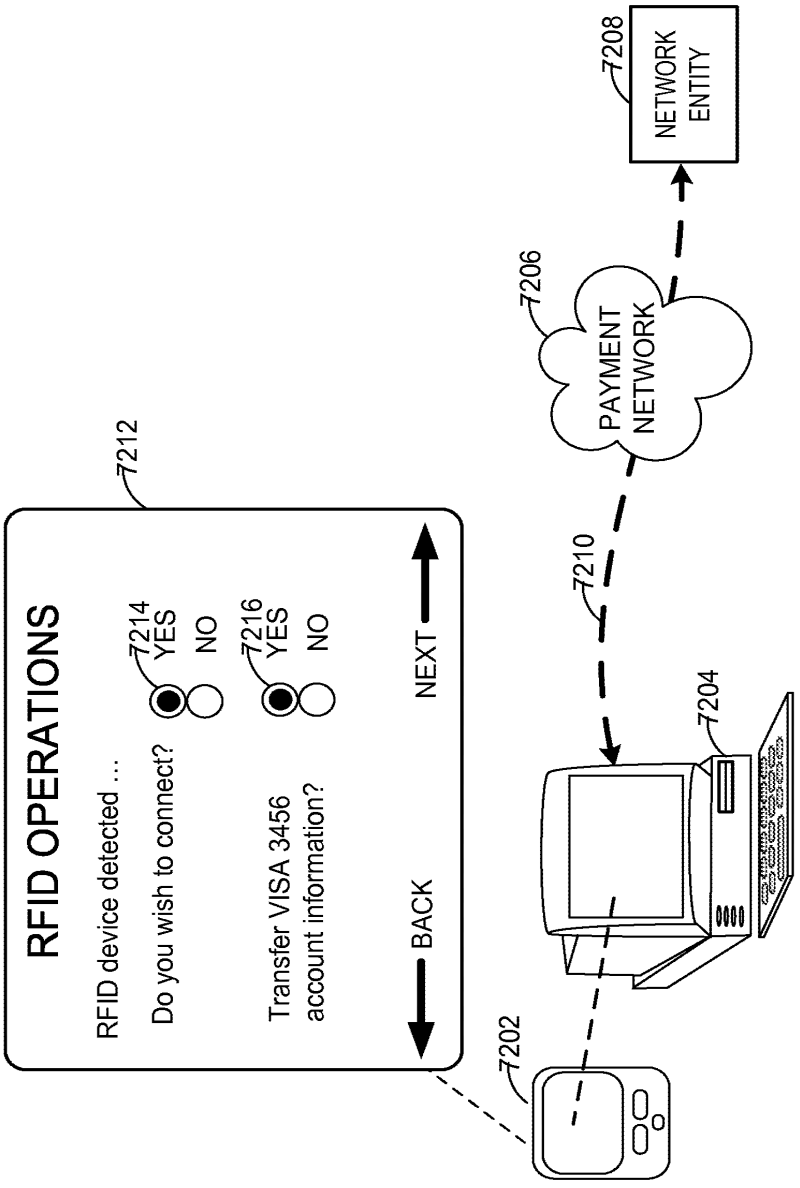


FIG. 72

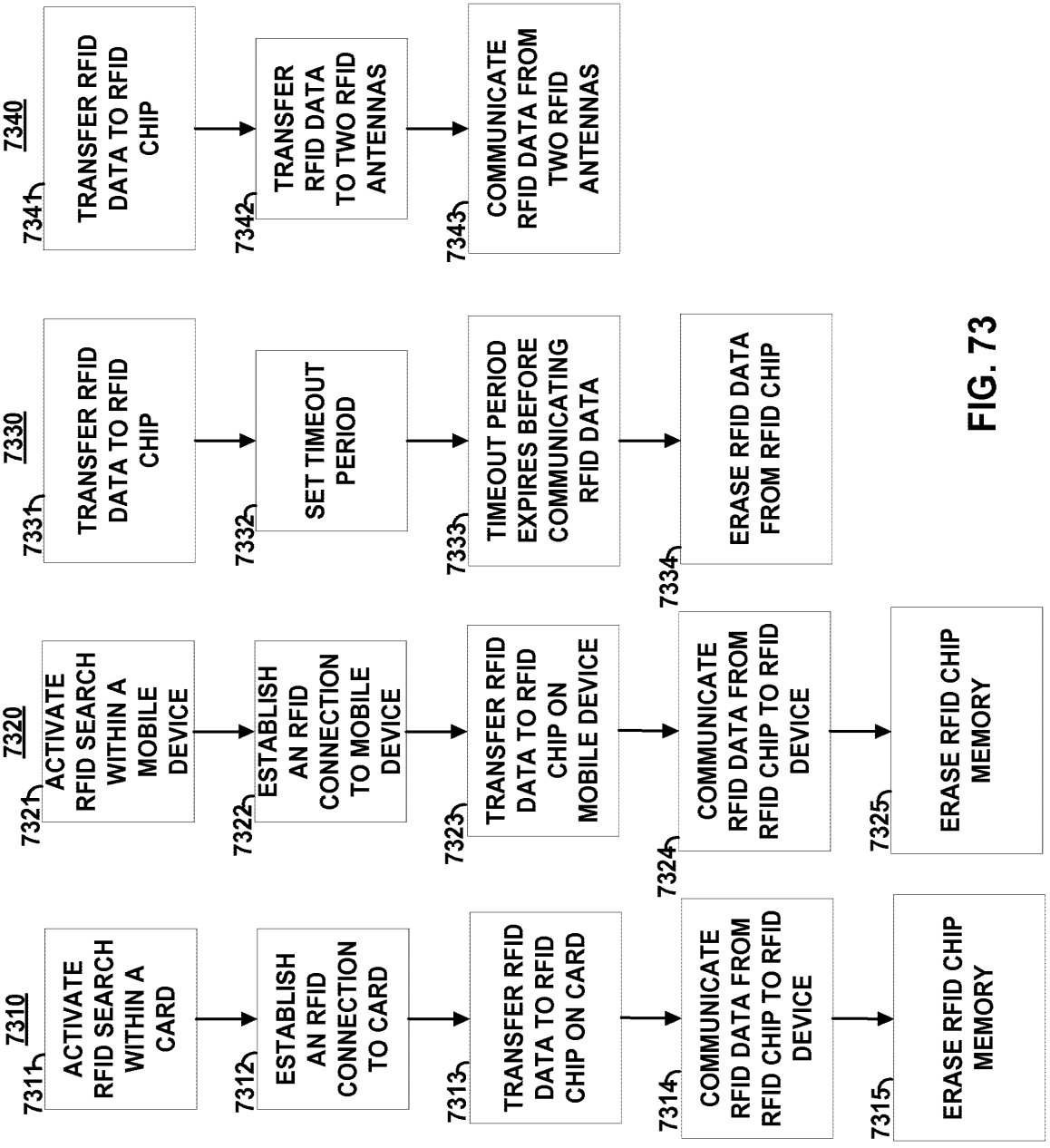

7310
7311
ACTIVATE RFID SEARCH WITHIN A CARD
7312
ESTABLISH AN RFID CONNECTION TO CARD
7313
TRANSFER RFID DATA TO RFID CHIP ON CARD
7314
COMMUNICATE RFID DATA FROM RFID CHIP TO RFID DEVICE
7315
ERASE RFID CHIP MEMORY
7320
7321
ACTIVATE RFID SEARCH WITHIN A MOBILE DEVICE
7322
ESTABLISH AN RFID CONNECTION TO MOBILE DEVICE
7323
TRANSFER RFID DATA TO RFID CHIP ON MOBILE DEVICE
7324
COMMUNICATE RFID DATA FROM RFID CHIP TO RFID DEVICE
7325
ERASE RFID CHIP MEMORY
7330
7331
TRANSFER RFID DATA TO RFID CHIP
7332
SET TIMEOUT PERIOD
7333
TIMEOUT PERIOD EXPIRES BEFORE COMMUNICATING RFID DATA
7334
ERASE RFID DATA FROM RFID CHIP
7340
7341
TRANSFER RFID DATA TO RFID CHIP
7342
TRANSFER RFID DATA TO TWO RFID ANTENNAS
7343
COMMUNICATE RFID DATA FROM TWO RFID ANTENNAS

FIG. 73

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US20 12/037237

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/02 (201 2.01)
USPC - 705/41
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06Q 30/06, 40/00, 40/02 (2012.01)
USPC - 455/41 .1, 705/39, 40, 4 1, 42

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Google Patents, Google.com

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	**US 2009/0210308 A 1 (TOOMER et al) 20 August 2009 (20.08.2009) entire document**	**1, 3-1 1, 81**
X	**US 2009/019181 1 A 1 (GRIFFIN et al) 30 July 2009 (30.07.2009) entire document**	**2, 12-21, 82**
A	**US 2010/0304670 A 1 (SHUO) 02 December 2010 (02.12.2010) entire document**	**1-21 , 81-82**
A	**US 2010/0023449 A 1 (SKOWRONEK et al) 28 January 2010 (28.01.2010) entire document**	**1-21, 81-82**
A	**US 2009/0170432 A 1 (LORTZ) 02 July 2009 (02.07.2009) entire document**	**1-21 , 81-82**
A	**US 2010/0153269 A 1 (MCCABE) 17 June 2010 (17.06.2010) abstract, Fig. 1-2, paragraphs 13, 15, 30-31, 36-40, 47.**	**1-21, 81-82**

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 September 2012	**1 6 OCT 2012**
Name and mailing address of the ISA/US **Mail Stop PCT, Attn: ISA/US, Commissioner for Patents** **P.O. Box 1450, Alexandria, Virginia 22313-1450** Facsimile No. **571-273-3201**	Authorized officer: **Blaine R. Copenheaver** **PCT Helpdesk: 571-272-4300** **PCT OSP: 571-272-7774**

Form PCT/ISA /**210** (second sheet) (July **2009**)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/037237

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-21 , 81-82

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

IPR2025-01150
Apple EX1071 Page 377

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US20 12/037237

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-21, 81-82, drawn to a method and system comprising accessing a network using a mobile device, selecting an object for purchase from said network, communicating payment information/target account information to a second device, and completing a purchase transaction/coordinating a money transfer.
Group II, claims 22-41, 83, drawn to a method and system comprising creating a mobile wallet of virtual cards within a memory of a mobile device from communicated information, and selecting one of said virtual cards to complete a purchase transaction.
Group III, claims 42-61, 84, drawn to a method and system comprising executing an application on a processor of a mobile device to perform a function, communicating information to said mobile device, confirming said communicated information matches at least a portion of predetermined information, and executing said function from said mobile device based on said confirmation.
Group IV, claims 62-78, drawn to a card comprising a second board including a processor, wherein first data is transferred from a processor to a first RFID chip via conductive terminals between first and second boards and wherein said first data is communicated from said first RFID chip to a first RFID communication channel via said first RFID antenna.
Group V, claims 79-80, drawn to a method comprising communicating second data from a device to a reader via a second RFID communication channel, receiving first and second data via said reader and avoiding collisions between said first and second data within said reader.

The inventions listed as Groups I, II, III, IV and IV do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: a method and system comprising accessing a network using a mobile device, selecting an object for purchase from said network, communicating payment information/target account information to a second device as claimed therein is not present in the invention of Groups II, III, IV or V. The special technical feature of the Group II invention: a method and system comprising creating a mobile wallet of virtual cards within a memory of a mobile device from communicated information, and selecting one of said virtual cards as claimed therein is not present in the invention of Groups I, III, IV or V. The special technical feature of the Group III invention: a method and system comprising executing an application on a processor of a mobile device to perform a function, confirming that communicated information matches at least a portion of predetermined information, and executing said function from said mobile device based on said confirmation as claimed therein is not present in the invention of Groups I, II, IV or V. The special technical feature of the Group IV invention: a card comprising a second board including a processor, wherein first data is transferred from a processor to a first RFID chip via conductive terminals between first and second boards as claimed therein is not present in the invention of Groups I, II, III or V. The special technical feature of the Group V invention: a method comprising communicating second data from a device to a reader via a second RFID communication channel, receiving first and second data via said reader and avoiding collisions between said first and second data within said reader as claimed therein is not present in the invention of Groups I, II, III or IV.

Groups I, II, III, IV and V lack unity of invention because even though the inventions of these groups require the technical feature of a method, system and card comprising establishing a contactless communication channel between a physical card and a mobile device through a first board including a first RFID chip and a first RFID antenna; communicating payment/source account information from a payment card to a mobile device using a contactless communication channel wherein first data is communicated from said first RFID chip to a first RFID communication channel visa said first RFID antenna; completing a purchase transaction/coordinating a money transfer, this technical feature is not a special technical feature as it does not make a contribution over the prior art in view of US 2010/0153269 A1 (MCCABE) 17 June 2010 (17.06.2010), abstract. Fig. 1-2, paragraphs 13, 15, 30-31, 36-40, 47.

Since none of the special technical features of the Group I, II, III, IV or V inventions are found in more than one of the inventions, unity of invention is lacking.

IPR2025-01150
Apple EX1071 Page 378

Electronic Acknowledgement Receipt	
EFS ID:	45256827
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Anthony C. Murabito/Mina Oliveri
Filer Authorized By:	Anthony C. Murabito
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Receipt Date:	17-MAR-2022
Filing Date:	16-NOV-2021
Time Stamp:	18:20:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	WYAT-0002USD1C1C1C1C1C_IDS_03-17-2022.pdf	612514 427eed86832963839eaf594865df5c2d49f6ac57	no	5
Warnings:					

Information:					
2	Foreign Reference	WO2012154915A1.pdf	2516187 c1c7bbd68df08bfa9b406ffb565ca8064c32717d	no	292
Warnings:					
Information:					
			Total Files Size (in bytes):	3128701	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 17/528,073

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	14 minus 20 =	*	x 50 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*	x 240 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	830		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2876	910	WYAT-0002.USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

UPDATED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

OC000000152365388

Date Mailed: 03/21/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

David WYATT, San Jose, CA;

Applicant(s)

Virtual Electric Inc., San Jose, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

IPR2025-01150
Apple EX1071 Page 382

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: 06/30/2022
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

IPR2025-01150
Apple EX1071 Page 383

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01150
Apple EX1071 Page 385

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

CORRECTED ADS FORM

Application Number	17528073
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Inventor Information

****If no data is shown, no data has been corrected****

	Data of Record	Updated Data
Order Number		
Name		
Residence Information		
Residency		
City		
State		
Country of Residence		
Mailing Address of Inventor		
Address 1		
Address 2		
City,State/Province, Postal Code		
Country		

Corrected ADS 1.0

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

Application Information

	Data of Record	Updated Data
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	
Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C	
Entity Type	Small	

Domestic Benefit/National Stage Information

****If no data is shown, no data has been corrected****

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121,365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S. C. 119(e) or 120, and 37 CFR 1.78(a).

		Data of Record	Updated Data
	Prior Application Status		
	Application Number		
	Continuity Type		
	Prior Application Number		
	Filing Date (YYYY-MM-DD)		
	Patent Number		
	Issue Date (YYYY-MM-DD)		

Foreign Priority Information

IPR2025-01150
Apple EX1071 Page 387

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

****If no data is shown, no data has been corrected****

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

		Data of Record	Updated Data
	Application Number		
	Country		
	Filing Date		
	Access Code		

Applicant Information

****If no data is shown, no data has been corrected****
Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

	Data of Record	Updated Data
Applicant Type	ASG	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is		
Name of the Deceased or Legally Incapacitated Inventor		
Applicant is an Organization	Yes	
Name		
Organization Name	~~Virtual Electric Inc.~~	CARDWARE, INC
Address 1		2470 CAMROSE AVE.
Address 2		

Corrected ADS 1.0

City,State/Province,Postal Code	~~San Jose CA~~	SAN JOSE CA 95130
Country		US
Phone Number		
Fax Number		
Email Address		

Assignee Information including Non-Applicant Assignee Information

****If no data is shown, no data has been corrected****
Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office

	Data of Record	Updated Data
Order		
Applicant is an Organization		
Name		
Organization Name		
Mailing Address		
Address 1		
Address 2		
City,State/Province,Postal Code		
Country		
Phone Number		
Fax Number		
Email Address		

Corrected ADS 1.0

Signature

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Jose S. Garcia/	Registration Number	43628
First Name	Jose	Last Name	Garcia

IPR2025-01150
Apple EX1071 Page 390

Doc Code: R46C.REQ
Document Description: Request under 37 CFR 1.46(c) to correct, update or change the applicant.

PTO/AIA/41 (04-15)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST TO CORRECT OR UPDATE THE NAME OF THE APPLICANT UNDER 37 CFR 1.46(c)(1), OR CHANGE THE APPLICANT UNDER 37 CFR 1.46(c)(2)
(FOR USE ONLY IN APPLICATIONS FILED ON OR AFTER SEPTEMBER 16, 2012)

Application Number	17/528,073
Filing Date	11-16-2021
First Named Inventor	David WYATT
Art Unit	2887
Examiner Name	
Practitioner Docket Number	WYAT-0002USD1C1C1C1C1C1

To: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Applicant hereby **requests that the name of the applicant be corrected or updated under 37 CFR 1.46(c)(1), or that the applicant be changed under 37 CFR 1.46(c)(2),** in the above-identified application. **Requests under 37 CFR 1.46(c)(1) or (c)(2) cannot be submitted after payment of the issue fee or if the application has been patented.**

Please check the applicable box(es) below.

☐ 1. This request is to **correct or update the name of the applicant** (**under 37 CFR 1.46(c)(1)**) and includes:

☐ An application data sheet (ADS) in accordance with 37 CFR 1.76(c) with the corrected or updated information shown with markings (*e.g.*, underlining for insertions, strikethrough for deletions). A Corrected Web-based ADS may be used.

Note: Requests under 37 CFR 1.46(c)(1) may be filed to correct typographical errors in the name of the § 1.46 applicant, or for updating the name of the § 1.46 applicant (*i.e.*, where there is no change in the applicant itself but just in the applicant's name). See the Manual of Patent Examining Procedure (MPEP) section 605.01.

■ 2. This request is to **change the applicant** (**under 37 CFR 1.46(c)(2)**) and includes:

■ An application data sheet (ADS) in accordance with 37 CFR 1.76(c) that identifies the changes with proper markings (underlining for insertions and strikethrough for deletions). A Corrected Web-based ADS may be used.

■ A Statement Under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent). See MPEP 325.

I am the

☐ applicant* ☐ attorney or agent of record Registration number _____ ■ attorney or agent acting under 37 CFR 1.34 Registration number 43628

Signature /Jose S. Garcia/
Typed or printed name Jose S. Garcia
Date 4/7/2022

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. *Juristic entities must be represented by a patent practitioner (See 37 CFR 1.31, applicable to any paper filed on or after September 16, 2012 that is presented on behalf of a juristic entity, regardless of application filing date). Submit multiple forms if more than one signature is required, see below**.

☐ ** Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.36. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: CARDWARE, INC

Application No./Patent No.: 17/528,073 Filed/Issue Date: 11-16-2021

Titled: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

CARDWARE, INC, a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: DAVID WYATT To: CARDWARE, INC

   The document was recorded in the United States Patent and Trademark Office at

   Reel 058892, Frame 0036, or for which a copy thereof is attached.

2. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Jose S. Garcia/	4/7/2022
Signature	Date
Jose S. Garcia	attorney for CARDWARE, INC
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	45418179
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Jose S. Garcia
Filer Authorized By:	
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Receipt Date:	07-APR-2022
Filing Date:	16-NOV-2021
Time Stamp:	12:28:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet to update/ correct info	CorrectedADS.pdf	100182 ed1691b6999d3775ccd7d3f96aa1fd4e9586e24d	no	5

Warnings:

Information:					
2	Request for Corrected Filing Receipt	WYAT-0002USD1C1C1C1C1C1_aia0041_Request_to_Change_Applicant.pdf	212116 af2eeefc8fd99dad1b6d78ec1f20b7b21570860e	no	2
Warnings:					
Information:					
3	Assignee showing of ownership per 37 CFR 3.73	WYAT-0002USD1C1C1C1C1C1_aia0096_Statement_under_3_73c.pdf	195895 c3dd1ee68f417b0640ad3e91d2850929ec52aa15	no	3
Warnings:					
Information:					
			Total Files Size (in bytes):	508193	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	17/528,073
Filing Date	11-16-2021
First Named Inventor	David WYATT
Title	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
Art Unit	2887
Examiner Name	
Attorney Docket Number	WYAT-0002USD1C1C1C1C1C1

SIGNATURE of Applicant or Patent Practitioner

Signature	/Jose S. Garcia/	Date (Optional)	4-8-2022
Name	Jose S. Garcia	Registration Number	43628
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 136197

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

CARDWARE, INC

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	D. Wyatt	Date (Optional)	March 29th, 2022
Name	David Wyatt		
Title	CEO/CTO/President		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	45432426
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Jose S. Garcia
Filer Authorized By:	
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Receipt Date:	08-APR-2022
Filing Date:	16-NOV-2021
Time Stamp:	15:28:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	WYAT-0002USD1C1C1C1C1C1_AIA_82_POA_to_MHB_Signed.pdf	345136 4c387207c72c0ac4445a2f2cf86c9e7239bf6721	no	2

Warnings:

Information:	
Total Files Size (in bytes):	345136

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2887	910	WYAT-0002.USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

OC000000133052809

Date Mailed: 04/11/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

David WYATT, San Jose, CA;

Applicant(s)

CARDWARE, INC., San Jose, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

IPR2025-01150
Apple EX1071 Page 402

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: 06/30/2022
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

IPR2025-01150
Apple EX1071 Page 403

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01150
Apple EX1071 Page 405

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C

CONFIRMATION NO. 4809

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

POA ACCEPTANCE LETTER

OC000000133095064

Date Mailed: 04/12/2022

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/08/2022.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ttran/

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/25 PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION AND TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	17528073
Filing Date	16-Nov-2021
First Named Inventor	David WYATT
Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
CARDWARE, INC	100 %

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

16854829 filed on 04/21/2020

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

9760884

9430765

9224083

9022286

10810579

10628820

10339520

10013693

11176538

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicants claims the following fee status:

◉ Small Entity

○ Micro Entity

○ Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

- (●) An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

  Registration Number 43628

- ( ) A sole inventor
- ( ) A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application
- ( ) A joint inventor; all of whom are signing this request

Signature	/Jose S. Garcia/
Name	Jose S. Garcia

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal	
Application Number:	17528073
Filing Date:	16-Nov-2021
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Filer:	Jose S. Garcia
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	2814	1	170	170
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**170**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 17528073

Filing Date: 16-Nov-2021

Applicant/Patent under Reexamination: WYATT

Electronic Terminal Disclaimer filed on April 14, 2022

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt	
EFS ID:	45473766
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Jose S. Garcia
Filer Authorized By:	
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Receipt Date:	14-APR-2022
Filing Date:	16-NOV-2021
Time Stamp:	12:12:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$170
RAM confirmation Number	E20224DC12394122
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	49733 32f0d2b9f03819f638cc9df5558feb66ad88c444	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	37770 2d456db61574a30b723db965788a3f1ae2fa2700	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	87503		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Wyatt

Serial:	17/528,073	Group Art Unit: 2887
Filed:	11/16/2021	Examiner: TBD
For:	Multi-Function Smart Tokenizing Electronic Payment Device	

Honorable Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Dear Sir:

Before examination on the merits, please enter the following amendments for filing in the above captioned patent application.

Listing of claims begins on page 2 of this paper. This listing of claims will replace all prior versions and listings of claims in the application.

Remarks/Arguments begin on page 29 of this paper.

IPR2025-01150
Apple EX1071 Page 415

LISTING OF CLAIMS

1. (Cancelled) A method of performing a transaction, the method comprising:

receiving an input at an electronic device,

wherein the input corresponds to a priming operation of the electronic device by an identified user, and,

wherein the electronic device comprises:

a processor;

a touch-screen display coupled to the processor; and

a near field communications (NFC) interface coupled to the processor;

receiving a request for a transaction payment at said electronic device via at least one the set consisting of: the NFC interface, the touch-screen display;

displaying, on the touch-screen display, information reflecting the request for the transaction payment, and images of:

a card issuer payment card method selection, including at least a 4-digit partial number of a card issuer supplied account number of the card issuer payment card,

a card issuer card logo, and

other iconography of the card issuer payment card;

generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of said card issuer supplied payment information;

IPR2025-01150
Apple EX1071 Page 416

transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface; and

visually conveying a status of said transaction via a user-interface displayed on said touch-screen display.

2. (Cancelled) The method of Claim 1, wherein the generating limited-use payment information comprises dynamically generating a cryptogram number for a use by the electronic device in place of a card validation value, associated with said card issuer payment card.

3. (Cancelled) The method of Claim 1, further comprising wirelessly receiving a static device account number from a card issuing authority, in response to a user-entry of a user's card issuer payment card information.

4. (Cancelled) The method of Claim 2, further comprising wirelessly receiving a static device account number from a card issuing authority, in response to a user-entry of a user's card issuer payment card information.

5. (Cancelled) The method of Claim 4, wherein the wirelessly received static device account number is for use in place of a user-entered card issuer payment card information, in a device payment transaction by an authorized device user.

IPR2025-01150
Apple EX1071 Page 417

6. (Cancelled) The method of Claim 5, wherein the limited-use payment information comprises combining the dynamic cryptogram number and the static device account number.

7. (Cancelled) The method of Claim 2, wherein the dynamically generated cryptogram number is based in part on a per-transaction sequential parameter originating from within the electronic device.

8. (Cancelled) The method of Claim 7, further comprising wirelessly receiving a static device account number from a card issuing authority, in response to a user-entry of a user's card issuer payment card information.

9. (Cancelled) The method of Claim 8, wherein the wirelessly received static device account number is for use in place of a user-entered card issuer information, in a device payment transaction by an authorized device user.

10. (Cancelled) The method of Claim 9, wherein the limited-use payment information comprises combining the dynamic cryptogram number and the static device account number.

11. (Cancelled) A system comprising:

IPR2025-01150
Apple EX1071 Page 418

an electronic device responsive to a priming operation from an authorized device user;

wherein the priming operation comprises a user input to the device enabling a payment transaction by the device;

wherein the electronic device comprises:

a processor;

at least one user input means, coupled to the at least one processor for receiving the user input;

a near field communications (NFC) interface coupled to the processor and operable to receive a request for a transaction payment; and,

a touch-screen display coupled to the processor, and

operable to display information reflecting the request for a payment transaction and information reflecting at least one payment option of at least one card issuer payment card;

wherein the electronic device is operable to dynamically generate a limited-use payment number based on a payment transaction sequential parameter originating from within the device;

wherein the electronic device is operable to store device-secret information; and,

wherein the electronic device is operable to transmit limited-use payment information comprising a combination of said dynamically generated limited-use

IPR2025-01150
Apple EX1071 Page 419

payment number and said device-secret information, to an NFC recipient via said NFC interface in connection with the request for a payment transaction; and,

wherein the touch-screen display is operable to visually convey a status of said payment transaction

wherein the touch-screen display is operable to visually convey that the payment transaction is approved only when at least the following conditions are met: the device transacted limited-use payment number matches a payment number similarly generated by a payment card processing authority, the payment transaction sequential parameter matches a transaction sequential parameter similarly generated by a payment card processing authority, and when the device-secret information matches a device-secret information stored within the payment card processing authority.

12. (Cancelled) The system of Claim 11, wherein the secret information from a payment card processing authority comprises a static device account number.

13. (Cancelled) The system of Claim 12, wherein said static device account number is specific to the electronic device.

14. (Cancelled) The system of Claim 13, wherein the payment card processing authority recognizes said use of said static device account number, as being from a recognized device in a user-authorized transaction, when payment

IPR2025-01150
Apple EX1071 Page 420

card processing authority generated limited-use payment number based at least in part on a transaction sequential parameter similarly generated by a payment card processing authority, matches in comparison with said transacted limited-use payment information.

15. (Newly Presented) A method of generating and using limited-use payment information for performing a payment transaction, the method comprising:

receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises:

a processor;

a touch-screen display coupled to the processor; and

a near field communications (NFC) interface coupled to the processor;

responsive to said priming operation, readying said device to perform a payment transaction by an identified user;

receiving a payment request for the payment transaction at said electronic device;

displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;

dynamically generating, by the processor, limited-use payment information;

wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device;

IPR2025-01150
Apple EX1071 Page 421

using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account;

transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient;

responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and

displaying the status of said payment transaction via said touch-screen display.

16. (Newly Presented) The method of Claim 15, wherein the limited-use payment information comprises a cryptogram number.

17. (Newly Presented) The method of Claim 15, wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient.

18. (Newly Presented) The method of Claim 17, wherein said readying said device to perform a payment transaction comprises:

identifying said proximity NFC recipient is an NFC payment facility;

IPR2025-01150
Apple EX1071 Page 422

successfully validating the identified user as authorized to perform the payment transaction via said electronic device; and

receiving a user approval for performing the payment transaction.

19. (Newly Presented) The method of Claim 18, wherein said user approval for performing a payment transaction comprises displaying a request for user input at said electronic device, for both said identifying and said user approval of said payment transaction, and further comprising:

the processor identifying that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction; and,

disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed.

20. (Newly Presented) The method of Claim 18, wherein said successfully validating the identified user comprises the processor successfully determining a match between:

firstly, a user input received via at least one of a set of user input sensors of the electronic device; and,

secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.

IPR2025-01150
Apple EX1071 Page 423

21. (Newly Presented) The method of Claim 20, wherein said user input received via at least one of a set of user input sensors of the electronic device comprises a passcode entry sequence performed by a user input via the touch-screen display.

22. (Newly Presented) The method of Claim 20, wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch characteristics.

23. (Newly Presented) The method of Claim 20, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture.

24. (Newly Presented) The method of Claim 20, wherein said predetermined user characteristics stored within the electronic device comprise a known user motion of the device.

25. (Newly Presented) The method of Claim 15, wherein the input comprising a priming operation is a user input.

IPR2025-01150
Apple EX1071 Page 424

26. (Newly Presented) The method of Claim 25, wherein said readying said device to perform a payment transaction comprises:

successfully identifying said identified user from said user input; and,

wherein said user input further comprises a user approval for performing the payment transaction received from said identified user; and,

wherein said successfully identifying further comprises said electronic device validating an authorized user of said electronic device by comparing a user-touch input received via a touch input sensor on the electronic device with a recognized valid user-touch, stored in a memory of the electronic device; and,

wherein said user approval for performing the payment transaction further comprises:

visually presenting information of the payment transaction on the touch screen display of said electronic device;

visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and,

subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device.

27. (Newly Presented) The method of Claim 15, further comprising:

prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,

IPR2025-01150
Apple EX1071 Page 425

in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.

28. (Newly Presented) The method of Claim 15, further comprising:

prior to the priming operation, transmitting the issued payment information, user information and device-specific information; and,

in response to transmitting said issued payment information, user information, and device-specific information, receiving a payment processing authority supplied secret information.

29. (Newly Presented) The method of Claim 28 wherein said payment processing authority supplied secret information comprises static device account information.

30. (Newly Presented) The method of Claim 29 wherein said static device account information comprises a static device account number and a static device-specific expiration date.

31. (Newly Presented) The method of Claim 30 wherein the static device account number is associated with the selected issued payment account on said electronic device.

IPR2025-01150
Apple EX1071 Page 426

32. (Newly Presented) The method of Claim 16, further comprising:

prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,

in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.

33. (Newly Presented) The method of Claim 27 further comprising:

combining said limited-use payment information and said static device account information, to produce a combined payment information;

transmitting said combined payment information, in place of the issued payment account information, via said NFC interface for receipt by an NFC recipient; and

receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.

34. (Newly Presented) The method of Claim 32 further comprising:

combining said limited-use payment information and said static device account information, to produce a combined payment information;

transmitting said combined payment information, in place of the issued payment account information, via said NFC for receipt by an NFC recipient; and

IPR2025-01150
Apple EX1071 Page 427

receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.

35. (Newly Presented) The method of Claim 15, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.

36. (Newly Presented) The method of Claim 35 wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority; and

further wherein the at least one secret information is not exchanged when preforming the payment transaction.

37. (Newly Presented) The method of Claim 27, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.

38. (Newly Presented) The method of Claim 37, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.

IPR2025-01150
Apple EX1071 Page 428

39. (Newly Presented) The method of Claim 32, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.

40. (Newly Presented) The method of Claim 39, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.

41. (Newly Presented) The method of Claim 33, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.

42. (Newly Presented) The method of Claim 41, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.

43. (Newly Presented) A system for completing a payment transaction, the system comprising:

an electronic device operable to receive a priming operation, wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user, and, wherein the electronic device further comprises:

IPR2025-01150
Apple EX1071 Page 429

a processor;

a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; and,

a touch-screen display coupled to the processor, and

wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account;

wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device;

wherein the electronic device is operable to store a static device-specific user account information;

wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static device-specific user account information to an NFC recipient via said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account;

wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and,

IPR2025-01150
Apple EX1071 Page 430

wherein the touch-screen display is operable to display an indication of said status information.

44. (Newly Presented) The system of Claim 43, wherein the dynamically generated limited-use payment information comprises a cryptogram number.

45. (Newly Presented) The system of Claim 43, wherein the device-specific user account information comprises static device account information.

46. (Newly Presented) The system of Claim 45, wherein the static device account information comprises a static device account number that is unique to the electronic device.

47. (Newly Presented) The system of Claim 46 wherein the static device account information further comprises a static device account expiration date.

48. (Newly Presented) The system of Claim 46 wherein the sequential counter count is changed per payment transaction.

49. (Newly Presented) The system of Claim 48 wherein the electronic device is operable to transmit issued payment account information and in response thereto, to receive the static device account information.

IPR2025-01150
Apple EX1071 Page 431

50. (Newly Presented) The system of Claim 43 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on a shared information: from said user, information associated with said electronic device, information associated with said selected issued payment account, and at least one secret; and,

wherein said shared information is shared by both the electronic device and a payment processing authority.

51. (Newly Presented) The system of Claim 43 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.

52. (Newly Presented) The system of Claim 50 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.

53. (Newly Presented) An electronic device for completing a payment transaction, the electronic device comprising:

a processor;

IPR2025-01150
Apple EX1071 Page 432

a memory coupled to the processor, wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information;

a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;

a user interface coupled to the processor;

a user input device coupled to the processor; and,

wherein said processor is operable to:

responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,

cause the display of information associated with the payment request;

cause the display of an image representing at least one user-selectable issued payment account; and,

dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and,

cause the transmission, via said NFC interface, a payment information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient;

IPR2025-01150
Apple EX1071 Page 433

wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and

wherein the user interface is operable to provide an indication of the status information.

54. (Newly Presented) The device of Claim 53 wherein the payment authority information comprises information that is unique to the electronic device.

55. (Newly Presented) The device of Claim 53 wherein the payment authority information comprises a secret information shared by both the electronic device and a payment processing authority.

56. (Newly Presented) The device of Claim 53 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the processing authority information.

57. (Newly Presented) The device of Claim 55 wherein the processing authority information comprises a static device account number.

58. (Newly Presented) The device of Claim 57 wherein the processing authority information further comprises a static device account expiration date.

IPR2025-01150
Apple EX1071 Page 434

59. (Newly Presented) The device of Claim 53 wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further wherein the processor is operable to cause transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said payment authority information in connection with the payment transaction in place of at least a portion of the payment information associated with said selected issued payment account.

60. (Newly Presented) The device of Claim 59 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the processing authority information.

61. (Newly Presented) The device of Claim 60 wherein the processing authority information comprises a static device account number.

62. (Newly Presented) The device of Claim 61 wherein the processing authority information further comprises a static device account expiration date.

63. (Newly Presented) The device of Claim 53, wherein said user interface comprises a display and wherein said user input device comprises a touch panel

IPR2025-01150
Apple EX1071 Page 435

disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch panel.

64. (Newly Presented) The device of Claim 53, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response thereto.

65. (Newly Presented) The device of Claim 53, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of a continuous user touch.

66. (Newly Presented) The device of Claim 53, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch panel.

67. (Newly Presented) The device of Claim 53, wherein said user interface comprises a display and wherein said user input device comprises a touch panel

IPR2025-01150
Apple EX1071 Page 436

disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification.

68. (Newly Presented) The device of Claim 53, wherein said user input device comprises an array of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.

69. (Newly Presented) The device of Claim 53, wherein the processor is operable to:

receive a user-selection of an issued payment account presented on the user interface, received via the user input device coupled to the processor, and

responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and

use at least a portion of said specific processing authority information in place of at least a portion of the issued payment account information to generate a combined payment information to complete a payment transaction per the input user-selection.

70. (Newly Presented) An electronic device for completing a payment transaction, the electronic device comprising:

IPR2025-01150
Apple EX1071 Page 437

a processor;

a memory coupled to the processor, wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information;

a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;

a user interface coupled to the processor;

a user input device coupled to the processor; and,

wherein said processor is operable to:

responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,

cause the display of information associated with the payment request;

cause the display of an image representing the user-selectable issued payment account; and,

dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret information associated with the user-selectable issued payment account; and,

cause the transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said payment authority information, for receipt by an NFC recipient;

IPR2025-01150
Apple EX1071 Page 438

wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and

wherein the user interface is operable to provide an indication of the transaction status information.

71. (Newly Presented) The device of Claim 70, wherein the payment authority information comprises information that is unique to the electronic device.

72. (Newly Presented) The device of Claim 70, wherein the secret information is shared by both the electronic device and a payment processing authority.

73. (Newly Presented) The device of Claim 70, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the payment authority information.

74. (Newly Presented) The device of Claim 71, wherein the payment authority information comprises a static device account number.

75. (Newly Presented) The device of Claim 74, wherein the payment authority information further comprises a static device account expiration date.

IPR2025-01150
Apple EX1071 Page 439

76. (Newly Presented) The device of Claim 70, wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further payment information combination is used in place of at least a portion of fixed payment information associated with said user-selectable issued payment account.

77. (Newly Presented) The device of Claim 76, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the payment authority information.

78. (Newly Presented) The device of Claim 77, wherein the payment authority information comprises a static device account number.

79. (Newly Presented) The device of Claim 78, wherein the payment authority information further comprises a static device account expiration date.

80. (Newly Presented) The device of Claim 70, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch screen interface.

IPR2025-01150
Apple EX1071 Page 440

81. (Newly Presented) The device of Claim 70, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response via said touch screen interface of the display.

82. (Newly Presented) The device of Claim 70, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of said user touch.

83. (Newly Presented) The device of Claim 70, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch screen interface.

84. (Newly Presented) The device of Claim 70, wherein said user interface comprises a display and wherein said user input device comprises a touch input of the electronic device and wherein further the processor is operable to identify an

IPR2025-01150
Apple EX1071 Page 441

authorized user by biometric recognition of a valid user identification via the touch input.

85. (Newly Presented) The device of Claim 70, wherein said user input device comprises an array of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.

86. (Newly Presented) The device of Claim 70, wherein the processor is operable to receive, via the user input device, a user-selection of said user-selectable issued payment account presented on the user interface, and

in response thereto, is further operable to select from memory the payment authority information corresponding to selected user-selectable issued payment account, and

is further operable to use said payment information combination in place of at least a portion of fixed payment information associated with said selected user-selectable issued payment account.

IPR2025-01150
Apple EX1071 Page 442

REMARKS/ARGUMENTS

Claims 15-86 are pending in the present application. Claims 1-14 are cancelled herein without prejudice. Claims 15-86 are added herein. Applicants respectfully request reconsideration of the present application in view of the claim amendments presented herein. Applicants assert no new matter has been added as a result of these claim amendments submitted herewith.

The Examiner is invited to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present Application.

Respectfully submitted,

MURABITO, HAO & BARNES LLP

Date: 04/22/2022

/Anthony C. Murabito/
Anthony C. Murabito
Reg. No. 35,295

111 North Market Street
Suite 700
San Jose, California 95113
(408) 938-9060

IPR2025-01150
Apple EX1071 Page 443

Please charge any additional fees or apply any credits to our PTO deposit account number: 50-4160.

Dated: 01/30/2022

/Anthony C. Murabito/
Anthony C. Murabito
Registration #: 35,295
111 North Market Street
Suite 700
San Jose, California 95113
(408) 938-9060

Electronic Patent Application Fee Transmittal	
Application Number:	17528073
Filing Date:	16-Nov-2021
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Filer:	Anthony C. Murabito/Missy Isaac
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	52	50	2600
INDEPENDENT CLAIMS IN EXCESS OF 3	2201	1	240	240
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2840**

Electronic Acknowledgement Receipt	
EFS ID:	45541736
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Anthony C. Murabito/Missy Isaac
Filer Authorized By:	Anthony C. Murabito
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Receipt Date:	22-APR-2022
Filing Date:	16-NOV-2021
Time Stamp:	15:53:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	EFT
Payment was successfully received in RAM	$2840
RAM confirmation Number	E20224LF54202614
Deposit Account	504160
Authorized User	Missy Isaac
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.19 (Document supply fees) 37 CFR 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		WYAT-0002USD1C1C1C1C1C_PRELIM_AMDT_04-22-2022_.pdf	12505608 d2c62c920b36b7ce4942fb0d4193348490e40ccc	yes	29

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Claims	2	28
Applicant Arguments/Remarks Made in an Amendment	29	29

Warnings:

Information:

2	Miscellaneous Incoming Letter	acm_depositaccount_blurb.pdf	41871 51e693c8b0b73d0b1f55fc5df0ef8df0fd49e46d	no	1

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	40435 5906289376271cbcf664789aded87c8e633f5390	no	2

Warnings:

Information:

Total Files Size (in bytes):	12587914

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 17/528,073	Filing Date 11/16/2021	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $240 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT	04/22/2022	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 72	Minus	** 20	= 52		x $50 =	2600
	Independent (37 CFR 1.16(h))	* 4	Minus	*** 3	= 1		x $240 =	240
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	2840

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/AMANDA N FORD/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C

CONFIRMATION NO. 4809

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

PUBLICATION NOTICE

OC000000134871476

Title:MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Publication No.US-2022-0207517-A1
Publication Date:06/30/2022

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IPR2025-01150
Apple EX1071 Page 451

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

136197 7590 11/16/2022

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

EXAMINER
LEE, SEUNG H

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 11/16/2022

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	02/16/2023

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PTOL-85 (Rev. 02/11)

IPR2025-01150
Apple EX1071 Page 452

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

136197 7590 11/16/2022

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	02/16/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEE, SEUNG H	2876	235-380000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1_____
2_____
3_____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required) ❑Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

IPR2025-01150
Apple EX1071 Page 453

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

136197 7590 11/16/2022

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

EXAMINER	
LEE, SEUNG H	

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 11/16/2022

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

IPR2025-01150
Apple EX1071 Page 454

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 17/528,073	Applicant(s) WYATT, David	
	Examiner SEUNG H LEE	Art Unit 2876	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 4/22/2022.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 15-86 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 3/17/2022.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/SEUNG H LEE/
Primary Examiner, Art Unit 2876

IPR2025-01150
Apple EX1071 Page 456

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

Prelim. Amdt./Amendment

2. Receipt is acknowledged of the Preliminary Amendment filed on April 22, 2022.

Terminal Disclaimer

3. The terminal disclaimer filed on April 14, 2022 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of **U.S. Patent Nos 9760884, 9430765, 9224083, 9022286, 10810579, 10628820, 10339520, 10013693, and 11176538** has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

4. Claims 15-86 are allowed.

5. The following is an examiner's statement of reasons for allowance:

None of prior art teaches a method of generating and using limited-use payment information for performing a payment transaction, the method comprising: receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises: a processor; a touch-screen display coupled to the processor; and a near field communications (NFC) interface coupled to the processor; responsive to said priming operation, readying said device to perform a

payment transaction by an identified user; receiving a payment request for the payment transaction at said electronic device; displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account; dynamically generating, by the processor, limited-use payment information; wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device; using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account; transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient.; responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display, and a system of the same as set forth in the claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SEUNG H LEE whose telephone number is (571)272-2401. The examiner can normally be reached 7-4:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steven Paik can be reached on 571-272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SEUNG H LEE/
Primary Examiner, Art Unit 2876

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

CPC						
Symbol					**Type**	**Version**
G06Q	/	20	/	341	F	2013-01-01
G07F	/	19	/	00	I	2013-01-01
G06Q	/	20	/	06	I	2013-01-01
G06Q	/	20	/	223	I	2013-01-01
G06Q	/	20	/	347	I	2013-01-01
G06Q	/	20	/	385	I	2013-01-01
G07F	/	7	/	0873	I	2013-01-01
G06K	/	19	/	06206	I	2013-01-01
G06K	/	19	/	0716	I	2013-01-01
G06K	/	19	/	07749	I	2013-01-01
G06Q	/	20	/	24	I	2013-01-01
G06Q	/	20	/	352	I	2013-01-01
G06Q	/	20	/	409	I	2013-01-01
G06Q	/	20	/	065	I	2013-01-01
G06Q	/	20	/	346	I	2013-01-01
G06Q	/	20	/	3827	I	2013-01-01
G06Q	/	20	/	4012	I	2013-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	05 November 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20221105

IPR2025-01150
Apple EX1071 Page 460

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06Q20/34	/	20	/	34

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	05 November 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office

Part of Paper No.: 20221105

IPR2025-01150
Apple EX1071 Page 461

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	15	14	24	18	33	20	42	38	51	46	60	55	69	64	78
2	16	15	25	4	34	29	43	37	52	47	61	56	70	65	79
7	17	16	26	27	35	30	44	39	53	48	62	57	71	66	80
8	18	17	27	28	36	31	45	40	54	49	63	60	72	67	81
9	19	23	28	21	37	32	46	41	55	50	64	61	73	68	82
10	20	24	29	22	38	33	47	44	56	51	65	58	74	69	83
11	21	25	30	5	39	34	48	42	57	52	66	59	75	70	84
12	22	26	31	6	40	35	49	43	58	53	67	62	76	71	85
13	23	3	32	19	41	36	50	45	59	54	68	63	77	72	86

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	05 November 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20221105

IPR2025-01150
Apple EX1071 Page 462

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

CPC - Searched*		
Symbol	Date	Examiner
G06Q20/341 or G06K19/06206 or G06K19/0716 or G06K19/07749 or G06Q20/06 or G06Q20/065 or G06Q20/223 or G06Q20/24 or G06Q20/346 or G06Q20/347 or G06Q20/352 or G06Q20/3827 or G06Q20/385 or G06Q20/4012 or G06Q20/409 or G07F7/0873 or G07F19/00	11/05/2022	sl

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
PE2E	11/05/2022	sl
14/680979,14/981757,15/701261,16/459150, 17/075637 (parent cases)	11/05/2022	sl
NPL	11/05/2022	sl

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	same as above	11/05/2022	sl

IPR2025-01150
Apple EX1071 Page 463

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

IPR2025-01150
Apple EX1071 Page 464

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	11/05/2022								
1	15	=								
2	16	=								
7	17	=								
8	18	=								
9	19	=								
10	20	=								
11	21	=								
12	22	=								
13	23	=								
14	24	=								
15	25	=								
16	26	=								
17	27	=								
23	28	=								
24	29	=								
25	30	=								
26	31	=								
3	32	=								
18	33	=								
4	34	=								
27	35	=								
28	36	=								
21	37	=								
22	38	=								
5	39	=								
6	40	=								
19	41	=								
20	42	=								
29	43	=								
30	44	=								
31	45	=								
32	46	=								
33	47	=								
34	48	=								
35	49	=								
36	50	=								
38	51	=								
37	52	=								
39	53	=								
40	54	=								
41	55	=								
44	56	=								

IPR2025-01150
Apple EX1071 Page 465

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

CLAIM		DATE								
Final	Original	11/05/2022								
42	57	=								
43	58	=								
45	59	=								
46	60	=								
47	61	=								
48	62	=								
49	63	=								
50	64	=								
51	65	=								
52	66	=								
53	67	=								
54	68	=								
55	69	=								
56	70	=								
57	71	=								
60	72	=								
61	73	=								
58	74	=								
59	75	=								
62	76	=								
63	77	=								
64	78	=								
65	79	=								
66	80	=								
67	81	=								
68	82	=								
69	83	=								
70	84	=								
71	85	=								
72	86	=								

IPR2025-01150
Apple EX1071 Page 466

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	TBD
Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9818104		2017-11-14	KATZER; ET AL.	
	2	9105020		2015-08-11	RONCA; ET AL	
	3	8571937		2013-10-29	ROSE; ET AL	
	4	11100431		2021-08-24	MULLEN; ET AL	
	5	10037524		2018-07-31	ROYYURU; ET AL	
	6	8690055		2014-04-08	ANDERSON; ET AL	
	7	7100821		2006-09-05	RASTI	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	TBD
	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020153424		2002-10-24	LI	
	2	20110276416		2011-11-10	MULLEN, et al.	
	3	20150317632		2015-11-05	PARK, et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2012154915	WO	A1	2012-11-15	DYNAMICS INC		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	11/05/2022

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	TBD
	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	TBD
	Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Anthony C. Murabito/	Date (YYYY-MM-DD)	2022-03-17
Name/Print	Anthony C. Murabito	Registration Number	35295

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Bibliographic Data

Application No: 17/528,073

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /SEUNG H LEE/ (Examiner's Signature) | (Initials)

Title: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/16/2021 RULE	235	2876	WYAT-0002.USD1C1C1C1C1C

APPLICANTS

CARDWARE, INC., San Jose, CA, UNITED STATES

INVENTORS

David WYATT, San Jose, CA, UNITED STATES

CONTINUING DATA

This application is a CON of 17075637 10/20/2020 PAT 11176538

17075637 is a CON of 16459150 07/01/2019 PAT 10810579

16459150 is a CON of 15701261 09/11/2017 PAT 10339520

15701261 is a CON of 14981757 12/28/2015 PAT 9760884

14981757 is a CON of 14680979 04/07/2015 PAT 9224083

14680979 is a DIV of 14217261 03/17/2014 PAT 9022286

14217261 has PRO of 61794891 03/15/2013

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

11/30/2021

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113
UNITED STATES

FILING FEE RECEIVED

$1,230

Search History

Report Run Date: 2022-11-05 UTC
Searches: 9
Markers: 0

IPR2025-01150
Apple EX1071 Page 474

Search #	Timestamp	Results	Page
1	2022-11-05 19:09 UTC	22,728,331	3
2	2022-11-05 19:10 UTC	27,487,901	4
3	2022-11-05 19:11 UTC	22,728,342	4
4	2022-11-05 19:12 UTC	3,980,669	5
5	2022-11-05 19:13 UTC	3,980,669	5
6	2022-11-05 19:14 UTC	22,728,342	7
7	2022-11-05 19:15 UTC	3,980,669	7
8	2022-11-05 19:15 UTC	3,974,553	8
9	2022-11-05 19:15 UTC	22,506,685	9

Content: Patent Publications (167)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Applications | Jordan Patents | Jordan Applications | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Saudi Arabia Applications | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Patents | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications

1 **2022-11-05 19:09 UTC | 22,728,331 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text

A method of generating and using limited-use payment information for performing a payment transaction, the method comprising: receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises: a processor; a touch-screen display coupled to the processor; and a near field communications (NFC) interface coupled to the processor; responsive to said priming operation, readying said device to perform a payment transaction by an identified user; receiving a payment request for the payment transaction at said electronic device; displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account; dynamically generating, by the processor, limited-use payment information; wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device; using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected

IPR2025-01150
Apple EX1071 Page 476

issued payment account; transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient.; responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display.

Concept Modifiers: None

Filters: None

2 **2022-11-05 19:10 UTC | 27,487,901 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
A system for completing a payment transaction, the system comprising: an electronic device operable to receive a priming operation, wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user, and, wherein the electronic device further comprises: a processor; a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; and. a touch-screen display coupled to the processor, and wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account; wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device; wherein the electronic device is operable to store a static device-specific user account information; wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment inform ation and said static device- specific user account information to an NFC recipient via said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account; wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and, wherein the touch-screen display is operable to display an indication of said status information.

Concept Modifiers: None

Filters: None

3 **2022-11-05 19:11 UTC | 22,728,342 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
An electronic device for completing a payment transaction, the electronic device comprising: a processor; a memory coupled to the processor, wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information; a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; a user interface coupled to the processor; a user input device coupled to the processor; and, wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction, cause the display of information associated with the payment request; cause the display of an image representing at least one user-selectable issued payment account; and, dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and, cause the transmission, via said NFC interface, a paymien t information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient; wherein the

IPR2025-01150
Apple EX1071 Page 477

NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the status information.

Concept Modifiers: None

Filters: None

Content: Non-Patent Literature (23)

IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | IEEE Xplore Publications: SMPTE Periodicals | IEEE Xplore Publications: SMPTE Conferences | IEEE Xplore Publications: SMPTE Standards | IEEE Xplore Publications: MIT Press eBooks | IEEE Xplore Publications: Wiley-IEEE eBooks | IEEE Xplore Publications: IBM Periodicals | IEEE Xplore Publications: URSI Periodicals | IEEE Xplore Publications: VDE Conferences | IEEE Xplore Publications: Periodicals from China | IP.com Prior Art Database: The IP.com Journal | IP.com Prior Art Database: Internet Society RFC | IP.com Prior Art Database: IBM TDB Archive | IP.com Prior Art Database: Legacy Journals | IP.com Prior Art Database: Software Patent Institute | OnePetro.org: Periodicals at OnePetro.org | OnePetro.org: Conferences at OnePetro.org | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

4 **2022-11-05 19:12 UTC | 3,980,669 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text

An electronic device for completing a payment transaction, the electronic device comprising: a processor; a memory coupled to the processor, wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information; a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; a user interface coupled to the processor; a user input device coupled to the processor; and, wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction, cause the display of information associated with the payment request; cause the display of an image representing at least one user-selectable issued payment account; and, dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and, cause the transmission, via said NFC interface, a paymien t information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient; wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the status information.

Concept Modifiers: None

Filters: None

5 **2022-11-05 19:13 UTC | 3,980,669 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text

IPR2025-01150
Apple EX1071 Page 478

An electronic device for completing a payment transaction, the electronic device comprising: a processor; a memory coupled to the processor, wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information; a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; a user interface coupled to the processor; a user input device coupled to the processor; and, wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction, cause the display of information associated with the payment request; cause the display of an image representing the user-selectable issued payment account; and, dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret inform a.tion associated with the user-selectable issued payment account; and, cause the transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said p ayment authority information, for receipt by an NFC recipient; wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the transaction status information.

Concept Modifiers: None

Filters: None

Content: Patent Publications (167)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Applications | Jordan Patents | Jordan Applications | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Saudi Arabia Applications | Singapore

IPR2025-01150
Apple EX1071 Page 479

Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Patents | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications

6 **2022-11-05 19:14 UTC | 22,728,342 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
An electronic device for completing a payment transaction, the electronic device comprising: a processor; a memory coupled to the processor, wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information; a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; a user interface coupled to the processor; a user input device coupled to the processor; and, wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction, cause the display of information associated with the payment request; cause the display of an image representing the user-selectable issued payment account; and, dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret inform a.tion associated with the user-selectable issued payment account; and, cause the transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said p ayment authority information, for receipt by an NFC recipient; wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the transaction status information.

Concept Modifiers: None

Filters: None

Content: Non-Patent Literature (23)

IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | IEEE Xplore Publications: SMPTE Periodicals | IEEE Xplore Publications: SMPTE Conferences | IEEE Xplore Publications: SMPTE Standards | IEEE Xplore Publications: MIT Press eBooks | IEEE Xplore Publications: Wiley-IEEE eBooks | IEEE Xplore Publications: IBM Periodicals | IEEE Xplore Publications: URSI Periodicals | IEEE Xplore Publications: VDE Conferences | IEEE Xplore Publications: Periodicals from China | IP.com Prior Art Database: The IP.com Journal | IP.com Prior Art Database: Internet Society RFC | IP.com Prior Art Database: IBM TDB Archive | IP.com Prior Art Database: Legacy Journals | IP.com Prior Art Database: Software Patent Institute | OnePetro.org: Periodicals at OnePetro.org | OnePetro.org: Conferences at OnePetro.org | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

7 **2022-11-05 19:15 UTC | 3,980,669 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

IPR2025-01150
Apple EX1071 Page 480

Main Concept: Text
An electronic device for completing a payment transaction, the electronic device comprising: a processor; a memory coupled to the processor, wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information; a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; a user interface coupled to the processor; a user input device coupled to the processor; and, wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction, cause the display of information associated with the payment request; cause the display of an image representing the user-selectable issued payment account; and, dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret inform a.tion associated with the user-selectable issued payment account; and, cause the transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said p ayment authority information, for receipt by an NFC recipient; wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the transaction status information.

Concept Modifiers: None

Filters: None

8 **2022-11-05 19:15 UTC | 3,974,553 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
An embodiment includes a multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card. An apparatus is described to allow the device to emulate behavior of a credit card when used in electronic credit card readers. Additionally, methods are described to allow user control of the device for the purpose of authorizing or controlling use of the device in the application of credit, debit and cash transactions, including cryptocurrency and device-to-device transactions. Methods are also described for generating a limited-duration payment number when performing a transaction for the purpose of creating a limited-use payment number, which is limited in scope of use to a predetermined number of authorized transactions. Furthermore the device may interact with other similar devices in proximity for the purpose of funds or credit/debit transfers.

Concept Modifiers: None

Filters: None

Content: Patent Publications (167)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium

IPR2025-01150
Apple EX1071 Page 481

Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Applications | Jordan Patents | Jordan Applications | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Saudi Arabia Applications | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Patents | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications

9 **2022-11-05 19:15 UTC | 22,506,685 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text

An embodiment includes a multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card. An apparatus is described to allow the device to emulate behavior of a credit card when used in electronic credit card readers. Additionally, methods are described to allow user control of the device for the purpose of authorizing or controlling use of the device in the application of credit, debit and cash transactions, including cryptocurrency and device-to-device transactions. Methods are also described for generating a limited-duration payment number when performing a transaction for the purpose of creating a limited-use payment number, which is limited in scope of use to a predetermined number of authorized transactions. Furthermore the device may interact with other similar devices in proximity for the purpose of funds or credit/debit transfers.

Concept Modifiers: None

Filters: None

IPR2025-01150
Apple EX1071 Page 482

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	30843	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/04/27 12:21 PM
L2	1	nfc same transaction same payment same logo same limited same issuer	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/04/27 12:22 PM
L4	311	monitor$4 same master same node same wireless same sensor	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:55 PM
L5	18	L4.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:55 PM
L6	107	L4 same (slave peripheral)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:56 PM
L7	7	L6.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:56 PM
L8	17	("20030018927"|"9860688"|"20180165568"|"20150154531"|"9189226"|"20100082870"|"20170039666"|"20180046964"|"9824329"|"20080239282"|"9182231"|"20130107770"|"20070049291"|"6614392"|"20100299401"|"20160233927").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:58 PM
L9	9	L6 same (environment$4 temperature)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 01:00 PM
L10	9	("20130250357"|"20150324745"|"7177054"|"8292173"|"7048194"|"7299990"|"7540603"|"8072620"|"20100096181").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 01:04 PM

IPR2025-01150
Apple EX1071 Page 483

L11	39	("2015/0324745").URPN.	(USPAT)	OR	OFF	OFF	2020/05/02 08:57 AM
L12	35	label same wireless same master same (slave peripheral)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/02 09:00 AM
L13	39	"517508"	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/02 09:19 AM
L14	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:07 AM
L15	55	nfc same transaction same payment same limited same issuer	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:07 AM
L16	5	L15 same proximity	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:08 AM
L17	30909	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:24 AM
L18	129	L17 and (nfc same select$4 same payment same limit$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:25 AM
L19	43	L17 and (nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:26 AM
L20	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L21	0	L20 and (nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L22	109	(nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L23	94	L22 same (mobile portable)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:34 AM
L24	4186	dynamic same credit	(US-PGPUB; USPAT;	OR	OFF	OFF	2020/05/05

IPR2025-01150
Apple EX1071 Page 484

		same card	EPO; JPO)				08:35 AM
L25	7	L22 and L24	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:35 AM
L26	23	("20020073025" | "20030101137" | "20070278290" | "20100057553" | "20100082487" | "20110137748" | "20110302089" | "20120006891" | "20140052607" | "20140129422" | "20140143037" | "20140195324" | "20140249941" | "20140279474" | "20150058145" | "20160027005" | "20160086161" | "20160162857" | "20160162887" | "20160335619" | "6633223" | "9292849" | "9489671").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2020/05/05 08:38 AM
L27	6	("20040168067" | "20090276347" | "20110016047" | "20120173311" | "20130159186" | "6163771").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2020/05/05 08:39 AM
L28	4	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2020/05/05 09:39 AM
L29	1	L28 and (respons$4 same nfc same generat$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 09:40 AM
L30	31288	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:19 PM
L31	135	L30 and (nfc same	(US-PGPUB; USPAT;	OR	OFF	OFF	2020/06/21

IPR2025-01150
Apple EX1071 Page 485

		select$4 same payment same limit$4)	EPO; JPO)				02:19 PM
L32	112	L30 and (nfc same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:20 PM
L33	7	L30 and (nfc same payment same limit$4 same approv$4 same interface)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:20 PM
L34	10	L30 and (nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:28 PM
L35	36	(nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:29 PM
L36	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:30 PM
L37	51	"075637"	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/28 10:02 PM
L38	1	"10810579".pn.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/28 10:03 PM
L39	35569	(G06Q20/341 or G06K19/07749 or G06Q20/347 or G06Q20/06 or G06Q20/409 or G06Q20/4012 or G06Q20/346 or G06Q20/3827 or G06K19/0716 or G07F19/00 or G06Q20/223 or G06Q20/24 or G06Q20/385 or G07F7/0873 or G06K19/06206 or G06Q20/065 or G06Q20/352).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:36 AM
L40	6275	payment same transaction same (limit$4 tempora$6) same generat$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:39 AM
L41	1592	L39 and L40	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:39 AM
L42	862	L40 same issuer same account	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:40 AM
L43	265	L39 and L42	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:40 AM
L44	30	L42 same wireless$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:42 AM

L45	2	("8851370"|"9646301").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:07 AM
L46	31	("10013693" | "20060032908" | "20080223937" | "20100260388" | "20110140841" | "20130048712" | "20130124292" | "20130297509" | "20140052632" | "20140279555" | "20180240106" | "6631849" | "6641050" | "7128274" | "7202825" | "7360688" | "7784692" | "7793851" | "7841539" | "8577813" | "8639629" | "8702007" | "8768838" | "8856539" | "9022286" | "9100826" | "9224083" | "9430765" | "9530137" | "9536238" | "9760884").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2021/09/29 07:08 AM
L47	229	("7128274").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:16 AM
L48	369	("7793851").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:22 AM
L49	77	L40 and L48	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:22 AM
L50	47	L39 and L49	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:22 AM
L51	130	("2013/0159186").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:36 AM
L52	41	(nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L53	1218	(select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L54	267	L39 and L53	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L55	346	L53 same generat$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:49 AM
L56	2785621	L55 sane dynamic$6	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:49 AM
L57	48	L55 same dynamic$6	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:50 AM
L58	11	L55 same static$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:51 AM
L59	543	("10043164" | "10075437" | "10129648" |	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2021/09/29 08:20 AM

IPR2025-01150
Apple EX1071 Page 487

		"10133979" | "10217105" | "20010010723" | "20010029485" | "20010034702" | "20010054003" | "20020078345" | "20020093530" | "20020100808" | "20020120583" | "20020152116" | "20020153424" | "20020165827" | "20030023554" | "20030034873" | "20030055727" | "20030078882" | "20030167350" | "20030208449" | "20040015958" | "20040039919" | "20040127256" | "20040215674" | "20040230799" | "20050044367" | "20050075985" | "20050081038" | "20050138387" | "20050156026" | "20050160049" | "20050195975" | "20050247797" | "20060006230" | "20060040726" | "20060041402" | "20060044153" | "20060047954" | "20060085848" | "20060136334" | "20060173985" | "20060174331" | "20060242698" | "20060280338" | "20070033642" | "20070055630" | "20070061266" | "20070061487" | "20070116292" | "20070118745" | "20070197261" | "20070224969" | "20070241182" | "20070256134" | "20070258594" | "20070278291" | "20080008315" | "20080011831" | "20080014867" |				

IPR2025-01150
Apple EX1071 Page 488

		"20080035738" | "20080071681" | "20080072303" | "20080086767" | "20080103968" | "20080109309" | "20080110983" | "20080120711" | "20080156873" | "20080162312" | "20080164308" | "20080207307" | "20080209543" | "20080223918" | "20080285746" | "20080308641" | "20090048026" | "20090132417" | "20090143104" | "20090171682" | "20090210308" | "20090235339" | "20090249077" | "20090282264" | "20100023449" | "20100023455" | "20100029202" | "20100030549" | "20100033310" | "20100036769" | "20100078471" | "20100082491" | "20100094754").PN. OR ("20100095130" | "20100100480" | "20100114731" | "20100192230" | "20100207742" | "20100211797" | "20100240413" | "20100257357" | "20100312634" | "20100312635" | "20110035604" | "20110060631" | "20110084132" | "20110101093" | "20110113245" | "20110125638" | "20110131415" | "20110153437" | "20110153496" | "20110208658" | "20110208965" | "20110211219" | "20110218911" | "20110238564" | "20110246780"					

		"20110258452" | "20110280406" | "20110282785" | "20110294418" | "20110312271" | "20120009946" | "20120024947" | "20120030047" | "20120030121" | "20120047071" | "20120079281" | "20120109735" | "20120143754" | "20120150737" | "20120178366" | "20120196583" | "20120207305" | "20120209773" | "20120238206" | "20120239560" | "20120252350" | "20120254394" | "20120284194" | "20120290472" | "20120296818" | "20120316992" | "20120317035" | "20120317628" | "20130005245" | "20130008956" | "20130026229" | "20130054474" | "20130065564" | "20130080228" | "20130080229" | "20130099587" | "20130104251" | "20130106576" | "20130119130" | "20130130614" | "20130144793" | "20130171929" | "20130179351" | "20130185772" | "20130191279" | "20130200999" | "20130216108" | "20130226791" | "20130226796" | "20130232082" | "20130238894" | "20130282360" | "20130303085" | "20130304651" | "20130312082" | "20130314593" | "20130344857" | "20140002238" |				

IPR2025-01150
Apple EX1071 Page 490

		"20140019352" | "20140027506" | "20140032409" | "20140032410" | "20140040120" | "20140040139" | "20140040147" | "20140047235" | "20140067690" | "20140074637").PN. OR ("20140074655" | "20140081720" | "20140095227" | "20140138435" | "20140171034" | "20140171039" | "20140172700" | "20140180851" | "20140208112" | "20140214674" | "20140229375" | "20140245391" | "20140256251" | "20140258099" | "20140258113" | "20140258125" | "20140274179" | "20140279479" | "20140337235" | "20140339315" | "20140346860" | "20140365780" | "20140379361" | "20150012444" | "20150032635" | "20150071486" | "20150088757" | "20150089586" | "20150134452" | "20150140960" | "20150154595" | "20150170138" | "20150178724" | "20150186871" | "20150205379" | "20150235211" | "20150302409" | "20150317626" | "20150332266" | "20150339474" | "20150371234" | "20160012465" | "20160026997" | "20160048913" | "20160055480" | "20160057619" | "20160065370" | "20160087957"					

		"20160092696" | "20160148193" | "20160232523" | "20160239672" | "20160253651" | "20160255072" | "20160267486" | "20160277383" | "20160277388" | "20160307187" | "20160307189" | "20160314472" | "20160330027" | "20160335531" | "20160379217" | "20170004502" | "20170011395" | "20170011406" | "20170017957" | "20170017964" | "20170024716" | "20170039566" | "20170041759" | "20170068950" | "20170103388" | "20170104739" | "20170109509" | "20170109730" | "20170116447" | "20170124568" | "20170140379" | "20170154328" | "20170154333" | "20170180134" | "20170221047" | "20170230189" | "20170237301" | "20170289127" | "20170295013" | "20170316696" | "20170317834" | "20170330173" | "20170374070" | "20180034507" | "20180039986").PN. OR ("20180068316" | "20180129945" | "20180160255" | "20180191501" | "20180205712" | "20180240106" | "20180254909" | "20180268132" | "20180270214" | "20180294959" | "20180300716" | "20180302396" | "20180315050"					

IPR2025-01150
Apple EX1071 Page 492

		"20180316666" | "20180322486" | "20180359100" | "20190014107" | "20190019375" | "20190036678" | "20190238517" | "4683553"	"4827113" | "4910773"	"5036461" | "5363448"	"5377270" | "5533126"	"5592553" | "5616901"	"5666415" | "5764789"	"5768373" | "5778072"	"5796827" | "5832090"	"5883810" | "5901874"	"5929413" | "5960411"	"6021203" | "6049328"	"6058373" | "6061666"	"6105013" | "6199114"	"6199762" | "6216227"	"6227447" | "6282522"	"6324271" | "6342844"	"6367011" | "6402028"	"6438550" | "6501847"	"6631197" | "6641050"	"6655585" | "6662020"	"6721706" | "6731778"	"6779115" | "6792533"	"6829711" | "6834271"	"6834795" | "6852031"	"6865547" | "6873260"	"6877656" | "6889198"	"6905411" | "6910627"	"6971031" | "6990588"	"7006986" | "7085931"	"7127605" | "7128274"	"7140550" | "7152045"	"7165727" | "7175076"	"7202773" | "7206806"	"7232073" | "7246752"	"7254569" | "7263507"	"7270276" | "7278025"	"7287692" | "7290709"	"7306143" | "7319986"	"7325132" | "7373515"	"7374099" | "7375616"	"7380710" | "7424977"	"7453439" | "7472829"	"7487357" | "7568631"	"7584153" | "7597250"	"7628322" | "7652578"	"7689832" | "7703142"	"7748609" | "7748617"	"7748636" | "7762457"	"7789302" | "7793851" | "7796013").PN. OR ("7801799"	"7801829"					

		| "7805755" | "7809643" | "7827115" | "7828214" | "7848746" | "7882553" | "7900048" | "7908216" | "7922082" | "7933589" | "7949559" | "7954716" | "7954723" | "7962369" | "7993197" | "8005426" | "8010405" | "8041954" | "8060012" | "8074877" | "8082450" | "8095113" | "8099332" | "8103249" | "8108687" | "8127143" | "8135648" | "8140010" | "8141136" | "8150321" | "8150767" | "8186602" | "8196131" | "8215563" | "8224753" | "8232879" | "8233841" | "8245292" | "8249654" | "8266451" | "8285329" | "8302872" | "8312519" | "8316237" | "8332272" | "8365988" | "8369960" | "8371501" | "8381307" | "8391719" | "8417231" | "8439271" | "8475367" | "8489112" | "8511542" | "8559872" | "8566916" | "8567670" | "8572386" | "8577810" | "8583454" | "8589335" | "8594730" | "8615468" | "8620218" | "8667285" | "8723941" | "8726405" | "8740073" | "8750514" | "8752189" | "8794509" | "8799668" | "8806592" | "8807440" | "8811892" | "8814039" | "8814052" | "8818867" | "8850538" | "8861733" | "8880027" | "8888002" | "8898088" | "8934837" | "8977569" | "8994498" | "9004365" | "9038894" | "9042814" | "9047531" | "9069976" | "9081948" | "9104853" | "9118663" | "9122964" | "9129280" | "9152832" | "9203800" | "9209867" | "9251330" | "9251518" | "9258715" | "9270337" | "9306626" | "9306942" | "9324066" | "9324067" | "9332587" | "9338622" | "9373141" | "9379841" | "9413430" | "9413768" | "9420496" | "9426132"					

		| "9432339" | "9455968" | "9473509" | "9491626" | "9553637" | "9619952" | "9635000").PN. OR ("9665858" | "9674705" | "9679286" | "9680942" | "9710804" | "9740342" | "9740988" | "9763097" | "9767329" | "9769662" | "9773151" | "9780953" | "9891823" | "9940571" | "9953323" | "9961194" | "9965756" | "9965911" | "9978058" | "RE42762").PN.					
L60	84	L40 same dynamic$6 same static$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:34 AM
L61	3	L60.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:34 AM
L62	417	("7580898").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 08:37 AM
L63	233	L39 and L62	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:38 AM
L64	87	L63 and nfc	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L65	160	L63 and online	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L66	62	L64 and L65	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L67	43	(Artificial Intelligence) Similar to: 17/528,073 with 0 CPC Selections and 0 Text Selections Text: (US-20210304187-A1 OR US-11176538-B2 OR US-20220207517-A1 OR US-20190325428-A1 OR US-10810579-B2 OR US-20220270077-A1 OR US-20210027276-A1 OR US-11328286-B2 OR US-10339520-B2 OR US-10628820-B2 OR US-20220318784-A1 OR US-20160148190-A1 OR US-20170132616-A1 OR US-9430765-B2 OR US-9760884-B2 OR US-10013693-B2 OR US-20190197520-A1 OR US-20150213351-	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN))	OR	ON	ON	2022/11/05 01:38 PM

IPR2025-01150
Apple EX1071 Page 495

		A1 OR US-20140263627-A1 OR US-20150213437-A1 OR US-9022286-B2 OR US-20180247300-A1 OR US-9224083-B2 OR US-10332101-B2 OR KR-102395069-B1 OR US-11341470-B1 OR US-20110240745-A1 OR US-10248949-B2 OR WO-2008035174-A3 OR US-20190188687-A1 OR US-5564486-A OR US-20210272091-A1 OR NL-2004464-B1 OR NL-2004464-A OR TW-200705350-A OR US-7328840-B2 OR US-10528941-B2 OR US-9830598-B2 OR WO-2006134545-A3 OR US-10984407-B2 OR US-20170109738-A1 OR US-20180005226-A1 OR US-8998096-B2 OR US-9183480-B1 OR US-20150186877-A1 OR GB-1446170-A OR WO-2018011630-A1 OR EP-3482366-A1 OR CN-111899412-A OR NL-2002671-C2).did.					
L68	35	"528073"	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2022/11/05 01:45 PM
L69	39353	(G06Q20/341 OR G06K19/06206 OR G06K19/0716 OR G06K19/07749 OR G06Q20/06 OR G06Q20/065 OR G06Q20/223 OR G06Q20/24 OR G06Q20/346 OR G06Q20/347 OR G06Q20/352 OR G06Q20/3827 OR G06Q20/385 OR G06Q20/4012 OR G06Q20/409 OR G07F7/0873 OR G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2022/11/05 02:30 PM
L70	336	69 AND dynamic$6 SAME generat$4 SAME nfc	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2022/11/05 03:37 PM
L71	161	card SAME issu$4	(US-PGPUB; USPAT;	OR	OFF	OFF	2022/11/05

IPR2025-01150
Apple EX1071 Page 496

		SAME dynamic$6 SAME generat$4 SAME nfc	EPO; JPO)				03:38 PM
L72	66	69 AND 71	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2022/11/05 03:38 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

PE2E SEARCH - Search History (Similarity Search)

Ref #	Application Number	Text Selections	CPC Selections
L67	17/528,073	No selections	No selections

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2876	3750	WYAT-0002.USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

OC000000136882754

Date Mailed: 11/17/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

David WYATT, San Jose, CA;

Applicant(s)

CARDWARE, INC, San Jose, CA;

Power of Attorney: The patent practitioners associated with Customer Number 136197

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

IPR2025-01150
Apple EX1071 Page 498

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

IPR2025-01150
Apple EX1071 Page 499

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01150
Apple EX1071 Page 501

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	17528073	Filing Date	2021-11-16	Docket Number (if applicable)	WYAT-0002-13C12US	Art Unit	2876
First Named Inventor	David WYATT			Examiner Name	LEE, SEUNG H.		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☒ Enclosed

☐ Amendment/Reply

☒ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 504160

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) UK Patent Application (19) GB (11) 2485442 (13) A

(43) Date of A Publication 16.05.2012

(21) Application No: 1118513.9

(22) Date of Filing: 26.10.2011

(30) Priority Data:
(31) 61406821 (32) 26.10.2010 (33) US
(31) 13281272 (32) 25.10.2011 (33) US

(71) Applicant(s):
Cubic Corporation
(Incorporated in USA – California)
9333 Balboa Avenue, San Diego, California 92123, United States of America

(72) Inventor(s):
Philip B Dixon
David Lapczynski

(74) Agent and/or Address for Service:
J A Kemp
14 South Square, Gray's Inn, London, WC1R 5JJ, United Kingdom

(51) INT CL:
G06Q 50/30 (2012.01) ***G06Q 20/22*** (2012.01)

(56) Documents Cited:
None

(58) Field of Search:
Other: **No search performed: Section 17(5)(b)**

(54) Title of the Invention: **Determining companion and joint cards in transit**
Abstract Title: **Analysis of transport identifier data to recognize potential patterns, relationships or sequences that could represent misuse of an account**

(57) Detecting potential misuse of a primary account number (PAN) associated with a first handheld media in a transit system having one or more access points, including creating a user account, enrolling a first handheld media for use as a fare media for a transit product, where the PAN is stored in the user account, receiving a plurality of fare transaction records, each fare transaction record includes the PAN associated with the first handheld media and a transaction identifier, determining a potential misuse of a handheld media associated with the PAN based on at least the relationship, pattern or sequence between a plurality of the transaction identifiers and in response an action is taken related to using the first handheld media as a fare media for the transit product.

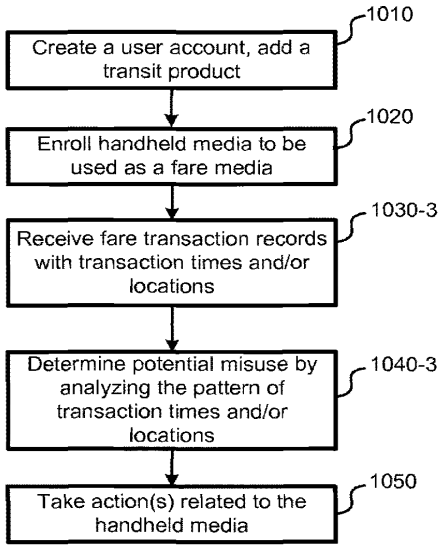


FIG. 10C

GB 2485442 A

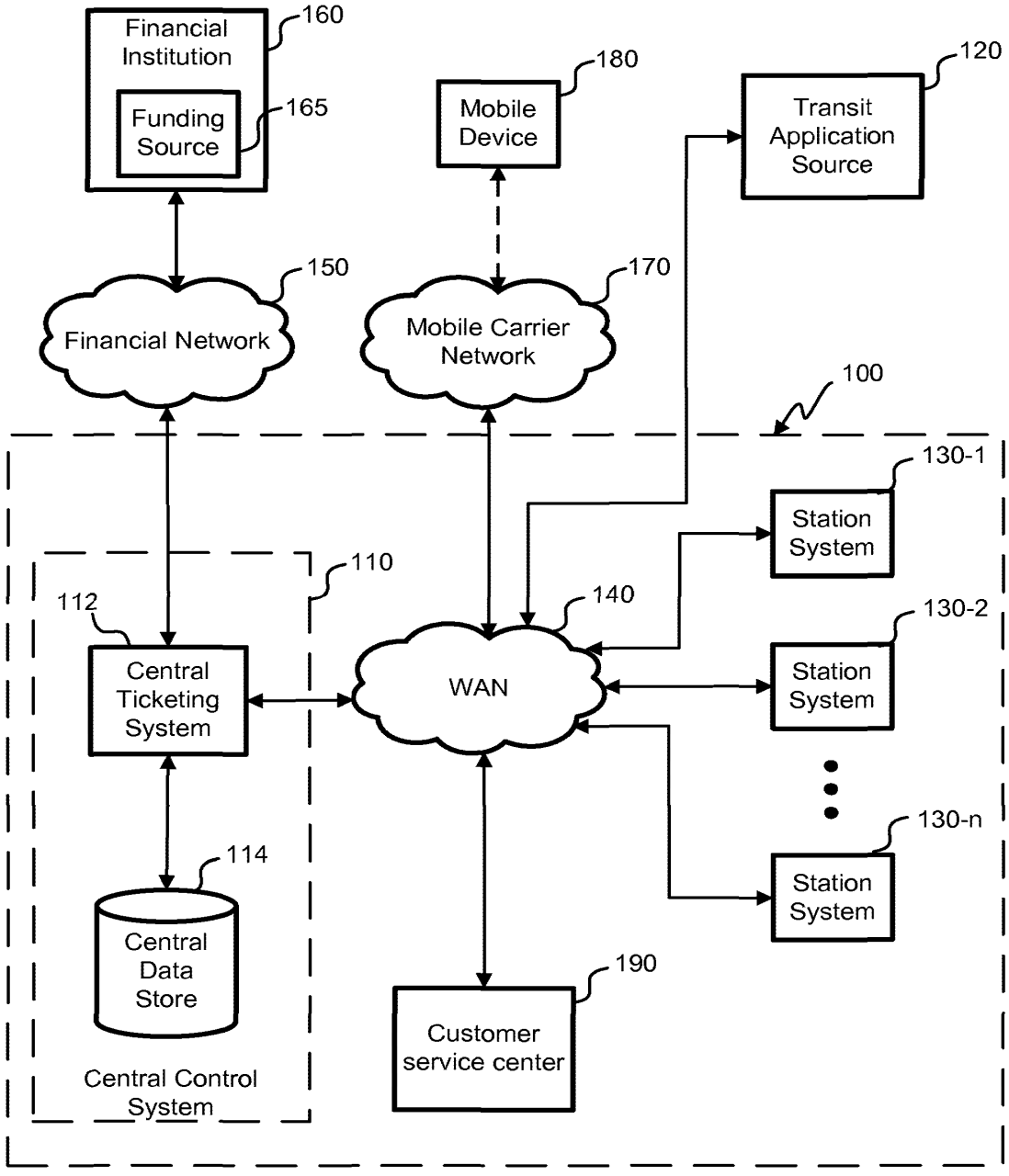

Financial Institution
160
Funding Source
165
Mobile Device
180
Transit Application Source
120
Financial Network
150
Mobile Carrier Network
170
100
130-1
Station System
110
112
140
130-2
Central Ticketing System
WAN
Station System
130-n
114
Station System
Central Data Store
190
Customer service center
Central Control System

FIG. 1

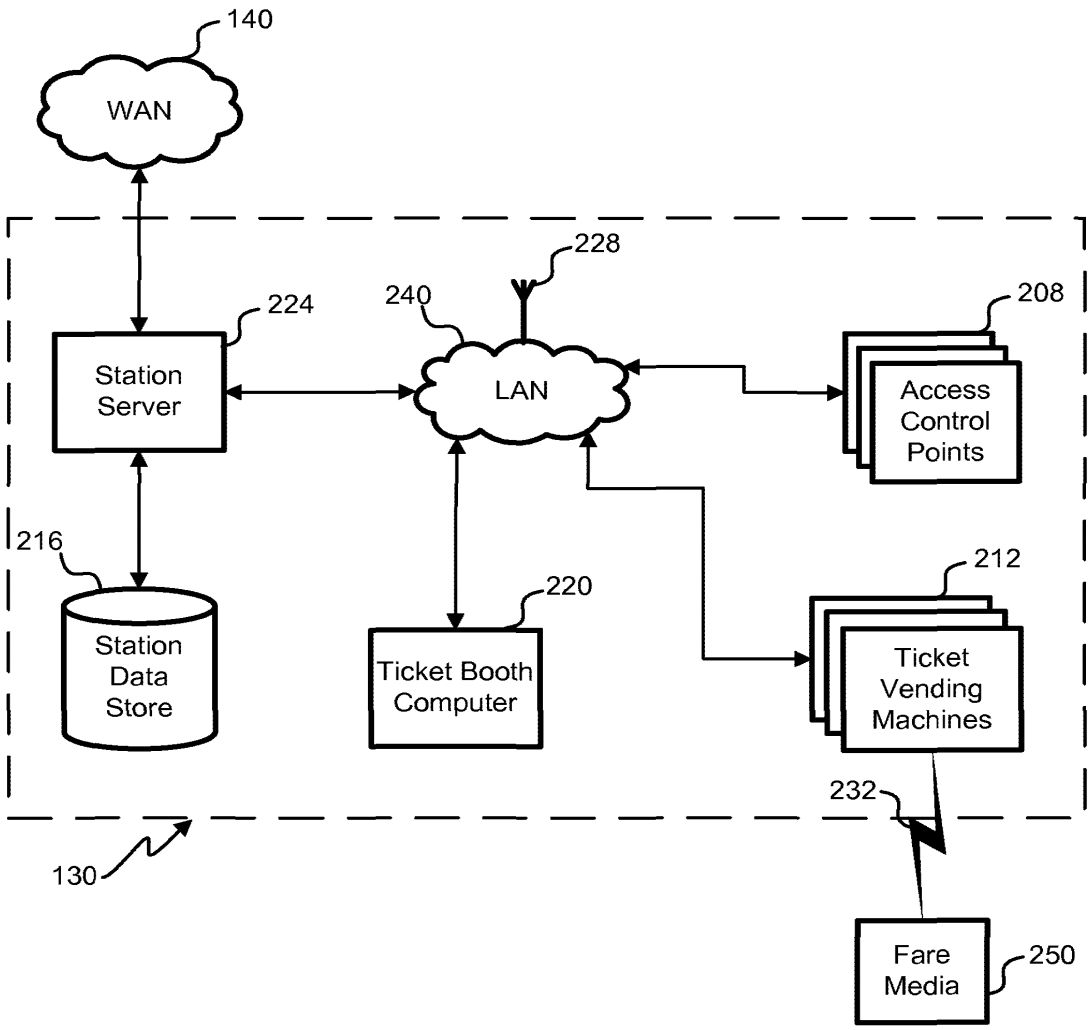

140
WAN
228
240
224
208
Station Server
LAN
Access Control Points
216
212
220
Station Data Store
Ticket Booth Computer
Ticket Vending Machines
232
130
Fare Media
250

FIG. 2

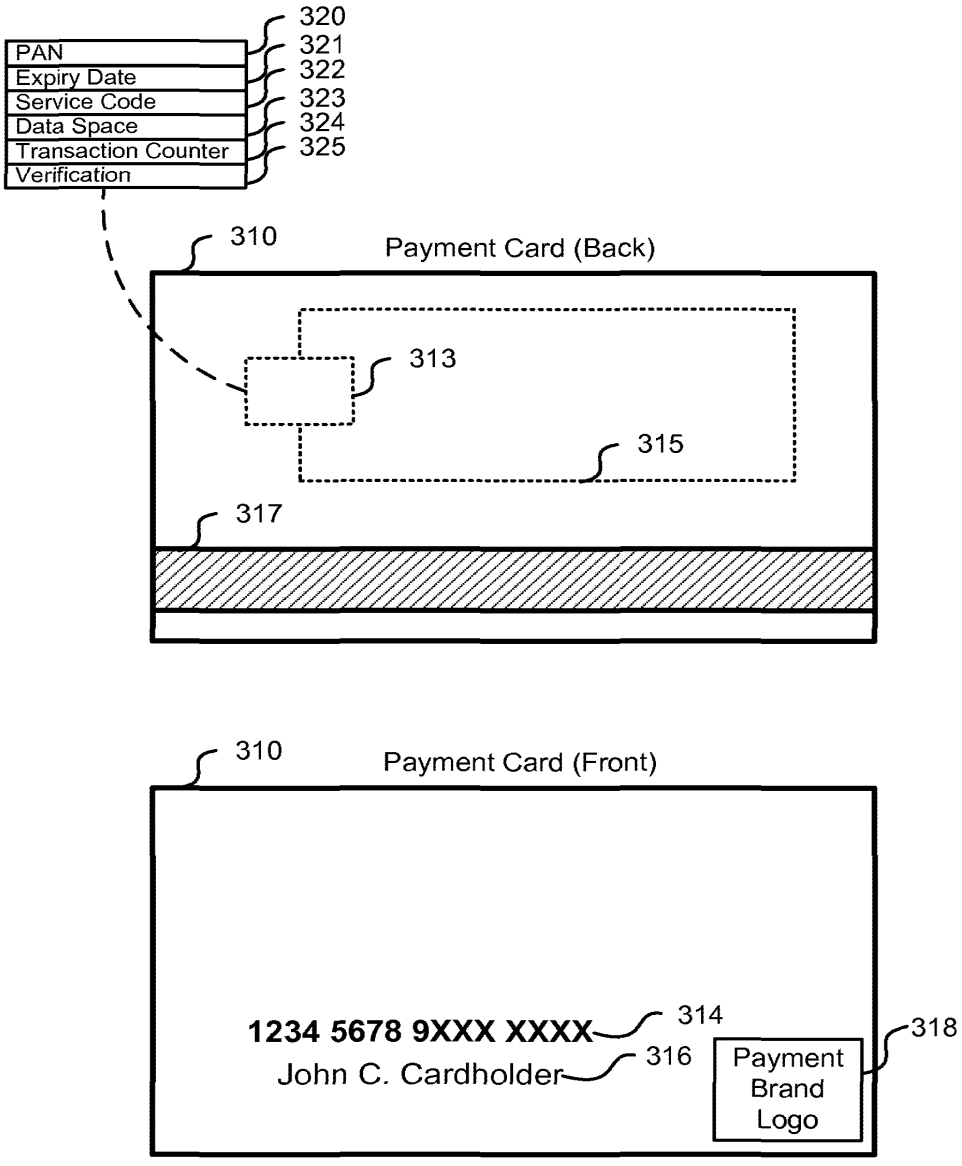

320
PAN
321
Expiry Date
322
Service Code
323
Data Space
324
Transaction Counter
325
Verification
310
Payment Card (Back)
313
315
317
310
Payment Card (Front)
1234 5678 9XXX XXXX
314
John C. Cardholder
316
Payment Brand Logo
318

FIG. 3

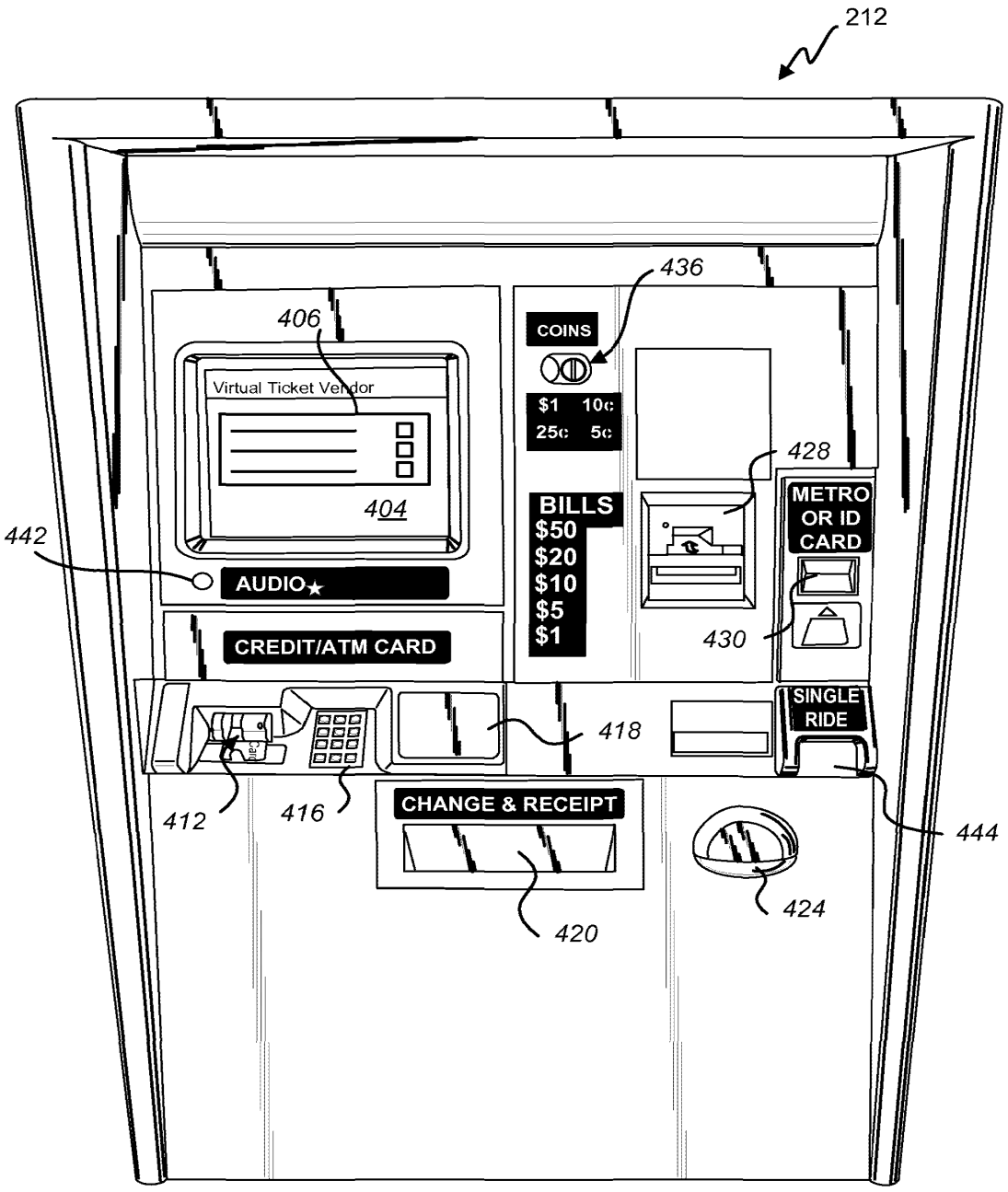

212
436
406
COINS
Virtual Ticket Vendor
$1 10¢
25¢ 5¢
428
404
BILLS
$50
$20
$10
$5
$1
METRO OR ID CARD
442
AUDIO
CREDIT/ATM CARD
430
SINGLE RIDE
418
412
416
CHANGE & RECEIPT
444
424
420

FIG. 4

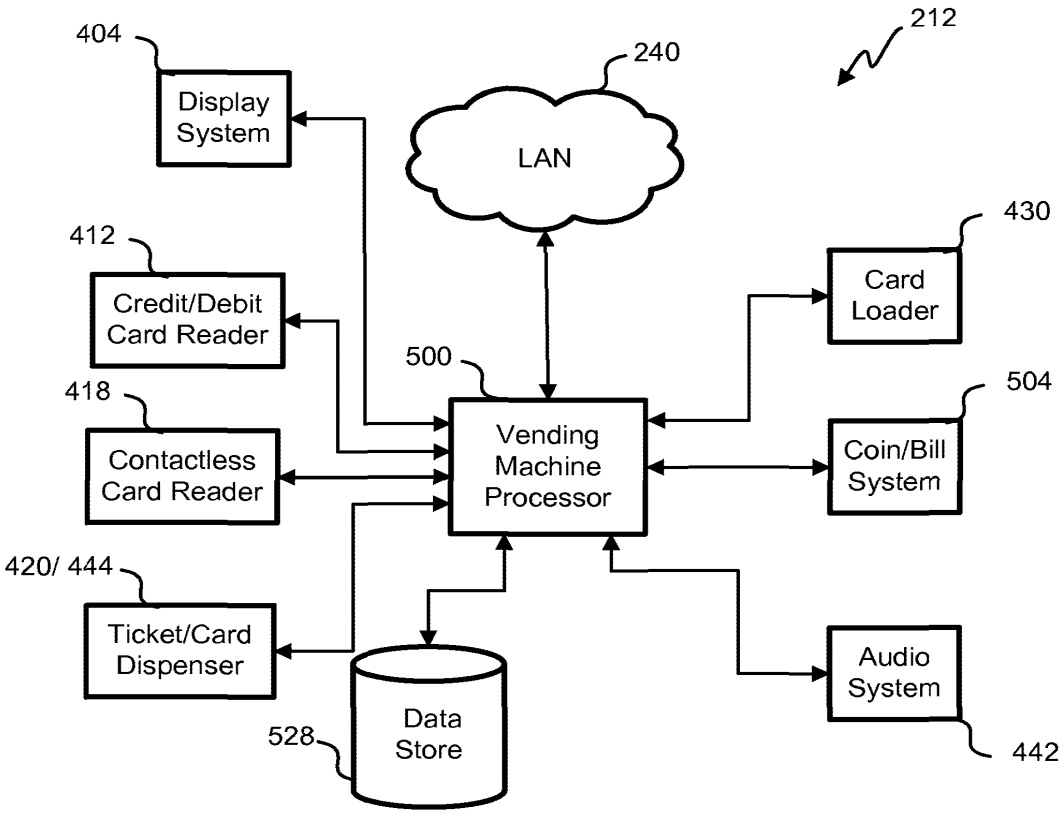

404
Display System
240
LAN
212
412
Credit/Debit Card Reader
430
Card Loader
500
418
Contactless Card Reader
Vending Machine Processor
504
Coin/Bill System
420/ 444
Ticket/Card Dispenser
Audio System
528
Data Store
442

FIG. 5

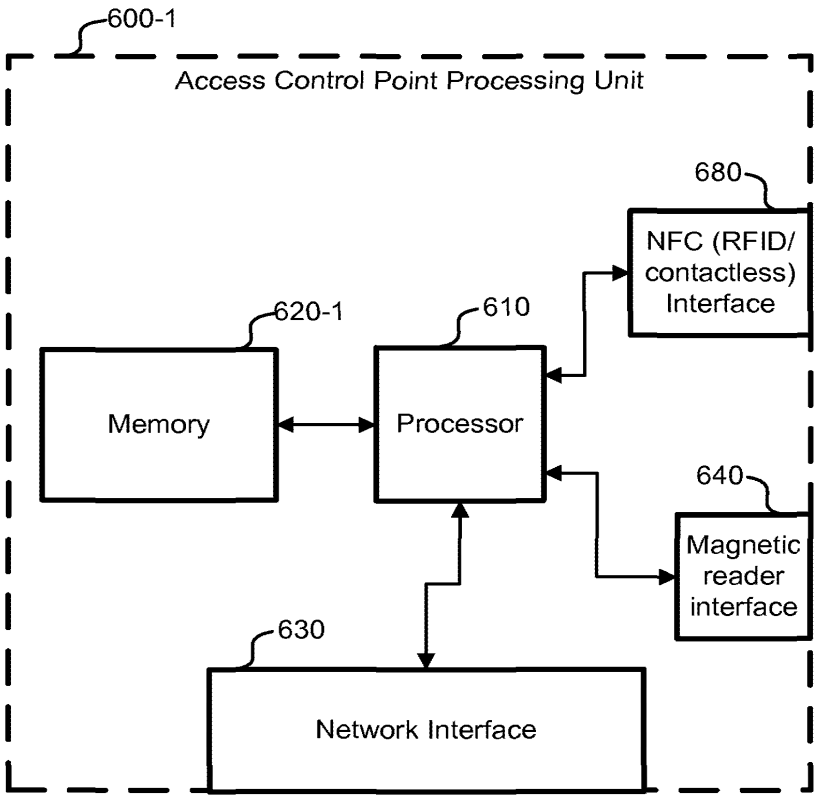

600-1
Access Control Point Processing Unit
680
NFC (RFID/ contactless) Interface
620-1
610
Memory
Processor
640
Magnetic reader interface
630
Network Interface

FIG. 6A

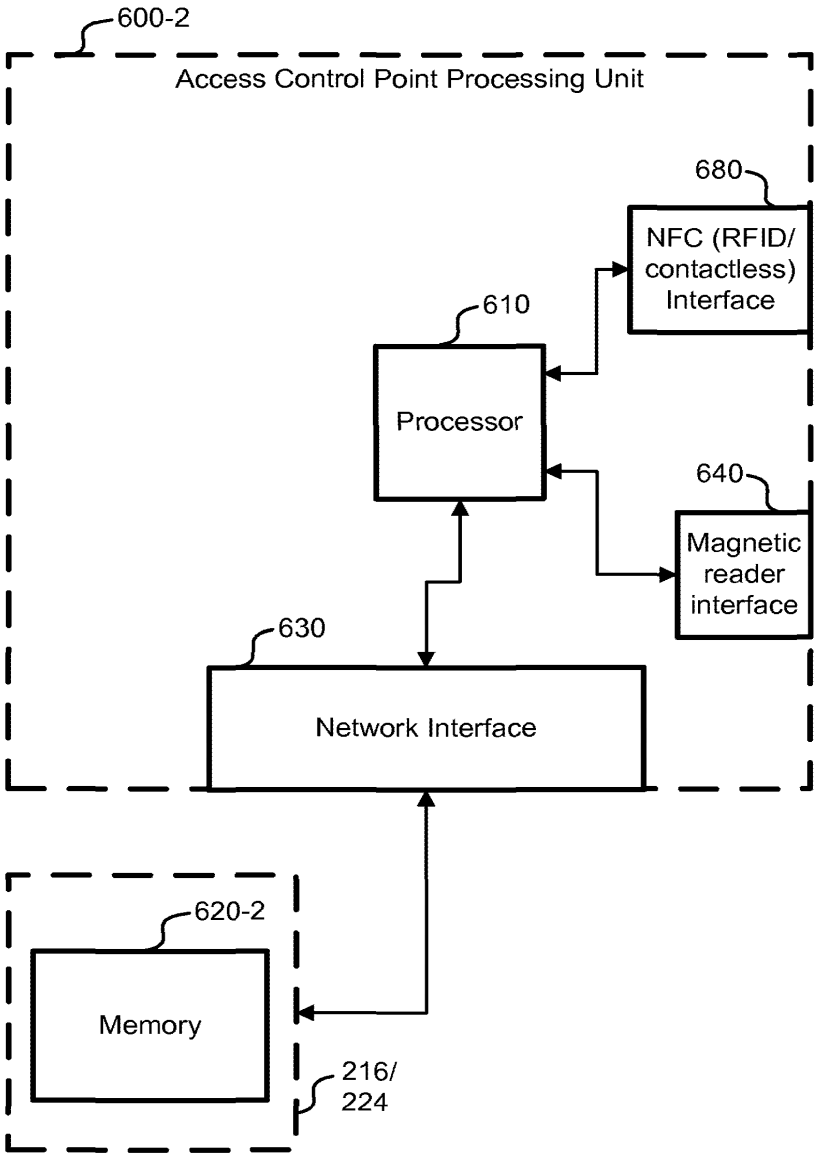

600-2
Access Control Point Processing Unit
680
NFC (RFID/ contactless) Interface
610
Processor
640
Magnetic reader interface
630
Network Interface
620-2
Memory
216/ 224

FIG. 6B

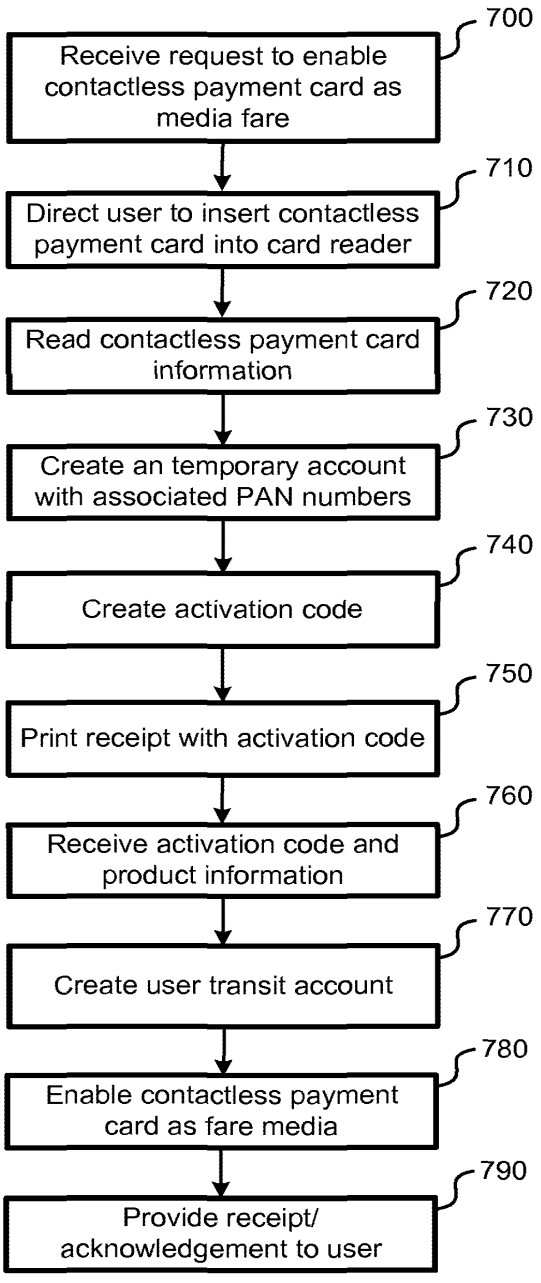

700
Receive request to enable contactless payment card as media fare
710
Direct user to insert contactless payment card into card reader
720
Read contactless payment card information
730
Create an temporary account with associated PAN numbers
740
Create activation code
750
Print receipt with activation code
760
Receive activation code and product information
770
Create user transit account
780
Enable contactless payment card as fare media
790
Provide receipt/ acknowledgement to user

FIG. 7A

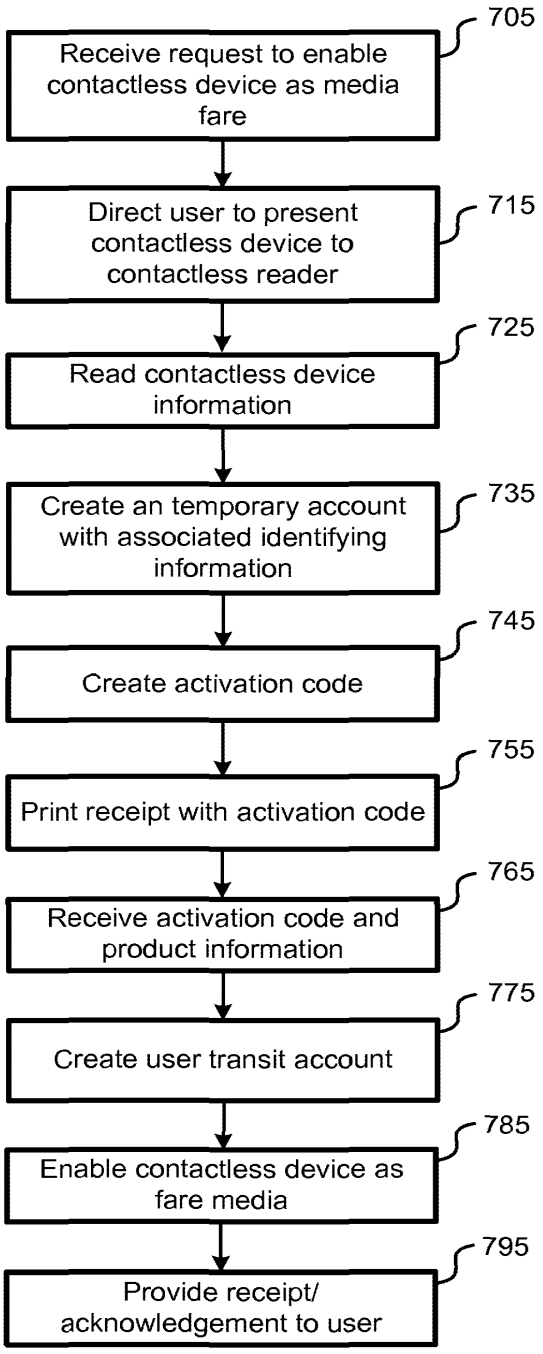

705
Receive request to enable contactless device as media fare
715
Direct user to present contactless device to contactless reader
725
Read contactless device information
735
Create an temporary account with associated identifying information
745
Create activation code
755
Print receipt with activation code
765
Receive activation code and product information
775
Create user transit account
785
Enable contactless device as fare media
795
Provide receipt/ acknowledgement to user

FIG. 7B

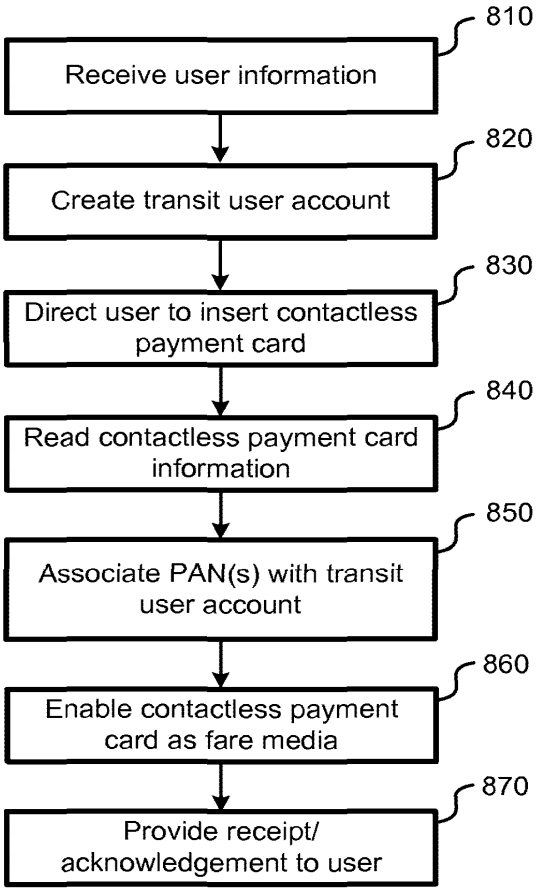

810
Receive user information
820
Create transit user account
830
Direct user to insert contactless payment card
840
Read contactless payment card information
850
Associate PAN(s) with transit user account
860
Enable contactless payment card as fare media
870
Provide receipt/ acknowledgement to user

FIG. 8A

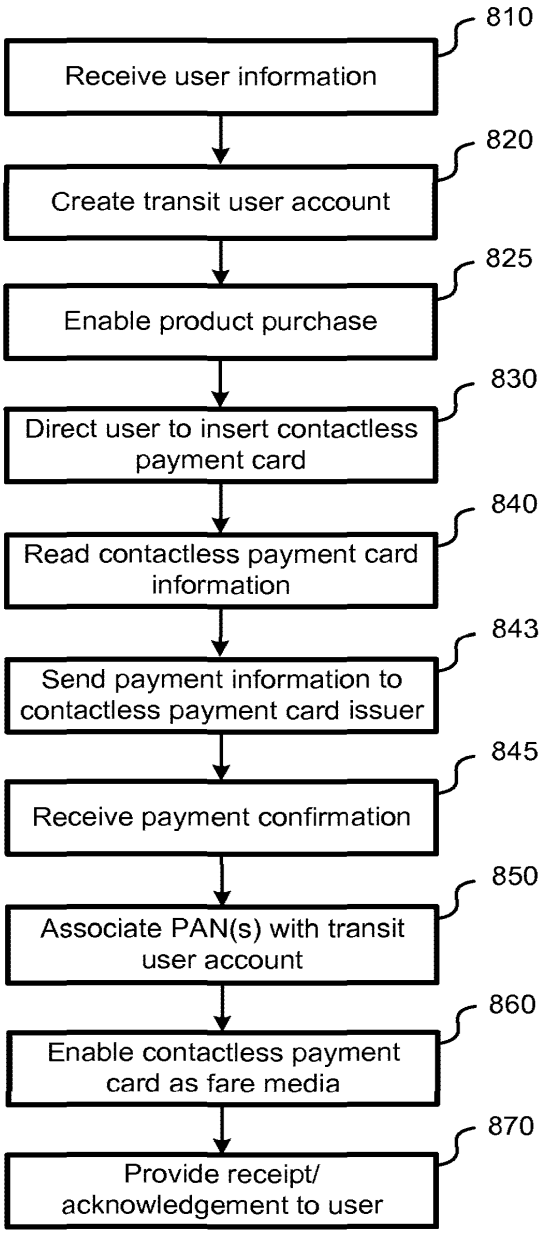

810
Receive user information
820
Create transit user account
825
Enable product purchase
830
Direct user to insert contactless payment card
840
Read contactless payment card information
843
Send payment information to contactless payment card issuer
845
Receive payment confirmation
850
Associate PAN(s) with transit user account
860
Enable contactless payment card as fare media
870
Provide receipt/ acknowledgement to user

FIG. 8B

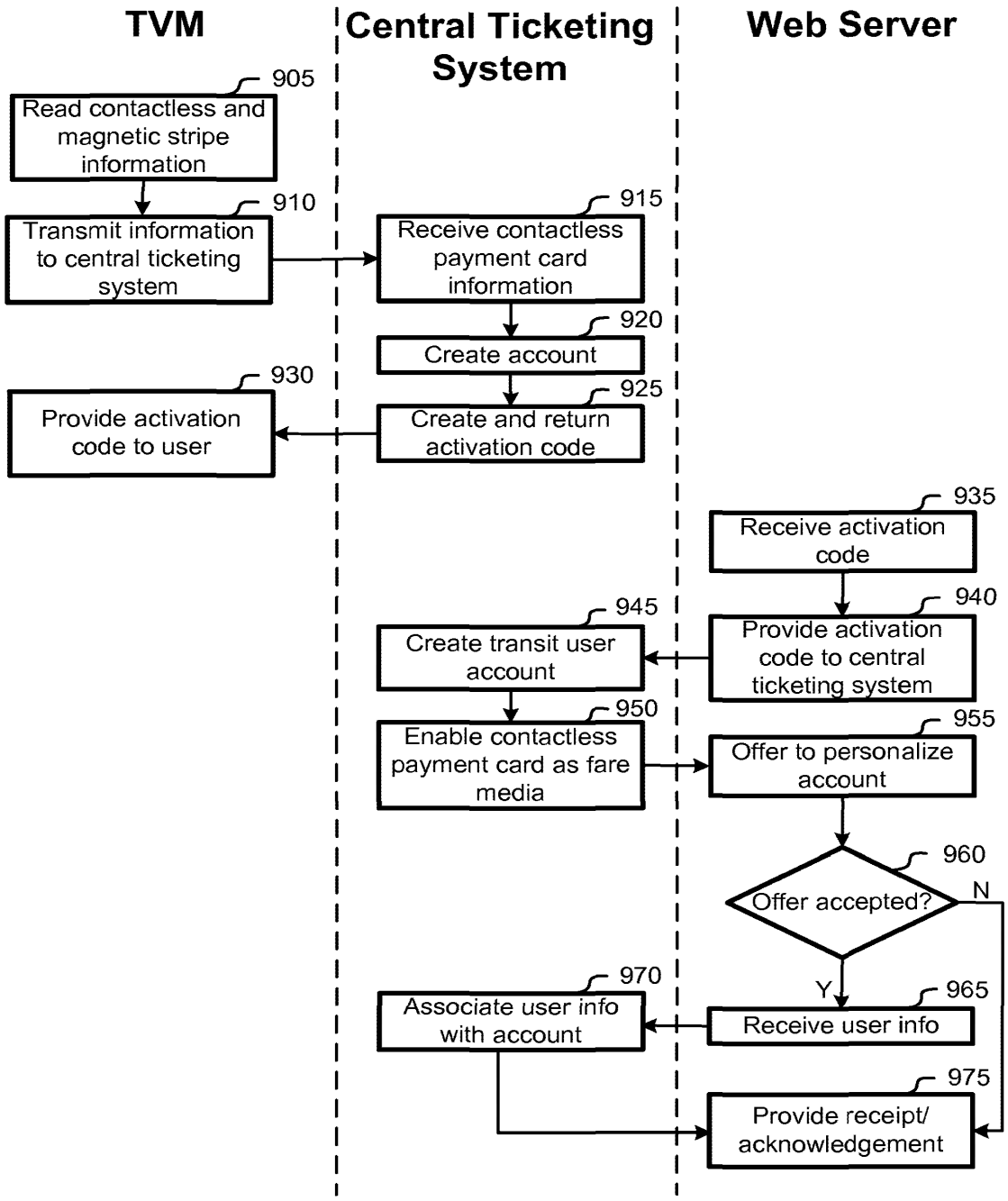

TVM
Central Ticketing System
Web Server
905
Read contactless and magnetic stripe information
910
Transmit information to central ticketing system
915
Receive contactless payment card information
920
Create account
925
Create and return activation code
930
Provide activation code to user
935
Receive activation code
940
Provide activation code to central ticketing system
945
Create transit user account
950
Enable contactless payment card as fare media
955
Offer to personalize account
960
Offer accepted?
N
Y
965
Receive user info
970
Associate user info with account
975
Provide receipt/ acknowledgement

FIG. 9

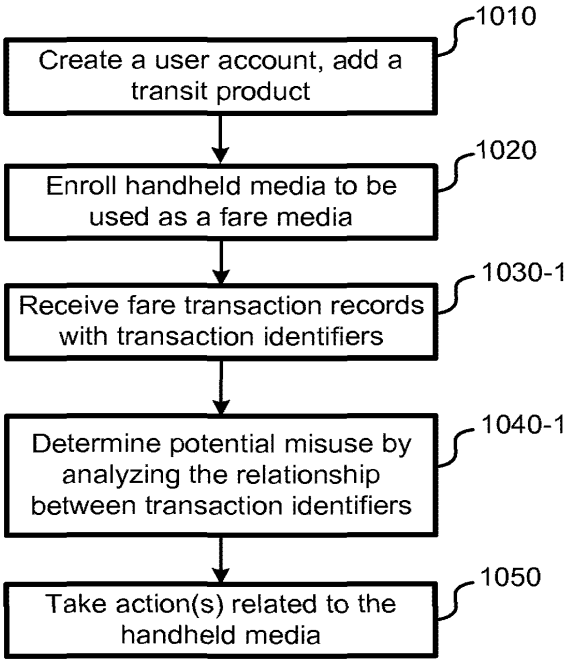

1010
Create a user account, add a transit product
1020
Enroll handheld media to be used as a fare media
1030-1
Receive fare transaction records with transaction identifiers
1040-1
Determine potential misuse by analyzing the relationship between transaction identifiers
1050
Take action(s) related to the handheld media

FIG. 10A

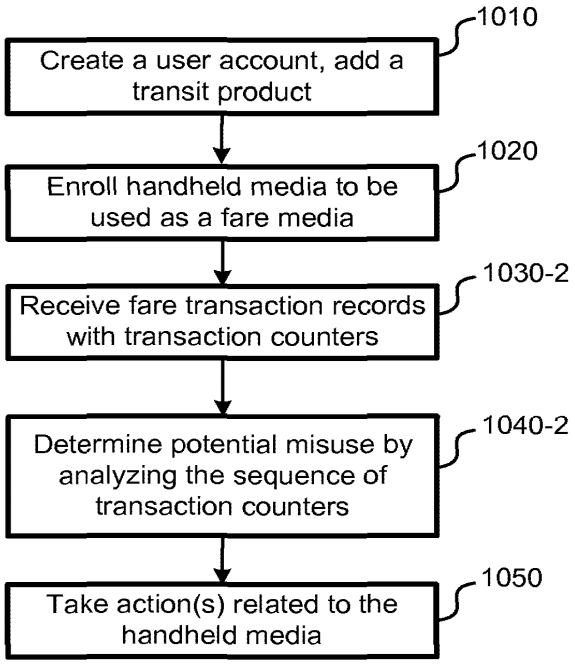

1010
Create a user account, add a transit product
1020
Enroll handheld media to be used as a fare media
1030-2
Receive fare transaction records with transaction counters
1040-2
Determine potential misuse by analyzing the sequence of transaction counters
1050
Take action(s) related to the handheld media

FIG. 10B

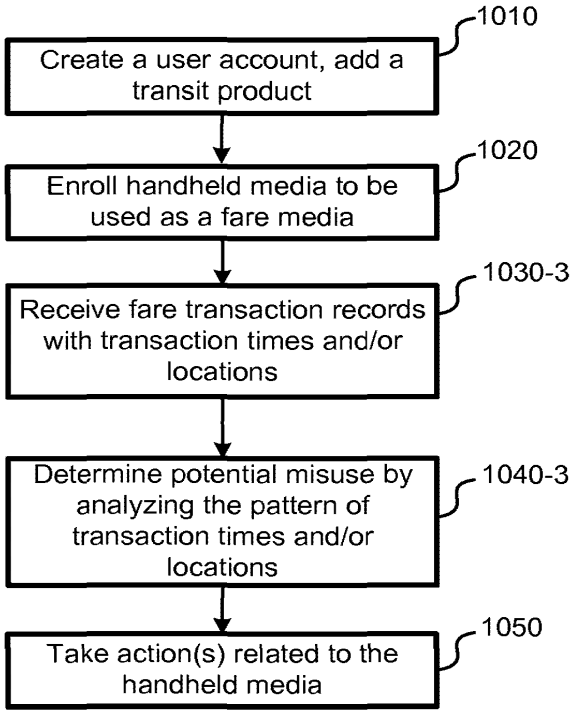

1010
Create a user account, add a transit product
1020
Enroll handheld media to be used as a fare media
1030-3
Receive fare transaction records with transaction times and/or locations
1040-3
Determine potential misuse by analyzing the pattern of transaction times and/or locations
1050
Take action(s) related to the handheld media

FIG. 10C

DETERMINING COMPANION AND JOINT CARDS IN TRANSIT

[0001] This application claims priority to Provisional U.S. Patent Application Number 61/406,821 filed October 26, 2010, entitled "Determining Companion and Joint Cards in Transit," of which the entire disclosure is hereby incorporated by reference for all purposes.

CROSS-REFERENCES TO RELATED APPLICATIONS

[0002] The present application is also related to U.S. Patent Application No. 12/877,691, filed on September 8, 2010, entitled "Association of Contactless Payment Card Primary Account Number," which is incorporated herein by reference for all purposes.

BACKGROUND

[0003] As transit systems throughout the world continue to mature, so do the technologies that support them. Many transit systems use impersonalized fare media that carry a value, such as stored-value cards, but other transit systems are taking a more personalized, account-based approach. Account-based transit systems can provide transit users with a personalized account, which can store product and funding information. Because value is associated with an account rather than a fare media, a transit system can disable a lost or stolen fare media and issue a new fare media to a transit user without the loss of any value to either the transit user or the transit system.

[0004] Because fare media does not store a value in these account-based transit systems, items other than those issued by a transit system may be enabled for use as fare media. Payment cards, for example, can be configured for use in such account-based transit systems. For transit systems utilizing wireless, or contactless, technology, contactless payment cards may be used. Occasionally, this process may be not be straight forward if multiple fare media become associated with the same primary account number, or if multiple users use the same fare media to access a transit product meant to be used by a single person.

BRIEF SUMMARY

[0005] Embodiments of methods and machines are disclosed for detecting potential misuse of handheld media, such as contactless payment cards and/or other devices having near-field communication (NFC) capabilities, for use as fare media in a transit and/or transportation system. Embodiments include reading contactless data from a contactless device and associating it with information received from another source on the device. For example, associating a primary account number (PAN) and/or other information received from a contactless payment card's

IPR2025-01150
Apple EX1071 Page 521

contactless interface with a PAN obtained from a magnetic stripe of the contactless payment card. The information can then be further associated with one or more products and/or a transit user account. A plurality of transaction identifiers may be collected from fare transactions at the transit station's access control points, and potential misuse of the PAN and/or handheld media may be determined, at least in part, by analyzing the relationship between a plurality of the transaction identifiers.

[0006] An example method for detecting potential misuse of a primary account number associated with a handheld media in a transit system having one or more access points, according to the description, may include creating a user account for managing transactional information, where the user account includes at least one transit product. The method may also include enrolling the handheld media for use as fare media for at least one of the transit products, where the PAN is stored in the user account. A plurality of fare transaction records are received from one or more access points of the transit system, and each fare transaction record may include the PAN associated with the handheld media and a transaction counter. The method may additionally include determining that a potential misuse of a handheld media associated with the PAN has occurred. The determination may be based, at least in part, on a sequence of the transaction counters from the fare transaction records. Finally, the method includes taking an action related to using the handheld media as fare media for the transit product.

[0007] The example method for detecting potential misuse of a PAN associated with a handheld media may include one or more of the following features. The handheld media may be a smart card having near-field communication capabilities, and the transaction counter may increment at least every time the handheld media is used at the access points and may be stored on the handheld media. The potential misuse may be determined by identifying gaps in the sequence of the plurality of transaction counters. The potential misuse may also be determined by determining that the sequence of transaction counters is not ascending. The potential misuse may also be determined by comparing the sequence of transaction counters to a user profile and identifying deviations. Additionally, each fare transaction record may also include a transaction time and a transaction location, and the potential misuse may also be determined, at least in part, on a pattern of the transaction times and locations from the fare transaction records.

[0008] Another example method for detecting potential misuse of a primary account number associated with a handheld media in a transit system having one or more access points, according to the description, may include creating a user account for managing transactional information,

IPR2025-01150
Apple EX1071 Page 522

where the user account includes at least one transit product. The method may also include enrolling the handheld media for use as fare media for at least one of the transit products, where the PAN is stored in the user account. A plurality of fare transaction records are received from one or more access points of the transit system, and each fare transaction record may include the PAN associated with the handheld media and a transaction time and location. The method may additionally include determining that a potential misuse of a handheld media associated with the PAN has occurred. The determination may be based, at least in part, on a pattern of the transaction times and locations from the fare transaction records. Finally, the method may also include taking an action related to using the handheld media as fare media for the transit product.

[0009] The example method for detecting potential misuse of a primary account number associated with a handheld media may include one or more of the following features. The potential misuse may be determined by indentifying multiple fare transactions that take place within a predetermined time window. The potential misuse may also be determined by indentifying fare transactions at distant locations that occur within a predetermined time window. The potential misuse may also be determined by indentifying first and second fare transactions where travel time between the locations exceeds a difference between the transaction times of the transactions. The potential misuse may also determined by comparing the pattern of the transaction times and locations to a user profile and identifying deviations. Finally, each transaction record may also include a plurality of transaction counters, and the potential misuse may also be determined, at least in part, on a sequence of the transaction counters.

[0010] An example server for detecting potential misuse of a PAN associated with a handheld media in a transit system, according to the description may include a network interface configured to communicate with a network, an input interface configured to receive information from one or more of the access points of the transit system, and a processor communicatively coupled with the network interface, the input interface, and a memory. The memory may contain instructions that cause the server to create a user account for managing transactional information in the memory. The user account may include a transit product, and a handheld media may be enrolled for use as fare media for the transit product. The PAN may be stored in the user account. The memory also may contain instructions that cause the server to receive, from the input interface, a plurality of fare transaction records, where each fare transaction record includes the PAN associated with the handheld media and a transaction identifier. The memory may also contain instructions that cause the server to determine potential misuse of a handheld media associated with the PAN based, at

IPR2025-01150
Apple EX1071 Page 523

least in part, on a relationship between some of the transaction identifiers from the fare transaction records. Finally, the memory may also contain instructions that cause the server to take an action related to using the handheld media as fare media for using the transit product.

[0011] The example server for detecting potential misuse of a PAN associated with a handheld media in a transit system may include one or more of the following features. Each transaction identifier may include a transaction counter, and the potential misuse may be determined, at least in part, on a sequence of the transaction counters. Each transaction identifier may include a transaction time and location, and the potential misuse may be determined, at least in part, on a pattern of the transaction times and locations. The action related to using the handheld media as fare media for using the transit product may include denying future use as fare media of any handheld media associated with the PAN. The action related to using the handheld media as fare media for using the transit product may also include charging the user account a fee for one or more of the fare transaction records. Finally, the server may also include an output interface configured to send notifications associated with potential misuse of the handheld media associated with the PAN, and the action related to using the handheld media as fare media for using the transit product comprises sending, from the output interface, a notification regarding the potential misuse of the handheld media associated with the PAN.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 is a block diagram of an embodiment of a transit system providing transit user accounts for management of transactions of a user of the transit system.

[0013] FIG. 2 is a block diagram of an embodiment of a transit station system.

[0014] FIG. 3 is a simplified illustration of front and back views of a contactless payment card that can be enabled as fare media in a transit system, according to certain embodiments.

[0015] FIG. 4 is a perspective view of an embodiment of a transit vending machine that can be used to enable contactless devices, such as a contactless payment card, for use as fare media.

[0016] FIG. 5 is a block diagram of an embodiment of a transit vending machine that can be used to enable contactless devices, such as a contactless payment card, for use as fare media.

[0017] FIG. 6A is a simplified block diagram of an embodiment of an access control point processing unit of a transit system.

[0018] FIG. 6B is a simplified block diagram of an alternative embodiment of an access control point processing unit of a transit system.

IPR2025-01150
Apple EX1071 Page 524

[0019] FIG. 7A is a diagram of a method for enabling a contactless payment card to be used as fare media in a transit system, according to some embodiments.

[0020] FIG. 7B is a diagram of an alternative method for enabling a contactless payment card to be used as fare media in a transit system, according to some embodiments.

[0021] FIG. 8A is a block diagram of yet another method for enabling a contactless payment card for use as fare media in a transit system, according to some embodiments.

[0022] FIG. 8B is an embodiment of a method that incorporates the enablement of a contactless payment card for use as fare media with the payment of a transit and/or transportation product using the contactless payment card.

[0023] FIG. 9 is a swim-lane diagram of yet another embodiment of a method for enabling a contactless payment card for use as fare media.

[0024] FIG. 10A is a block diagram of an embodiment for detecting potential misuse of a fare media using transaction identifiers.

[0025] FIG. 10B is a block diagram of an embodiment for detecting potential misuse of a fare media using transaction counters as transaction identifiers.

[0026] FIG. 10C is a block diagram of an embodiment for detecting potential misuse of a fare media using transaction times and/or locations as transaction identifiers.

DETAILED DESCRIPTION

[0027] In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of various embodiments. It will be apparent, however, to one skilled in the art that various embodiments may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form.

[0028] The ensuing description provides exemplary embodiments only, and is not intended to limit the scope, applicability, or configuration of the disclosure. Rather, the ensuing description of the exemplary embodiments will provide those skilled in the art with an enabling description for implementing an exemplary embodiment. It should be understood that various changes may be made in the function and arrangement of elements without departing from the spirit and scope of the disclosed systems and methods as set forth in the appended claims.

[0029] Specific details are given in the following description to provide a thorough understanding of the embodiments. However, it will be understood by one of ordinary skill in the art that the embodiments may be practiced without these specific details. For example, circuits,

IPR2025-01150
Apple EX1071 Page 525

systems, networks, processes, and other components may be shown as components in block diagram form in order not to obscure the embodiments in unnecessary detail. In other instances, known circuits, processes, algorithms, structures, and techniques may be shown without unnecessary detail in order to avoid obscuring the embodiments.

[0030] Also, it is noted that individual embodiments may be described as a process which is depicted as a flowchart, a flow diagram, a data flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed, but could have additional steps not included in a figure. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination can correspond to a return of the function to the calling function or the main function.

[0031] Furthermore, embodiments may be implemented by hardware, software, firmware, middleware, microcode, hardware description languages, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine readable medium. A processor(s) may perform the necessary tasks.

[0032] The term "payment brand" as used herein includes, but is not limited to payment card networks, such as VISA®, MASTERCARD®, AMERICAN EXPRESS®, and DISCOVER®. These networks may issue payment cards, such as reloadable prepaid cards, directly or though a separate card issuer, such as an authorized issuing bank. Furthermore, payment-branded cards as described herein may be "co-branded," meaning that the cards may be accepted, issued, and/or authorized by a transit agency or other entity in addition to a bank and/or payment brand.

[0033] Account-based transit systems are uncommon among current transit systems. Because transit systems require quick transactions, it is easier to use stored-value fare media (e.g., fare media, such as a transit fare card, that can store a value and a trip history on the card). However, encoding the value or transit product onto a fare media, rather than associate the value or fare media to a transit user, has its limitations. If the fare media is lost or stolen, it is difficult to remove the value from the lost or stolen fare media and restore it to a transit user. On the other hand, an account-based transit system can enable a transit user to enroll a variety of items as fare media. The fare media can be disabled if lost or stolen, without any lost value to the account.

IPR2025-01150
Apple EX1071 Page 526

And the account may be linked to a funding source to conveniently increase the account value and purchase additional products.

[0034] **FIG. 1** illustrates a block diagram of an embodiment of a transit system 100, in communication with other systems, providing transit user accounts for management of transactions of users of the transit system 100. The transit system can include various forms of transit, including subway, bus, ferry commuter rail, para-transit, etc., or any combination thereof. The transit user account can comprise information regarding a certain user of the transit system 100, such as a name, address, phone number, email address, user identification (such as a unique identifier of the user or other user ID), passcode (such as a password and/or personal identification number (PIN)), an identification code associated with a fare media used to identify a user and/or a transit user account (such as a primary account number (PAN)), information regarding user preferences and user opt-in or opt-out selections for various services, product(s) associated with the transit user account, a value and/or credit associated with the product(s), information regarding a funding source 165 for the transit user account, and more. The transit user account can further comprise funding and transaction information, such as product information, a funding source, and a payment amount. A transit user may request a transit user account and provide the information listed above by phone (such as a call to a customer service center 190 maintained and/or provided by the transit service provider of the transit system 100), on the Internet, at ticket booth, at a ticket venting machine, or by other means. A central ticketing system 112, which can comprise of one or more servers and/or other computing systems having processors, memories, and network interfaces for processing and communicating information. The central ticketing system 112 can use the information provided by the user to create the transit user account, which can be stored and/or maintained on a database, such as a central data store 114 of a central control system 110. It will be recognized that such a transit system 100 can be enabled for use in applications beyond transit, such as transportation systems (e.g., airline systems, car rental systems, etc.).

[0035] A funding source 165 for a transit user account can provide funding to purchase products of the transit services system. It can be external to the central control system 110 and maintained, for example, by a financial institution 160. Such a funding source 165 may include a savings or checking account, a prepaid account, a credit account, an e-commerce account (such as a PAYPAL® account), or more, which can transfer funds via automated clearing house (ACH) or other means. If a transit user account comprises information regarding a funding source 165 for

IPR2025-01150
Apple EX1071 Page 527

the account, the central ticketing system 112 can use the information to fund purchases or other transactions of a user of the transit system 100. These transactions can be made at stations, on the Internet, by phone, text, email, or a variety of other different ways, and transaction information can then be sent to the central ticketing system 112 to update the transit user account associated with the transactions and reconcile payments and purchases with the funding source 165. The central ticketing system 112 can communicate with the financial institution 160 (or other entity maintaining the funding source 165) through a financial network 150.

[0036] The central ticketing system's reconciliation with a funding source 165 may vary depending on one or more products associated with the transit user account and the functionality desired by a transit services provider. For example, the transit user account may include a running balance mirroring a balance of the funding source 165. In such a case, transactions, such as passage of a user at an access control point (such as a turnstile, faregate, platform validator, para-transit vehicle, bus, conductor handheld unit, or fare box at a entry, exit, or other location of a transit station) can be recorded and/or tracked by the central ticketing system 112 and reconciled, on a per-transaction basis and/or collectively with other transactions. Along these lines, the central ticketing system 112 may reconcile payment for the transactions with the funding source 165 as the transactions are received and/or on a scheduled basis, such as on an hourly or daily basis.

[0037] Additionally or alternatively, when transit products or services are associated with a transit user account, the central ticketing system 112 can draw funds from a funding source 165 less frequently. For example, a transit product can include a certain number of rides or an unlimited number of rides for a certain period of time. In this case, the central ticketing system 112 can track transactions associated with the passage of a user at an access control point (i.e., transactions in the transit system associated with a ride), but may only need to reconcile with the funding source 165 once, for the purchase of the transit product.

[0038] The transit user account may further include information regarding a user's preferences with regard to funding. For example, the transit user account may be configured to automatically draw a certain amount of funds from the funding source 165 each month to pay for a certain transit product or service, or to add value and/or credits to an existing transit product or service. The value and/or credits can include a monetary credit, a usage credit, and/or a usage period. Additionally or alternatively, the transit user account can be configured to automatically withdraw a certain amount of funds from the funding source 165 to add additional value and/or credits to an

IPR2025-01150
Apple EX1071 Page 528

existing product when the value and/or credits of the existing product drops below a certain threshold level. Various other configurations are allowable by the transit user account. It will be understood that other systems of the transit system 100, such as a station system 130, may draw funds from a funding source 165. Moreover, because cash payments can also be used to fund transactions associated with a transit user account, the transit user account may not require funding source 165.

[0039] Transactions of a user, such as passage at a transit access control points, can frequently occur at stations of the transit system 100, although it will be understood that access control points can exist elsewhere, such as on busses or trains. Station systems 130 can gather information regarding transactions and communicate the information to the central ticketing system 112 using a wide area network (WAN) 140. The WAN 140 can include one or more networks, such as the Internet, that may be public, private, or a combination of both. The WAN 140 could be packet-switched or circuit-switched connections using telephone lines, coaxial cable, optical fiber, wireless communication, satellite links, and/or other mechanisms for communication. Communication between the station systems 130 and the central control system 110 may be in real time or periodic. Thus, the usage of fare media throughout the transit system 100 can be tracked.

[0040] In this embodiment, a central ticketing system 112 and a central data store 114 are shown for the central control system 110. As discussed above, central ticketing system 112 receives periodic reports upon how credits or debits are being processed throughout the transit system 100. Additionally, changes in schedules, ticket prices, and delay notifications can be communicated from the central ticketing system 112 to the station systems 130 via the WAN 140.

[0041] A mobile device 180 may be communicatively coupled with the central control system 110. Such a mobile device may be a smart phone or other mobile phone (including a near-field-communication (NFC)-enabled mobile phone), a tablet personal computer (PC), a personal digital assistant (PDA), an e-book reader, or other device. In transit system 100, a communicative link from mobile device 180 to central ticketing system 112 can be provided by a mobile carrier network 170 in communication with WAN 140. Mobile device 180 can thereby communicate with the central ticketing system 112 to access and/or manage information of a transit user account. Furthermore, the central ticketing system 112 can send messages to the mobile device 180, providing transit, account, and/or advertisement information to a user of the transit system

IPR2025-01150
Apple EX1071 Page 529

100 in possession of the mobile device 180. Such messages may be based on, among other things, opt-in or opt-out selections and/or other user preferences as stored in a transit user account.

[0042] A transit user can use mobile device 180 to download a transit application from a transit application source 120. The transit application source 120 may be an application store or website provided by a mobile carrier, the hardware and/or software provider of the mobile device 180, and/or the transit service provider. The transit application can be uploaded or otherwise provided to transit application source 120 by the transit service provider. According to some embodiments, the transit application can provide additional functionality of mobile device 180, including enabling an NFC-enabled mobile device to be used as fare media and access control points of the transit system 100.

[0043] **FIG. 2** shows a block diagram of an embodiment of a transit station system 130. As discussed above, transit system 100 can include various forms of transit, such as subway, bus, ferry, commuter rail, para-transit, and more. Because different forms of transit may require different functionality, various transit station systems 130 may have some or all of the components shown in the block diagram. A local area network (LAN) 240 couples the various systems together and could include point-to-point connections, packet switched connections, wireless connections, and/or other networking techniques.

[0044] A station server 224 can be coupled to the WAN 140 to allow communication with the central ticketing system 112. Processing of local information can be performed on the station computer server 224. For example, fare information, schedule information, delay update information, and other transit related information can be processed at the station server 224 and communicated to the various other machines in the transit system 100.

[0045] A ticket booth computer 220, access control points 208, and transit vending machines (TVMs) 212 can communicate with the central ticketing system 112 through the station computer server 224 or directly with the central ticketing system 112 through LAN 240 or WAN 140 (e.g., the Internet). According to some embodiments, access control points 208 collect information from a user at various locations in the transit station system 130, and can come in various forms such as turnstiles, faregates, platform validators, para-transit vehicles, busses, conductor handheld units, and/or fare boxes. The access control points 208 can communicate with the station server 224 and/or central ticketing system 112 to determine whether to grant a user access when fare media has been presented at the access control points 208. If access control points communicate with a station server 224 during such transactions, identification codes of fare media, which can

IPR2025-01150
Apple EX1071 Page 530

be used to link a transaction with a transit user account, may be stored on lists in the station data store 216. Additionally, "hotlists", or lists of information identifying users, handheld media, PAN's, and/or user accounts may be stored on these lists. These lists can be updated on a regular basis to reflect other transactions of the fare media throughout the transit system 100. In other embodiments, identification codes of fare media 250 are stored at access control points 208.

[0046] Access control points 208 of the transit system 100 can be configured to read information from one or more sources of information on a fare media 250. To do so, access control points 208 can employ one or more technologies, such as WIFI, BLUETOOTH®, bar-code and/or other optical scanning. Access control points 208 may also employ near-field communication (NFC) technologies to read information from RFID tags, NFC-enabled mobile devices (such as certain personal digital assistants (PDAs), mobile phones, and other portable and/or personal electronics), contactless payment cards, and other contactless devices. The access control points 208 may also be configured to record, store, and/or transmit data regarding characteristics of the fare transactions, or transaction identifiers.

[0047] The access control points 208, TVMs 212, and one or more ticket booth computers 220, can communicate with the station server 224 via the LAN 204. This communication can be transmitted via a physical connection or wireless connection via one or more antennas 228. Transactions at access control points 208, TVMs 212, and one or more ticket booth computers 220 can be communicated to the station server 224, stored at station data store 216, and/or transmitted to central ticketing system, which can update information in a transit user account accordingly.

[0048] Various portable and/or handheld media with a unique identifier can be used as fare media, whether or not the media is issued by a transit services provider. Such media can include identification cards, payment cards, personal electronic devices, bar codes and items having bar codes, contactless devices, and more. Contactless devices can include media having a unique identification code readable by access control points 208 though NFC signals (e.g., radio frequency (RF) signals). By way of example, but not by limitation, such contactless devices can include devices comprising RFID tags and/or RFID-tagged items, contactless payment cards (including but not limited to credit cards, prepaid cards, debit cards, or other bank cards or contactless smart cards.), contactless identification cards and/or fobs, and NFC-enabled mobile devices.

IPR2025-01150
Apple EX1071 Page 531

[0049] Fare media 250 can have multiple sources of information, which may be read automatically by certain systems and devices in the transit system 100, depending on desired functionality. For contactless devices, such sources can include an IC, memory, and/or contactless interface of the device. Additionally or alternatively, contactless devices and other forms of fare media 250 can include a magnetic stripe, a bar code, and/or data imprinted and/or embossed on the device, which can serve as additional sources of information. Contactless and other sources of information can serve as repositories of account information related to, for example, a financial or user account associated with the fare media 250 (which may not be associated with the transit system 100).

[0050] TVMs 212 may interact directly with a fare media 250 through, for example, a contactless connection 232. Although communication of the contactless connection 232 may be two way, fare media 250 may simply communicate an identification code to TVM 212. This can be done, for example, to authenticate a contactless device for use as fare media 250 in the transit system 100. A contactless device does not have to be issued by a transit service provider in order to be authenticated and used as fare media 250 in the transit system, as long as the information communicated by the fare media 250 to the TVM 212 (and subsequently to access control points 208 for passage in the transit system 100) serves to uniquely identify the fare media 250. Such an authentication process is provided in greater detail below.

[0051] All or part of the information communicated by the fare media 250 can be used as an identification code to identify the transit fare media 250. This identification code can comprise one or more fields of data including or based on information such as a name, a birth date, an identification number (such as a PAN), a social security number, a drivers license number, a media access control (MAC) address, an electronic serial number (ESN), an international mobile equipment identifier (IMEI), and more. Because the identification code is unique, it can be associated with a transit user account, and utilized by a user at a TVM 212 to access and/or update information associated with the transit user account.

[0052] In some instances, an identification code may be assigned by a transit service provider and written to the fare media 250, such as an NFC-enabled mobile device 280. For example, a transit application running on an NFC-enabled phone can generate or otherwise provide an identification code to be transmitted from the phone at access control points 208 of the transit system 100. In other instances, if TVM 212 is utilized to enable a user to create a transit user account, the TVM 212 may also write an identification code to an unused portion of a memory of

IPR2025-01150
Apple EX1071 Page 532

the fare media, such as integrated circuit chip file space on a smart card or an NFC component on the NFC-enabled mobile device 280.

[0053] **FIG. 3** illustrates front and back views of an embodiment of a contactless payment card 310 that can be enabled as fare media 250 in the transit system 100. Such contactless payment cards are widely available, can be issued by any of a wide variety of issuing banks, and can include a payment brand. The contactless payment card 310 can include an integrated circuit (IC) 313 configured to, among other things, store account information, such as a PAN, expiry date, name associated with an account, etc. The IC 313 can adhere to one or more relevant standards, such as the Europay, MasterCard, and VISA (EMV) standard, and can be coupled with an antenna 315 for communicating information wirelessly to a contactless card reader (not shown). Contactless payment cards 310 frequently adhere to standards set by the International Organization for Standardization and/or International Electrotechnical Commission (ISO/IEC), such as ISO/IEC 14443 or ISO/IEC 15693 standards for contactless smart card communications. The IC 313 and antenna 315 can be embedded in the payment card and are frequently not visible to a card user.

[0054] The contactless payment card 310 can include features and/or data common to other payment cards, as defined in other ISO/IEC standards, such as ISO/IEC 7810 and ISO/IEC 7813. This can include a magnetic stripe 317, a payment brand logo 318, an account number 314 (such as a PAN, which can be printed and/or embossed on the contactless payment card 310) and a cardholder name 316.

[0055] EMV is an emerging global standard for the inter-operation of IC-enabled payment cards. The EMV standards define the interaction at the physical, electrical, data and application levels between IC cards and IC card processing devices for financial transactions. There are standards based on ISO/IEC 7816 for contact cards, and standards based on ISO/IEC 14444 for contactless cards. The cards following the EMV standard have additional information stored on the card 310. This information includes the PAN 320, an expiry date 321, a service code 322, an issuer discretionary data space 323, a transaction counter 324, and a calculated verification value based on an algorithm that includes the transaction counter 324 as a dynamic value 325. EMV transactions may also include other parameters outside of the track data.

[0056] For each use of the contactless interface antenna 315 on an EMV-compliant contactless payment card 310, the card 310 increments the transaction counter 324 value by one. The counter is incremented by the IC 313 on the card 310. Therefore, the counter increments whether or not

IPR2025-01150
Apple EX1071 Page 533

there is an associated retail transaction forwarded to an financial institution 160. Using the EMV card 310 as a contactless fare media would cause the transaction counter 324 to increment, even though financial institution that issued the card is not involved in the transaction.

[0057] In **FIGs. 4 and 5**, a perspective view and block diagram of an embodiment of a TVM 212 are shown. A vending machine processor 500 is coupled to the other components of the TVM 212 and transmits and receives signals to and from the other subsystems to cause the other components to perform their intended functions. Fare cards can be purchased and/or reloaded with value at the TVM 212. A coin/bill system 504, magnetic stripe card reader 412, and contactless card reader 418 are used to make payments for transactions at the TVM 212. Additionally or alternatively, a contactless card reader 418 may be coupled with a magnetic stripe card reader 412 to enable simultaneous reading of contactless and magnetic stripe information. A keypad 416 is provided adjacent to the credit/debit card reader 412 to enter numerical information such as a PIN code for a debit card. A coin slot 436 and bill loader 428 are used to accept cash. Change is returned in a change/receipt slot 420 and coin return 424. Reloadable fare cards and receipts, including receipts having a activation code, are also provided in the change/receipt slot. TVM 212 may further dispense single-ride fare cards through card dispenser 444, which is coupled with a card storage unit (not shown) storing reloadable prepaid cards for distribution. Information regarding transactions may be communicated through a LAN 240 by the vending machine processor 500 using, for example, a network interface (not shown).

[0058] Information regarding transactions may be communicated to various entities. For example, a contactless PAN, a magnetic stripe PAN, and/or other information may be communicated to the central ticketing system 112 to create a transit user or temporary account. Additionally or alternatively, a PAN and other payment information may be transmitted to a card issuer or other financial institution 160 for payment of a transit product. The financial institution 160 can receive communication from TVM 51 via financial network 150, central ticketing system 42, and/or WAN 140. Moreover, a financial account associated with a contactless payment card 310 may comprise a funding source 165 maintained by a financial institution 160.

[0059] A display system 404 prompts the card holder through the refill/purchase process. For example, the screen prompts the purchaser to touch a start button/icon on a touch screen display of the display system 404 to begin the process. A textual display portion 406 can display textual instructions for the user after the process has begun. Additionally or alternatively, an audio system 442, including a speaker, can produce audio commands. The user can be given a menu of

IPR2025-01150
Apple EX1071 Page 534

choices of how to proceed. For example, the menu may include choices to purchase or reload a reloadable fare card, purchase a single-ride fare card, purchase a product, setup a transit user account, and/or associate a contactless device, such as a contactless payment card, with a transit user account. It will be understood that, additionally or alternatively to a touch screen display, other input interfaces may be utilized to accept input from a user. This can include, but is not limited to a touchpad, keyboard, mouse, trackball, audio input interface, joystick, etc.

[0060] If the user chooses an option requiring payment, the user may be instructed, by menu prompts, pre-recorded video and/or audio, on how to proceed with the payment. The user can be given a choice to pay in cash or by a payment card. For cash purchases, the user is instructed to insert coins or bills into the coin slot 436 or the bill loader 428. For payment card purchases, the user is instructed to insert payment card into the magnetic stripe card reader 412, or touch a contactless payment card 310 to contactless card reader 418.

[0061] Different processes may be implemented if the user chooses to enable a contactless payment card 310 as fare media 250. For example, the user can be instructed to touch a contactless payment card 310 to contactless card reader 418. Additionally, the user would be instructed to insert the contactless payment card 310 into the magnetic stripe card reader 412 and/or input the imprinted and/or embossed PAN 314 by using the keypad 416, the display system 404 (if it includes touchscreen capabilities), or both. Alternatively, for TVMs 212 with a contactless card reader 418 coupled with a magnetic stripe card reader 412, a user can be instructed to insert the contactless payment card 310 into the magnetic stripe card reader 412, allowing the TVM 212 to read both the contactless and magnetic stripe information from the contactless payment card 310. The TVM 212 can be configured to provide additional functions such as allowing the user to purchase a product, activate the contactless payment card 310 as fare media 250, and/or create a transit user account, by, for example, accepting additional input through any one of the user interfaces described above. Additionally or alternatively, the TVM 212 can simply print out an activation code on a receipt and provide the receipt to the user from the change/receipt slot 420. The transit system 100 can associate the activation code with information collected from the contactless payment card 310, enabling the user to perform any of the additional functions listed above at a TVM 212, ticket booth, website and/or other system at a subsequent point in time.

[0062] It will be understood that any or all of the features and/or capabilities of the TVM 212 described above may be included in other locations and/or devices of the transit system 100. A

IPR2025-01150
Apple EX1071 Page 535

user may therefore register a contactless device, such as a contactless payment card 310, as fare media at other locations of the transit system 100. For example ticket booth computers 220 can be coupled with contactless card readers and/or magnetic stripe card readers, allowing a user to perform any or all of the functions described above by providing a contactless payment card 310 to a transit worker at a ticket booth. Additionally or alternatively, other devices may be configured to read contactless and magnetic stripe information from a contactless payment card 310 and transmit the information to a central ticketing system 112 of the transit system 100, without having the additional functionality of a TVM 212. Such devices further can be configured to print a receipt with an activation code, enabling a user to complete, at a later point in time, the process of activating a contactless payment card 310 for use as fare media 250. Moreover, these procedures may be carried out at a sales office, automated teller machine, and/or other manned or unmanned locations.

[0063] **FIG. 6A** is a simplified block diagram of an embodiment of an access control point processing unit 600-1, which can be coupled with and/or integrated into access control points 208 of a transit system 100 and can control certain physical properties of access control points 208 such as to allow or deny passage of a user. Among other things, the access control point processing unit 600-1 can be used to read an identification code, such as a contactless PAN and/or other contactless information, from fare media. The access control processing unit may also record transaction identifiers, such the time and location of the transaction. The access control point processing unit 600-1 also can determine whether to permit passage of a user at the access control point 208. Interfaces such as an NFC interface 680 (which can read RFID and contactless information), and/or magnetic reader interface 640, can be used to receive information from fare media 250, including an identification code. Alternative embodiments contemplate access control processing units 600 without a magnetic reader interface 640. Once the identification code is received, it can then be sent to processor 610.

[0064] In addition to performing any decryption and/or verifying any security features, the processor 610 can compare the identification code against lists stored in memory 620-1 and/or other data store to determine whether to allow passage of the user at the access control point 208. Lists can be generated and maintained from a central system, such as the central ticketing system 112. The central system can send updated list information to station server 224 via WAN 140 or directly with the central ticketing system 112 through WAN 140 (e.g., the Internet) or LAN 240. The station server 224 can store updated list at the station data store 216 and/or communicate the

IPR2025-01150
Apple EX1071 Page 536

updated list information via LAN 240 to access control point processing unit 600-1, which receives the information at network interface 630. U.S. Patent Application No. 12/833,404, entitled "Reloadable Prepaid Card Distribution, Reload, And Registration In Transit," (hereafter, the "'404 Application") which is incorporated herein, details how the transit system 100 and access control point processing units 600 may use lists to determine whether to allow passage of the user at access control points 208. Once the determination is made, the processor 610 can cause the access control point processing unit 600-1 to physically allow or deny passage of a user at the access control point 208.

[0065] The access control point processing unit 600-1 can also log transaction information in memory 620-1 and/or communicate the transaction information to station server 224 with a network interface 630. The station server 224 can, in turn, send the transaction information to the central ticketing system 112, which can store the information in central data store 114. The transaction information can be used to update transit user accounts associated with the transactions and to settle with a funding source 165.

[0066] **FIG 6B** is a simplified block diagram of an alternative embodiment of an access control point processing unit 600-2. As illustrated, a memory 620-2 may be located at a source external to access control point processing unit 600-2. The external source can include, for example, station server 224 or station data store 216. In such an embodiment, the processor 610 may communicate with the external source in deciding whether to allow or deny passage of a user at an access control point 208, or the decision may be made by station server 224. In either case, it is desirable to make the decision quickly, often in 500 milliseconds or less. Thus, in this embodiment, it can be desirable that the connection between access control point processing unit 600-2 and the external source having memory 620-2 have sufficient speed and minimal latency to provide for a quick decision. Methods of allowing or denying access to a user at access control points 208, as well as methods of processing transactions received from access control points 208, are described in more detail in the '404 Application.

[0067] **FIG. 7A** is a diagram of an embodiment of a method for enabling a contactless payment card 310 to be used as fare media 250 in a transit system 100 providing account-based transactions. Beginning at block 700, a request is received to enable a contactless payment card 310 as fare media. For example, a user may select a menu option at a TVM 212 to make such a request. At block 710, a user is directed to insert a contactless payment card 310 into a card reader.

IPR2025-01150
Apple EX1071 Page 537

[0068] At block 720, card information is read. As described above, a device such as a TVM 212 may include a magnetic stripe card reader 412 integrated and/or coupled with a contactless card reader 418 such that the device can read the magnetic stripe and contactless information at the same time. Alternative embodiments contemplate variations on reading card information. For instance, where card readers are not integrated, the user may be directed to tap a contactless card reader 418 and insert the card into a magnetic stripe card reader 412 separately, in which case, the contactless and magnetic stripe information correspondingly is read in discrete steps.

[0069] In some instances, the contactless PAN may match the PAN of the magnetic stripe. However, to overcome the problems introduced by multiple cards with an identical PAN, a unique "fingerprint" of the contactless payment card 310 can be identified. To do so, additional track data components can be used to decipher one contactless PAN from another. For instance, track data includes name and expiry data. Additionally, some card issuers place a sequence code into the track data to make the contactless payment card 310 uniquely distinguishable. Thus, in addition to reading the contactless PAN and the PAN of the magnetic stripe, the device in which a user inserts and/or taps a contactless payment card 310 can be configured to read additional contactless track data, such as a sequence code, account holder name, and/or expiry date. Access control points 208 of the transit system 100 can be similarly configured to read the additional contactless track data to be able to access the uniquely distinguishable information.

[0070] Because the PAN of the magnetic stripe is typically identical to the imprinted and/or embossed PAN 314, a device may be configured to receive the imprinted and/or embossed PAN 314 rather than the PAN of the magnetic stripe. For instance, a TVM 212 can be configured to allow a user to manually enter the imprinted and/or embossed PAN 314 using a keypad 416 or touchscreen. Moreover, a device may have visual scanning capabilities to read the imprinted and/or embossed PAN 314 directly. It will be understood that other information such as an expiry date or account holder name, can be read from the magnetic stripe and/or otherwise received by the transit system.

[0071] At block 730, a temporary account with associated PAN numbers, and any additional contactless track data, is created. The account simply can comprise an association of the contactless data with the other provided information. At block 740, an activation code is created, and at block 750, a receipt with the activation code is provided to the user.

[0072] At block 760, the activation code is provided, along with product information. The activation code and product information is associated with the information received earlier, and, at

IPR2025-01150
Apple EX1071 Page 538

block 770, a user transit account is created. The transit user account can comprise the information of the temporary account in addition to the product information provided at block 760. It may also include additional information provided by a user, as well as the activation code. For example, after receiving a receipt with the activation code, a user can provide the activation code at a website and purchase a product, such as a monthly pass.

[0073] A user may provide additional information to personalize the transit user account. For example, a user may provide a name, phone number, address, email address, social security number (SSN) or other government-issued identifier, a drivers license number, a username, a passcode (such as a personal identification number (PIN) or a password), other identification verification information, and/or funding information. Depending on the desired functionality of the transit system, a user also may input information regarding opt-in or opt-out selections for additional services, user preferences, and/or additional product(s) for purchase to be associated with a transit user account. The account further may include other data generated by the transit service provider.

[0074] At block 780, the contactless payment card 310 is enabled as fare media, and a receipt and/or acknowledgement is provided to the user at block 790. Enabling the contactless payment card 310 for use as fare media within the transit system 100 can comprise sending the contactless information (e.g. uniquely-identifying information) of the contactless payment card 310 to a central database, such as the central data store 114 and/or multiple remote databases, such as the station data store 216, with which access control points 208 can communicate. Additionally or alternatively, the contactless information may be propagated to the access control points 208 themselves. Thus, in subsequent transactions where the contactless information is read from the contactless payment card 310 at an access control point 208, the access control point 208 can recognize the information as being related to a valid transit user account and allow a transit user access accordingly.

[0075] It will be understood that embodiments contemplate numerous variations to the method shown in FIG. 7A. For example, although providing a receipt with a activation code is desirable, it is not required. Rather than provide an activation code, a method include simply receiving the imprinted and/or embossed PAN, which a user can provide a subsequent registration over the Internet, at a ticket booth, or at another location of the transit system 100. Additionally or alternatively, embodiments contemplate allowing a user to link information received from the contactless payment card 310 to an existing user account. For instance, a user can provide user

IPR2025-01150
Apple EX1071 Page 539

information contained in the transit user account, such as a username and/or passcode, at any time before or after information is read from the contactless payment card 310, allowing a the contactless and other information to be associated with the user account.

[0076] **FIG. 7B** illustrates how a method similar to that shown in FIG. 7A can be extended to apply more broadly to contactless devices. Access control points 208 can be configured to read wireless information from contactless devices other than contactless payment cards 310, such as NFC-enabled mobile devices, RFID tags/stickers, contactless identification cards, etc. These devices may have contactless information uniquely identifying the device that may differ from information from another source of the device. Accordingly, a transit, transportation, or similar system can be configured to enable such contactless devices for use within the system in a manner similar to that of contactless payment cards 310.

[0077] **FIG. 8A** is a block diagram of an embodiment of another method for enabling a contactless payment card 310 for use as fare media 250 in transit system 100. FIG. 8A illustrates how a user account may be created before information is read from the contactless payment card 310. FIG. 8A also demonstrates how the creation of the transit user account and the enablement of the contactless payment card 310 as fare media 250 can be done in a single session, without requiring additional steps at a later point in time.

[0078] At block 810, user information is received, and at block 820, a transit user account is created. Similar to the user information described above, the user information can comprise any of a variety of information, including product and payment information, among other things. At block 830, a user is directed to insert a contactless payment card 310. And at block 840, information is read from the contactless payment card, including contactless information. The information may also include information from a magnetic stripe, bar code, imprinted and/or embossed characters, and/or other sources of information.

[0079] At block 850, the contactless information, including a PAN, is associated with the transit user account. A PAN provided by another data source of the contactless payment card can also be associated with the transit user account. After which, at block 860, the contactless payment card 310 is enabled as fare media. And at block 870, a receipt and/or other acknowledgement is provided to the user. It will be understood that certain blocks, such as blocks 840-870, can be repeated at any time to allow a user with an existing transit user account to enable a handheld media, such as a contactless payment card or other NFC-enabled device, to be used as fare media.

IPR2025-01150
Apple EX1071 Page 540

Such occasions can arise, for example, when a card issuer provides a user with a new contactless payment card before the expiry of an existing payment card.

[0080] **FIG. 8B** is an embodiment of a method that incorporates the enablement of a contactless payment card 310 for use as fare media 250 with the payment of a transit and/or transportation product using the contactless payment card 310. In addition to the steps shown in FIG. 8A, the embodiment of FIG. 8B includes block 825, enabling product purchase. This can include, for example, allowing a user to select a transit and/or transpiration product from a menu. Additionally, block 843, payment information, such as the PAN, expiry date, and other information is sent to a card issue for verification. At block 845, payment confirmation is received. As with all methods described herein, numerous variations may be made. For example, at any of a variety of points during the process, a user may be allowed to select whether or not to enable the contactless payment card 310 for use as fare media 250. It will be understood further that other embodiments described herein can incorporate payment of a product with the contactless payment card 310 similarly.

[0081] **FIG. 9** is a swim-lane diagram of yet another embodiment of a method for enabling a contactless payment card 310 for use as fare media 250. FIG. 9 illustrates how the method may be performed by a TVM 212, a central ticketing system 112, and a web server. The web server can host a web site for receiving input from a user. Such a web server can be maintained or otherwise communicatively connected with the central ticketing system 112. Moreover, the web server comprise part of the central control system 110 of a transit system 100.

[0082] At block 905 the TVM 212 reads the contactless and magnetic stripe information from a contactless payment card 310. At block 910 all, or at least a part, of the information is communicated to the central ticketing system 112. At block 915, the central ticketing system 112 receives the information, and at block 920, creates the account. At block 925, the central ticketing system 112 can then create and return an activation code. At block 930, the TVM 212 provides the activation code to the user.

[0083] With the activation code, the user can then access a website hosted by the web server to complete the enablement process. At block 935, the web server receives the activation code. This can be done, for example, simply by providing a website with a small form to fill out and submit, including a text box for the activation code. Product and payment information may also be received by the web server. At block 940, the web server provides the activation code to the central ticketing system 112.

IPR2025-01150
Apple EX1071 Page 541

[0084] At block 945, the central ticketing system 112 creates a transit user account with, among other things, information received at block 935. At block 950, the central ticketing system enables the contactless payment card 310 as fare media in the transit system 100. The central ticketing system 112 can notify the web server that the contactless payment card 310 has been enabled.

[0085] At block 955, or alternatively at an earlier point in the process, the web server can further offer to personalize the transit user account. At block 960, if the offer is rejected, the web site can, at block 975, simply relay receipt and/or acknowledgement information to the user. Otherwise, at block 965, the web server can receive additional information from the user by, for example, providing an additional online form, which is submitted by the user. The information is relayed to the central ticketing system 112, and at block 965, associated with the transit user account. At block 970, the web server provides receipt and/or acknowledgement information to the user.

[0086] Processing of contactless payment cards in the transit system can be based on the PAN as a unique identification code. The PAN is available to an access control point 208 configured to read contactless track data from the contactless payment card 310. The PAN can be extracted from the track data and used to identify the card for account-based processing. Under most circumstances, the PAN imprinted and/or embossed on the front of the card is the same as the PAN found in the track data and stored on in the card's 310 integrated circuit 313.

[0087] If the contactless PAN stored in memory of the IC 313 of a contactless payment card 310 is different than the PAN imprinted and/or embossed 314 on the front of the card, additional difficulties arise. For example, it would be particularly difficult to allow a transit user to use the Internet to register the contactless payment card 310 for use as a fare media 250. Because access control points 208 are configured to read the contactless PAN from the contactless payment card 310, it would not avail the transit user to enter the imprinted and/or embossed PAN 314.

[0088] One way to solve this and other problems may be solved by providing the imprinted and/or embossed PAN 314 and the contactless pan beforehand. For example, a transit user can swiping and/or dipping the contactless payment card 310 at a TVM 212 or other device of the transit system 100 configured to read information the magnetic stripe 317, which frequently includes a PAN that including a PAN that matches the imprinted and/or embossed PAN 314. The device can also read the contactless PAN from the IC 313. The transit system can then associate the contactless PAN with the imprinted and/or embossed PAN 314, enabling a user to access the

IPR2025-01150
Apple EX1071 Page 542

Internet subsequently and enter the imprinted and/or embossed PAN 314. The transit system 100 can then associate any additional user and/or product information with the contactless PAN, and enable the contactless payment card 310 for use as fare media in the transit system 100. More details describing this process are provided below.

[0089] Usually, the PAN 314 on one contactless card 310 will be different and distinct from the PANs on other payment cards, thus enabling the transit system to treat each PAN 314 as a unique identifier associated with each user account. However, there will be variations that the transit system 100 may need to contemplate. Bank card issuers have their own issuing rules and procedures, which may result in multiple cards 310 with the same PAN 314. Also, fraud and theft may result in illegitimate handheld media encoded with a stolen PAN 314 that could be used as a fare media 250. When different cards/devices have the same PAN there is a problem correctly associating the registered card with the purchased fare products. Accordingly, some embodiments disclosed herein include methods allowing for such determination and providing ways to combat a possible scam or fraud.

[0090] Contactless bank cards can be used in account-based transit fare collection in two modes: (1) pay as you go; and (2) where the card is registered and fare products are purchased and associated with that bank card account number. In the second case, when the bank card account number is read, for exampe at a contactless interface 680, and processed in the transit system 100 as a fare media 250, it is associated with the account-based fare product. This association can be made by the transit system 100 using hardware, software, or a combination of the two.

[0091] A problem arises when contactless account number (PAN) are not be unique amongst cardholders. Fraud may be prevented by not allowing random bank cards/devices to be registed against account-based products and/or requiring that cards used for passes and discounted fare products must be of agency issued media. But this would be limiting and not be convenient for the patron. Alternatively, a fare collection system could demand that card issuers do not issue single PANs 314 on multiple cards/devices. But this may not be practical. Many card issuers exist, each with their own process for card numbering, and they are unlikely to conform to the needs of a transit agency.

[0092] One variation of this problem can include multiple parties linked to one financial account, such as a husband and wife, a parent and child, or multiple business partners, each having access to the joint account. Each joint-account holder could be issued a payment card 310 associated with the joint account, and each card 310 could have the same PAN 314 embossed on

IPR2025-01150
Apple EX1071 Page 543

the card and/or stored in the track data (e.g., magnetic stripe 317) and/or IC 313. To further illustrate, if a transit user with a transit user account purchases a single, flat-fare monthly pass and associates the PAN 314 of a contactless payment card 310 with his/her transit user account, each additional contactless payment card having the same PAN 314 could also be used as fare media 250 for the monthly pass. Thus, if the multiple contactless payment cards 310 are distributed among several people, each person essentially would receive a monthly pass when only one monthly pass was purchased. In another variation, a single account holder may be issued multiple devices which provide access to one or more accounts. For example, a user may be issued multiple payment cards 310 and/or companion devices, such as another style of contactless payment card, an RFID-enabled sticker, a key chain tag, a FOB, etc. In another variation, an account holder may receive a replacement card prior to the time that an enrolled payment card 310 expires. This could result in a period of time between the time when the replacement card is activated and when the original card 310 expires when both cards could be validly read as a fare media 250 at a access control point 208.

[0093] Another problem may involve only a single card 310 that is used by multiple people as a fare media 250. In one variation, a user account may contain a type of transit product that allows for unlimited access to the transit system during a limited time, such as a monthly or weekly pass. In this case, a single payment card 310 may be used as a fare media by multiple users at one or more access control points. For example, the card owner could use the card 310 in conjunction with the NFC interface 680 of a single access control point 208 to allow additional transit users to enter an access control point 208 either before or after the card owner. In another variation, the card owner could use the payment card 301 himself/herself, and then pass the card 310 back to other transit patrons on the other side of the access control point 208 for reuse. In yet another variation, the transit product associated with the user account could be non-transferrable. In this case, a payment card 310 could be cancelled by the issuing bank at the request of the owner, then sold for use solely as a fare media 250 to another user until expiration of the transit product.

[0094] In addition to misuse by legitimate holders of the payment card 310, fraud and theft can also lead to multiple handheld media devices that are associated with the same PAN 314. In one variation, a payment card 310 could be stolen from a user, and a replacement card could be mailed from the issuing bank. If the replacement card had the same PAN 314, then both the stolen card 310 and the replacement card could be used as a fare media 250. In another variation, the payment card 310 itself may not be stolen; however, the stored data including the PAN 314 could

IPR2025-01150
Apple EX1071 Page 544

be stolen from the card 310, associated with another handheld media, and used as a fare media 250 without the knowledge of the card owner. This situation could be particularly worrisome to the transit system 100 if the thief were to only use the card 310 as a fare media 250. Unless the thief were to also use the PAN 314 in retail transactions, the issuing bank and the card owner would have no means of knowing that the payment card data had been stolen. Without being able to benefit from the issuing bank's existing fraud-detection schemes, the transit agency 100 would need its own method of detecting when a handheld media with a PAN 314 associated with a user account is being potentially misused.

[0095] In the above circumstances, the contactless payment card issuer knows how to associate each card variation and can charge the single bank account as appropriate. The transit system 100, however, will not be able to automatically decipher most of these circumstances. Because the transit system 100 allows for account-based transactions, the inability to take into account the above circumstances can be problematic in many ways. Ideally, the issuer would have to communicate to the transit agency regarding multiple card scenarios and fraud detection. This is not a practical solution due to the tremendous number of transit systems around the world and the number of payment cards in circulation. Regardless, the transit agency may be interested in determining whether more than one person is using a handheld media associated with a PAN 314 authorized as a fare media 250. As illustrated by the situations above, using the PAN 314 alone may not be sufficient to detect potential misuse. Additional data from the transaction may be necessary for the transit system 100 to perform this type of operation without assistance from the issuing bank.

[0096] According to certain embodiments of the present invention, this problem may be solved by using invented procedures and processes of automation to detect and stop multiple cards 310 and/or devices from using the same stored account-based fare product. This can include fraud detection mechanisms looking for exceptions and odd travel patterns on a single PAN 314 by analyzing additional transaction identifying data.

[0097] FIG. 10A illustrates one embodiment of a method wherein the transit system 100 may collect additional information that is characteristic of each individual fare transaction. This additional information may be referred to as a transaction identifier, and it can be used to detect potential misuse of a payment card as a transit fare. In this method, a user account is created for managing transactional information wherein at least one transit product is purchased and/or designated for use at block 1010. At block 1020, a handheld media is enrolled for use as a fare

IPR2025-01150
Apple EX1071 Page 545

media 250 for the transit product according to the various methods described above. The handheld media could be a payment card 310, a smart phone, a portable media player, a FOB, and/or the like. The handheld media may use contact with the access control point when used as a fare media, for instance with a magnetic stripe or a electrical contact. Alternatively, the handheld media may use a contactless connection with the access control point 208, such as with NFC-enabled devices, Bluetooth, RF, IR, or barcode devices. In one embodiment, the fare media is contactless payment card 310 using the EMV data standard.

[0098] The handheld media can be associated with all of the transit products associated with the user account, or the handheld media can be associated with one or more single transit products. In one embodiment, the transit product is an unlimited ride pass that is valid for a finite period of time, such as a monthly, weekly, or yearly pass. Alternatively, the transit product could include a limited-ride pass such as ten-ride pass. In this case, it would still be desirable for the transit system to detect potential misuse of a PAN 314 in order to protect its customers, to inspire customer loyalty, and/or to prevent the transfer of transit products between different users.

[0099] Next, at block 1030-1, the transit system 100 may receive a listing of transaction identifiers from one or more of the access control points 208. Each transaction identifier may be associated with a single use of a handheld media as a fare media 250. One or more transaction identifiers may be received and stored for each fare transaction involving a fare media 250, resulting in a plurality of transaction identifiers associated with a single PAN 314 over time. A transaction identifier may be a single piece of data, such as the time of the transaction. Alternatively, a transaction identifier may be comprised of more than one characteristic of the transaction. For example, a transaction identifier may include the time or location of the transaction, a user code, a one-time-use password, biometric data from the user, and/or track data from the card other than the PAN 314. In some embodiments, the misuse detection algorithms may also use other inputs in addition to the transaction identifiers, such as user inputs from the transit system 100, an authorized user, or law enforcement. These algorithms could incorporate other data, such as surveillance data or information from a financial institution. It will be understood that combinations of each of these data sources could also be incorporated to detect potential misuse.

[0100] The list of transaction identifiers may be stored and/or analyzed locally at the station server 224, or the list of transaction identifiers may be stored and/or analyzed remotely at the central ticketing system 112. If the transaction identifiers are analyzed remotely at the central

IPR2025-01150
Apple EX1071 Page 546

ticketing system 112, they may be transmitted from the station systems 130 individually as they are collected from the access control points 208. Or, in another embodiment, the transaction identifiers may be stored locally at the access control points 208 or at the station server 224 or at a comparable local system. In this case, a list of transaction identifiers associated with a PAN 314 could then be transmitted to the central ticketing system 112 periodically in batches during off-peak travel times to reduce network traffic. These batches could be sent periodically, such as every 15 minutes, or they could be sent when a predetermined number of fare transactions have taken place. The transaction identifiers could be stored and/or transmitted in a dedicated list, or they could each be packaged in with other data. For example, if the transaction counters 324 in the EMV data are used as transaction identifiers, then they could be stored in the EMV data format in a cryptogram that is received from the payment card 310. The encrypted packets could be decrypted locally at the station systems 130, and the transaction counters 324 could be analyzed or transmitted to the central ticketing system 112. Alternatively, the encrypted data packets themselves could be transmitted to the central ticketing system 112 for decryption and analysis. It will be understood that a fare transaction record analyzed for potential misuse may include any arrangement of the data described above.

[0101] At block 1040-1, after a number of fare transactions have been recorded for a given PAN 314, the transaction identifier list can be analyzed to determine if there is potential misuse involving the PAN 314. To detect potential misuse, the transit system 100 could examine the relationship between at least a subset of the recorded transaction identifiers to identify patterns that are associated with misuse. In one embodiment, the transaction identifiers could be compared to an expected pattern for a typical transit system patron. In another embodiment, the transaction identifiers could be compared to an expected pattern of use for the user associated with the user account. Alternatively, the transaction identifiers could be analyzed to detect abnormalities in the use of the fare media associated with the PAN 314, such as transactions that would indicate that multiple cards are being used with a single PAN 314.

[0102] At block 1050 the transit system 100 may take an action related to using the handheld media as a fare media 250 in association with the transit product. Various actions can be taken, as described later in this disclosure.

[0103] FIG. 10B illustrates one embodiment similar to that of FIG. 10A, wherein the transaction identifier is comprised of the transaction counter 324 from an EMV data packet that is incremented during each contactless use as a fare media. At block 1030-2, the fare transaction

IPR2025-01150
Apple EX1071 Page 547

records may include the transaction counter 324 as read from a payment card 310. The transaction counters 324 could be stored in the EMV data format in a cryptogram that is received from the payment card 310, and this entire cryptogram could be sent to the transit system 100 as a transaction fare record. Alternatively, the encrypted packets could be decrypted locally at the station systems 130, and the transaction counters 324 could be analyzed or transmitted to the central ticketing system 112.

[0104] At block 1040-2 potential misuse may be detected by analyzing the sequence of at least a subset of the transaction counters 324. Specifically, determining that potential misuse has occurred may be based on the relationship between the transaction counter 324 values. The detection algorithm may look for sequences of transaction counter values that appear to deviate from the expected pattern of values that would occur during normal use of a payment card 310. Normal use could include use as a fare media 250, use as in retail transactions, or a combination of the two. In most situations where the payment card 310 is also used for retail transactions, the algorithm may need to account for gaps in the transaction counter sequence depending on the time between uses as a fare media 250. The algorithm may also need to account for situations where the card 310 is reissued and used the transaction counter 324 is reset. Other variations in the transaction counter 324 sequence due to normal card use are contemplated by this invention.

[0105] In one embodiment, potential misuse may discovered by detecting large gaps in the transaction counter sequence that are not proportional to the time between uses as a fare media 250. In most cases, the transaction counter sequence should steadily increase, and the increments should go up in small numbers when the card 310 is used regularly as a fare media 250. For example, a set of transaction counters 324 sequentially recorded by a transit system that might not indicate potential misuse could be "5, 6, 8, 10, 13." Another example might be "125, 127, 128, 132." The small gaps in these sequences may indicate normal retail use between uses as a fare media 250. If the sequence reveals large gaps in the transaction counters 324, this may indicate that two cards 310 associated with the same PAN 314 are being used as a fare media 250 for the same transit product. For example, the sequence could be "12, 14, 15, 52, 53, 55." In this case, the gap between 15 and 52 could be used to determine that two different cards 310 with the same PAN 314 are being used. On the other hand, if there is a large amount of time between transaction number 15 and transaction number 52, then the gap may be attributed to normal retail use of the payment card 310 and not indicative of potential misuse. Therefore, some embodiments may determine whether the gap in the transaction counter sequence is proportional

IPR2025-01150
Apple EX1071 Page 548

to the amount of time between fare transactions involving the card 310. For example, the determination could take into account the average gap size in the transaction counter sequence to gauge when a gap is large enough to indicate potential misuse. Thus, a sequence of "5, 16, 30, 44, 45, 60" may not indicate potential misuse even though the gaps are large between each transaction. This situation may instead indicate that the user is involved in a large number of retail transactions on a regular basis between fare transactions, even if the fare transactions are not relatively far apart in time.

[0106] Alternatively or additionally, the determination of potential misuse may also be made by detecting patterns of transaction counters 324 that do not continually increase. Even if a payment card 310 is involved in retail transactions in addition to being used as a fare media 250, the transaction counter 324 would typically increase, even with gaps in the sequence. For example, a sequence of transaction counters 324 such as "5, 6, 189, 9, 191, 192, 12" could indicate that more than card 310 with the same PAN 314 is being used, one with a transaction count near "5", and one with a transaction count near "191". The detection may also anticipate situations where the large gaps occur, or where a sequence jumps from high numbers to low numbers as a result of legitimate single-card use. An example sequence could be "250, 253, 255, 1, 4." Such situations may arise when a card is reissued by the financial institution or when the transaction counter 324 rolls over. In these cases, the detection algorithm may consider other inputs, such as the card expiry date 321, a known transaction counter limit, a notification from the user, and/or the like.

[0107] More sophisticated misuse of a payment card 310 might be more difficult to detect. For example, two users could be using cards 310 with the same PAN 314 and could coordinate the cards' use to prevent glaring out-of-sequence transaction counters 324. This could result in a transaction counter 324 sequence such as "80, 81, 83, 83, 84, 86, 87." In this case, the algorithm may need to look for more subtle errors in the sequence. Therefore, the determination of misuse may also look for duplicate numbers or sequences that do not show signs of normal retail transactions. In another embodiment, the determination of potential misuse could detect repeated patterns, such as "120, 122, 123, 120, 122, 123." Repeated patterns may indicate a careful collaboration between users of duplicate cards 310, or could indicate that a card 310 has been electronically pick-pocketed or skimmed, and a duplicate card 310 is being used without the card owner's knowledge. A determination that potential misuse does not necessarily implicate the card owner may be valuable in determining an appropriate action to take in response at block 1050 described later in this disclosure.

IPR2025-01150
Apple EX1071 Page 549

[0108] A determination of potential misuse involving the transaction counters 324 can also be made by developing use profiles of different transaction counter sequences, and then comparing the recorded sequences with the profiles. Recorded sequences that deviate sufficiently from an expected profile could indicate potential misuse. A profile may consist of certain transaction counter sequence patterns that are common. Alternatively, a profile may consist of descriptive information about expected profile patterns, such as average gap size, average transaction counter limit, and/or total number of retail transactions for each fare transaction. The profiles could be derived from multiple users and combined to create an average user profile. Alternatively, a profile could be derived from the usage statistics from users that are similar to the suspect user. In another embodiment, a profile may be based on the actual use of each individual user's transaction history. In this case, the determination algorithm may identify types a card use which deviate from the historical usage pattern of the particular user. Other methods of generating a comparison profile are contemplated by various embodiments, and may involve combinations of the various methods described above.

[0109] Alternatively or additionally, other embodiments may use different data as a transaction identifier to detect potential misuse. FIG. 10C illustrates an embodiment wherein the time and/or location of a transaction is used as the transaction identifier. At block 1030-3, time and location data could be collected from the access control points 208 of the transit system 100 as a handheld media is used as a fare media 250. The data could be collected and packaged together in a data packet along with the data read from the handheld media. Alternatively, the time and location data could be stored and/or transmitted separately from the handheld media data. In another variation, the time and location data could be received from the handheld media itself, for example from a smart phone enabled with GPS location information. In any case, the transaction fare records made available to the transit system 100 may include transaction time and /or location data with an associated PAN 314.

[0110] At block 1040-3, potential misuse is determined, at least in part, by analyzing the pattern of transaction times and/or locations. The determination of potential misuse may identify travel patterns that are illogical, unlikely, out of character compared to a user profile, and/or physically impossible. In one embodiment, the determination may be made by detecting transaction times that are unlikely to occur. For example, multiple trips during the same day, although physically possible, may be unlikely. This situation may indicate that multiple users are handing off the same handheld media for use throughout the day. A large number of uses over a short period of

IPR2025-01150
Apple EX1071 Page 550

time may indicate that a PAN 314 has been stolen and associated with a large number of handheld media. In another embodiment, the transaction time may be analyzed in conjunction with the transaction location. For example, fare transactions near the same time at distant locations may be indicative of two handheld media associated with the same PAN 314 being used by two different users for the same transit product. While some time and location combinations may be physically impossible, others may be possible but unlikely. In these cases, the potential for misuse may be determined to be proportional to the time and distance between locations. For example, uses at transit stations that are 30 miles apart may indicate potential misuse if the uses were 20 minutes apart. On the other hand, uses at two stations that are 30 miles apart may not indicate potential misuse if the uses occur more than 60 minutes apart.

[0111] In one embodiment, the time and/or location data may be compared to an expected user profile, and potential misuse may be determined by detecting deviations from the expected user profile. The profiles could be derived from multiple users and combined to create an average user profile. Alternatively, a profile could be derived from the usage statistics from users that are similar to the suspect user account. In another embodiment, the profile may be based on the actual use of each individual user's transaction history. In this case, the determination algorithm may identify types of card use which deviate from the historical usage pattern of the particular user. For example, if a particular user only travels between two transit stations on weekdays, then travel between different stations, or from a different starting station, may indicate potential misuse. Similarly, usage statistics from a single user account that do not establish any recognizable and/or predictable pattern may indicate that a card 310 is being exchanged by multiple users contrary to the rules of the transit product. Other methods of generating a comparison profile are contemplated by various embodiments, and may involve combinations of the various methods described above.

[0112] Using a transaction counter 324 or the transaction time and/or location as the transaction identifier in the determination of potential misuse, as described in embodiments hereinabove, are not meant to be limiting. Other embodiments may include other data that may be used as transaction identifiers. It may also be advantageous to combine data together as transaction identifiers to increase the effectiveness of the misuse detection. In one embodiment, the transaction identifier may include both a transaction counter 324 and the transaction time and/or location. For example, if the times and locations of a series of fare transactions indicate that the potential for misuse exists, the transaction counter 324 may be used to verify or dismiss the

IPR2025-01150
Apple EX1071 Page 551

suspicious behavior. In another example, the transaction counter 324 might indicate potential misuse when the counter sequence contains a large gap or resets to a lower number. In this case, the times and locations of the transactions may be analyzed to either confirm the suspicious activity or to indicate that a valid user may instead be using a valid replacement card 310, that the user is making a large number of retail purchases, or that the card's transaction counter 324 has rolled over. It will be understood that further combinations of transaction data beyond those explicitly describe herein are also contemplated by these and other embodiments.

[0113] Block 1050 of FIGS. 10A-10C illustrates that in certain embodiments an action may be taken related to using a handheld media associated with the user account as a fare media 250. The type of action taken may be related to the type and/or severity of potential misuse. It may also depend on a customer preference or on the duration or extent of the potential misuse. For example, in some embodiments the potential misuse may be a type that could be unknown to an authorized user. In this case, the transit system could send a notification to the user alerting him/her to the possibility of fraud via text message, voice mail, email, telephone, traditional mail, and/or any other means of communication. A user preference may also be used to decide how to deal with potential misuse detected in the user's account. For instance, the user could specify that a notification be sent to the user. Notification could also be sent to the issuing bank in cases where the handheld media is a payment card. The user could also specify that more immediate action be taken to prevent further misuse and protect the user's account and the transit system 100.

[0114] In some embodiments, immediate action could include taking steps to restrict the use of the transit product, or to restrict the use of any handheld media with PANs 314 associated with the transit product. In one embodiment, the PAN 314 could be "hotlisted" to restrict the use of the associated handheld media at the access control points 208. This restriction could happen immediately when potential misuse is detected at the access control point 208, or the restricted PANs 314 could be sent our in batches periodically from the transit system 100. The restriction could prevent a PAN 314 from being used at all, including for any current transaction when potential misuse is detected. Alternatively, the restriction could allow any current transactions to proceed, but could restrict future transactions. The restriction could also be partial, allowing only a certain number of uses of the transit product during a time period. For example, a user account with a monthly transit pass could be restricted to ten uses per week, or to two uses per day.

IPR2025-01150
Apple EX1071 Page 552

[0115] In cases where the potential for misuse is less certain, the action taken may include manual inspection and/or further processing. For example, the times and locations associated with a PAN 314 may seem to indicate that although it would not be impossible for a single user to be using the PAN 314, it would be unlikely. In this case, the detection algorithm could flag the account as one possibly requiring more scrutiny. The travel patterns associated with the account could then be manually inspected by a human operator, or the travel patterns could be further analyzed by different types of detection methods to verify any potential misuse. If the further inspection or processing determines that the potential misuse is likely, then the account may be "hotlisted" as described above. Alternatively or additionally, the user and/or issuing bank institution could be notified. In one embodiment, a flagged account may collect more transaction identifiers from each subsequent transaction for processing. The detection algorithm could also use a larger subset of the transaction history or could compare the transaction identifiers with additional user profiles. It will be understood that other embodiments may use a combination of these and other techniques in taking an action after the detection of potential misuse.

[0116] In cases where it is determined that the user is allowing others to use his/her PAN 314 to access that transit system 100, either the transit system 100 or the user may specify that the additional uses be charged to the user account without restricting use of the card 310. For example, a user may swipe a payment card 310 multiple times at an access control point 208, allowing multiple users to enter the transit system 100 with his/her monthly pass. The first use of the card 310 could be allowed under the monthly pass, and each additional use could be charged to the user as an additional single-ride use. Charging for additional uses may result in a charge to the user account, or if the handheld media is a payment card 310, the additional charges may be charged directly to the payment card 310. Charging the payment card 310 in this manner may be the result of preference set by the user in the user account, and it may combined with other actions, such as restricting the PAN's 314 use or notifying the user.

[0117] In the foregoing description, for the purposes of illustration, methods were described in a particular order. It should be appreciated that in alternate embodiments, the methods may be performed in a different order than that described. It should also be appreciated that the methods described above may be performed by hardware components or may be embodied in sequences of machine-executable instructions, which may be used to cause a machine, such as a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the methods. These machine-executable instructions may be stored on one or more

IPR2025-01150
Apple EX1071 Page 553

machine readable mediums, such as CD-ROMs or other type of optical disks, floppy diskettes, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, flash memory, or other types of machine-readable mediums suitable for storing electronic instructions. Alternatively, the methods may be performed by a combination of hardware and software.

[0118] Although many of the embodiments disclosed hereinabove use a contactless payment card 310, this is only one type of handheld media that is contemplated by this invention. It will be understood that many other types of handheld media may be used as a fare media 250, and that all of the embodiments described herein can utilize various forms of handheld media, in addition, and as an alternative to, contactless payment cards.

[0119] While illustrative and presently preferred embodiments of the disclosed systems, methods, and machine-readable media have been described in detail herein, it is to be understood that the inventive concepts may be otherwise variously embodied and employed, and that the appended claims are intended to be construed to include such variations, except as limited by the prior art.

IPR2025-01150
Apple EX1071 Page 554

CLAIMS

1. A method for detecting potential misuse of a primary account number (PAN) associated with a handheld media in a transit system having one or more access points, the method comprising:

creating a user account for managing transactional information, the user account comprising a transit product;

enrolling the handheld media for use as fare media for the transit product, wherein the PAN is stored in the user account;

receiving, from the one or more access points of the transit system, a plurality of fare transaction records, wherein each fare transaction record in the plurality of fare transaction records comprises:

the PAN associated with the handheld media; and

a transaction counter;

determining a potential misuse of a handheld media associated with the PAN, wherein the determination is based, at least in part, on a sequence of a plurality of transaction counters corresponding to the plurality of fare transaction records; and

taking an action related to using the handheld media as fare media for using the transit product.

2. The method of claim 1, wherein the handheld media is a smart card having near-field communication capabilities, wherein the transaction counter is stored on the handheld media, and wherein the transaction counter increments at least every time the handheld media is used at the one or more access points.

3. The method of claim 1 or claim 2, wherein the potential misuse is determined by identifying gaps in the sequence of the plurality of transaction counters.

4. The method of claim 1 or claim 2, wherein the potential misuse is determined by determining that the sequence of the plurality of transaction counters is not ascending.

IPR2025-01150
Apple EX1071 Page 555

5. The method of claim 1 or claim 2, wherein the potential misuse is determined by comparing the sequence of the plurality of transaction counters to a user profile and identifying deviations.

6. The method of claim 1 or claim 2, wherein:

each fare transaction record further comprises a transaction time and a transaction location; and

the potential misuse is further determined, at least in part, on a pattern of the transaction times and locations of a plurality of the transaction times and locations corresponding to the plurality of fare transaction records.

7. The method claim 6, wherein the potential misuse is determined by identifying a gap in the sequence of the plurality of transaction counters that is larger than a corresponding time gap by a calculated amount.

8. A method for detecting potential misuse of a primary account number (PAN) associated with a handheld media in a transit system having one or more access points, the method comprising:

creating a user account for managing transactional information, the user account comprising a transit product;

enrolling the handheld media for use as fare media for the transit product, wherein the PAN is stored in the user account;

receiving, from the one or more access points of the transit system, a plurality of fare transaction records, wherein each fare transaction record in the plurality of fare transaction records comprises:

the PAN associated with the handheld media;

a transaction time; and

a transaction location;

determining a potential misuse of a handheld media associated with the PAN, wherein the determination is based, at least in part, on a pattern of the transaction times and locations of a plurality of the transaction times and locations corresponding to the plurality of fare transaction records; and

IPR2025-01150
Apple EX1071 Page 556

taking an action related to using the handheld media as fare media for using the transit product.

9. The method of claim 8, wherein the potential misuse is determined by indentifying multiple fare transactions that take place within a predetermined time window.

10. The method of claim 8, wherein the potential misuse is determined by indentifying fare transactions at distant locations that occur within a predetermined time window.

11. The method of claim 8, wherein the potential misuse is determined by indentifying first and second fare transactions wherein travel time between the locations of the first and second fare transactions exceeds a difference between the transaction times of the first and second fare transactions.

12. The method of claim 8, wherein the potential misuse is determined by comparing the pattern of the transaction times and locations to a user profile and identifying deviations.

13. The method of claim 8, wherein:

each fare transaction record further comprises a transaction counter; and

the potential misuse is determined, at least in part, on a sequence of a plurality of transaction counters.

14. A server for detecting potential misuse of a primary account number (PAN) associated with a handheld media in a transit system having one or more access points, the server comprising:

a network interface configured to communicate with a network;

an input interface configured to receive information from the one or more access points of the transit system;

a processor communicatively coupled with the network interface, the input interface, and a memory;

the memory having instructions that, when executed by the processor, cause the server to:

IPR2025-01150
Apple EX1071 Page 557

create a user account for managing transactional information in the memory, the user account comprising a transit product;

enroll the handheld media for use as fare media for the transit product, wherein the PAN is stored in the user account in the memory;

receive, from the input interface, a plurality of fare transaction records, wherein each fare transaction record in the plurality of fare transaction records comprises:

the PAN associated with the handheld media; and

a transaction identifier;

determine, by the processor, a potential misuse of a handheld media associated with the PAN, wherein the determination is based, at least in part, on a relationship between a plurality of transaction identifiers of the plurality of fare transaction records; and

take an action related to using the handheld media as fare media for using the transit product.

15. The server of claim 14, wherein the determination of potential misuse of the handheld media associated with the PAN comprises a determination that more than one individual is using the handheld media associated with the PAN.

16. The server of claim 14, wherein:

each transaction identifier comprises a transaction counter; and;

the potential misuse is determined, at least in part, on a sequence of a plurality of transaction counters.

17. The server of claim 14, wherein:

each transaction identifier comprises a transaction time and a transaction location; and

the potential misuse is determined, at least in part, on a pattern of the transaction times and locations of a plurality of the transaction times and transaction locations.

18. The server of any one of claims 14 to 17, wherein the action related to using the handheld media as fare media for using the transit product comprises denying future use as fare media of any handheld media associated with the PAN.

IPR2025-01150
Apple EX1071 Page 558

19. The server of any one of claims 14 to 17, wherein the action related to using the handheld media as fare media for using the transit product comprises charging the user account a fee for one or more of the plurality of fare transaction records.

20. The server of any one of claims 14 to 17,

further comprising an output interface configure to send notifications associated with potential misuse of the handheld media associated with the PAN; and

wherein the action related to using the handheld media as fare media for using the transit product comprises sending, from the output interface, a notification regarding the potential misuse of the handheld media associated with the PAN.

21. A method for detecting potential misuse of a primary account number (PAN) associated with a handheld media in a transit system having one or more access points, the method being substantially as described herein with reference to the accompanying drawings.

22. A server for detecting potential misuse of a primary account number (PAN) associated with a handheld media in a transit system having one or more access points, the server being substantially as described herein with reference to the accompanying drawings.

IPR2025-01150
Apple EX1071 Page 559

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 December 2005 (15.12.2005)

PCT

(10) International Publication Number
WO 2005/119607 A2

(51) International Patent Classification[7]: G07F 19/00

(21) International Application Number:
PCT/US2005/019988

(22) International Filing Date: 3 June 2005 (03.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/576,894 3 June 2004 (03.06.2004) US
60/591,998 28 July 2004 (28.07.2004) US

(71) Applicant *(for all designated States except US)*: **TYFONE, INC.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SPITZER, Thomas N.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US). **TADEPALLI, Prabhakar** [US/IN]; 290 Phase II, Adarsh Palm Meadows, Airport Whitefield Road, Bangalore, Karnataka 560066 (IN). **NARENDRA, Siva G.** [IN/US]; 7180 SW 84th Avenue, Portland, Oregon 97223 (US).

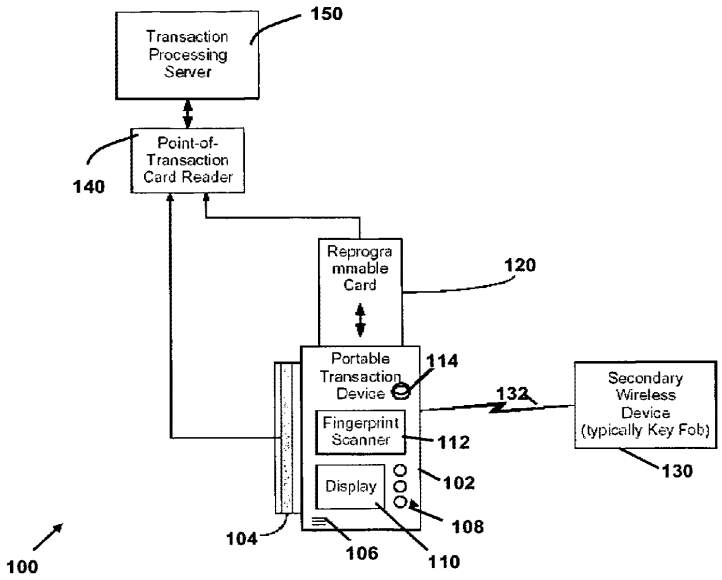
(74) Agent: **LEMOINE, Dana B.**; LeMoine Patent Services, PLLC, c/o Portfolio IP, P.O. Box 52050, Minneapolis, Minnesota 52050 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURING FINANCIAL TRANSACTIONS



(57) Abstract: A financial transaction system utilizes multi-factor authentication to secure financial transactions.

WO 2005/119607 A2

IPR2025-01150
Apple EX1071 Page 560

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR SECURING FINANCIAL TRANSACTIONS

Field

The present invention relates generally to portable transaction devices, and more specifically to portable transaction devices having various security features.

Background

Instances of financial card fraud and identity theft have increased dramatically in recent years, particularly with the rapid increase of online and electronic transactions. Solutions of varying efficacy have been proposed to protect financial information and otherwise guard against fraud and theft. Firewalls protect computer systems against unauthorized access; however, they cannot be completely assured of the identities of individuals accessing the network. Various electronic devices may be employed to verify the identity of individuals; however, these devices often permit authentication information to be accessed. Some systems provide significantly improved security, but at the expense of requiring substantial changes to point-of-sale devices or other parts of the transactional infrastructure.

Brief Description of the Drawings

Figures 1 and 2 show transaction systems with multi-factor authentication;

Figure 3 shows a block diagram of a programmable card;

Figure 4 shows a block diagram of a secondary wireless device;

Figure 5 shows a computer and base station;

Figure 6 shows usage models for various embodiments of the present invention;

Figure 7 shows an intelligent electronic device capable of printing checks;

Figures 8-10 show various methods for financial card transaction verification in accordance with various embodiments of the present invention;

IPR2025-01150
Apple EX1071 Page 562

Figure 11 shows a flexible form factor for a programmable financial card;

Figure 12 shows an exploded perspective view of the programmable financial card of Figure 11;

Figure 13 shows usage models for a secondary wireless device in card-present transactions and card-not-present transactions;

Figure 14 shows an architecture diagram for a transaction system with multi-factor authentication;

Figure 15 shows usage models for electronic money transfer;

Figure 16 shows usage models for pre-paid card recharge; and

Figure 17 shows business methods.

Description of Embodiments

In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, various embodiments of an invention. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

The present disclosure relates generally to use of a portable transaction device having various security features. The security features may be employed to particular advantage in financial transactions, so as to enhance security beyond that currently available in transactions conducted with financial cards,

IPR2025-01150
Apple EX1071 Page 563

bank checks and existing computing devices. Traditionally, financial cards have information physically present on the front face and in the magnetic stripe. Similarly, bank account number, account holder's name, routing number and the address are present in the face of the checks. If a financial card or a checkbook is lost or stolen, or if the card is skimmed (an unauthorized swipe to gather card holder information stored on the stripe), the information is insecure and is available for use by anyone. Similar risks are present with computing devices and other electronic devices used in financial transactions.

Accordingly, as shown in Fig. 1, a transaction system 100 with multi-factor authentication may be employed. As shown in this embodiment, the system 100 may include: a central transaction processing server 150; a point-of-sale transaction card reader 140; a portable transaction device 102 for use in credit/debit card type transactions; a key fob or other secondary wireless device 130 configured to wirelessly communicate with the portable transaction device 102; a reprogrammable card 120 that may be inserted into the portable transaction device 102 and reprogrammed with a one-time use transaction number or a reprogrammable electronic stripe 104 attached directly to the portable transaction device 102.

The portable transaction device 102 may include a camera (video and picture) component 114, a biometric (e.g., fingerprint) scanner 112, a display 110, a voice (microphone and speaker) component 106, and controls 108. The portable transaction device 102 may also include voice-activation and camera functionality. The secondary wireless device 130 may communicate wirelessly with the portable transaction device 102 using any type of wireless communications protocol. For example, the secondary wireless device 130 and the portable transaction device 102 may communicate using a Bluetooth type wireless link 132.

Where a one-time use transaction number is employed, the number may be generated by the card issuer or locally by the portable transaction device 102. Generation of the single-use number may be accomplished in one of several ways. For example, when an account is issued the card holder may get several pre-assigned surrogate numbers. The numbers will also have a pre-specified sequence. This sequence is known to the issuing bank and the user's portable

IPR2025-01150
Apple EX1071 Page 564

transaction device 102. The issuing bank will authorize payments only based on the expected sequence of account numbers. If out-of-sequence account numbers are used, then the issuing bank will consider that transaction as a potential theft. The issuing bank can also use this feature to track the merchant involved in the potentially fraudulent transaction.

According to another example, a pre-assigned sequence can be reset to the original starting number on the list depending on user input or other triggers. In addition, the list of numbers can be downloaded via the mobile phone network on a regular basis. This can enhance security by minimizing the potential for repetitive number lists.

Regardless of the particular method, upon receipt of the surrogate card number, the merchant typically sends the surrogate card number to the card issuer for authorization/validation. Merchants do not need to install additional software to receive surrogate card numbers or to transmit them to card issuers. When the card issuer receives the account number, it is flagged as a single-use number and decoded to reveal the cardholder's standing account number. An authorization or denial is attached to the account number, which is recoded back to the temporary account number and sent to the merchant. Any attempt to reuse a surrogate card number outside the parameter results in denied authorization. In addition to or instead of these examples, other methods for generating one-time use numbers may be employed.

In conducting a transaction, the user, possessing both the secondary wireless device 130 and the portable transaction device 102, may press a control button 108 on the portable transaction device 102 requesting that the card 120 or electronic stripe 104 be readied with a new one-time use transaction number. The electronic stripe 104 may be selected by the user for use in swipe-type card readers, and the card 120 may be selected for either swipe-type card readers or insertion-type card readers, such as ATMs. It will be appreciated that the device 102 may be manufactured with only an electronic stripe, or only a card reader, rather than both. It will be further appreciated that the card 120 may include a reprogrammable magnetic stripe, a reprogrammable electronic stripe, or may be a so-called "smart" card with a reprogrammable internal memory, and the

IPR2025-01150
Apple EX1071 Page 565

portable transaction device 102 may be configured to interface and reprogram one or more of these types of cards.

It should be appreciated that the portable transaction device 102 may be implemented in a variety of different configurations. For example, as described at length below and shown below in an alternate system depiction (Fig. 2), the portable transaction device may be implemented as, or in connection with, a mobile telephone.

Fig. 2 shows a transaction system with multi-factor authentication. Transaction system 200 includes transaction processing server 150, point-of-sale (POS) transaction card reader 140, mobile telephone 202, removable and reprogrammable card 205, and secondary wireless device 130. Mobile telephone 202 is an example of a portable transaction device, and any reference made herein to a portable transaction device is meant to include mobile telephones as well as other portable transaction device embodiments.

The mobile telephone 202 may include a camera (video and picture) component 114, a biometric (e.g., fingerprint) scanner 112, a display 110, a voice (microphone and speaker) component 106, and controls 108. The mobile telephone 202 may also include voice-activation and camera functionality. The secondary wireless device 130 may communicate wirelessly with the mobile telephone 202 using any type of wireless communications protocol. For example, the secondary wireless device 130 and the mobile telephone 202 may communicate using a Bluetooth type wireless link 132. Further, the mobile telephone may communicate with a cell network, shown by signal 232.

Removable and reprogrammable card 205 may be utilized in many ways. For example, removable and reprogrammable card 205 may be left in the mobile telephone 202 for use in swipe-type card readers, or may be removed from mobile telephone 202 for use with insertion-type card readers. Examples of insertion-type card readers include automatic teller machines (ATMs).

In the example of Fig. 2, the mobile phone 202 provides all the functionality of the previously-described portable transaction device 102 (Fig. 1). In addition, the ability of the mobile phone 202 to access a communications network (e.g., the cell phone network) may be used to provide additional functionality. For example, if the cell phone is lost, a call can be placed through

IPR2025-01150
Apple EX1071 Page 566

the network to disable all financial card functions. If the key fob is lost, a new key fob can be mailed to the user and the configuration information can be updated automatically by placing a call through the cell phone network.

Regardless of the particular configuration, the system may be configured to eliminate or reduce fraudulent transactions by performing multiple authentications of each transaction, as follows. Possession of the portable transaction device provides a first factor of authentication. Second, the fingerprint of the user may be scanned and checked against a fingerprint stored in memory on the device. Third, at the time of the transaction, the wireless link to the secondary wireless device may be checked to verify that the secondary wireless device is communicating a proper device ID to the portable transaction device, thus indicating that the secondary wireless device is located within a predetermined distance of the portable transaction device. If these authentication steps are satisfied, the electronic stripe or card is reprogrammed with a one time use transaction number. In addition, the portable electronic device may store information pertaining to multiple different cards, and the user would be allowed to supply an input specifying which of the cards would be designated for use in the upcoming transaction.

Once the card is readied for use after authentication and any required user input, the user or a store clerk may swipe the electronic stripe through a swipe-type card reader, remove the card from the device and swipe it in a swipe-type card reader, or feed it into an insertion-type card reader, such as found on an ATM. As an additional authentication step, the one-time use transaction number may be checked by the transaction processing server for validity.

As described above, various embodiments of the present invention provide multi-factor authentication. For example, various embodiments of the invention may use two or three factor authentication for access control and information or identity theft prevention of financial card, bank check, electronic and computing devices. Two-factor authentication is defined as providing access based on validating whether the user has access to at least two verifiable pieces of information that are truthful and are available only to him/her. An example of two factor authentication is having access to a debit card and knowing the correct PIN number to complete a debit card transaction. Similarly,

IPR2025-01150
Apple EX1071 Page 567

three-factor authentication is defined as providing access based on validating whether the user has access to at least three verifiable pieces of information that are truthful and are available only to him/her.

The following is an outline of various system elements that may be used in implemented various embodiments of the described systems and methods. It will be appreciated that no single element is essential to every possible exemplary embodiment.

1. Portable transaction device (e.g., portable telephone)
    A. Wireless interface configured to detect secondary wireless device when within predetermined distance (e.g. Bluetooth)
    B. Fingerprint scanner
    C. Memory storing fingerprint data of authorized user
    D. Display (optional)
    E. Controls for reprogramming card/stripe
    F. Card insertion slot
    G. Electronically reprogrammable stripe
    H. Camera functionality: when the portable transaction device is activated, a photograph of the user may be taken. The photograph may be send to the card issuer and/or displayed on the portable transaction device during use to provide additional security (e.g., a fourth authentication factor)
    I. Voice-activation functionality
2. Wireless secondary device (e.g. key fob)
    A. Wireless link to portable transaction device
3. Card
    A. Magnetically programmable stripe OR electronically programmable stripe, OR electronically programmable internal memory (so called smart card)
    B. Configured to be inserted into portable transaction device and programmed with a one-time use card number on a per-transaction basis
4. Point of Transaction Card Reader
5. Transaction Processing Server
6. Authentication factors (may be implemented in varying combinations) to determine if a pending transaction is fraudulent

IPR2025-01150
Apple EX1071 Page 568

A. Wireless secondary device within predetermined range of portable transaction device

B. Scanned fingerprint matches stored fingerprint

C. Single-use transaction number written to card is valid

The financial transaction system and portable electronic device described herein may be advantageously employed in various settings in addition to or instead of those already described. Discussed below are various additional usage models and settings under the headings "Quicker time-to-market software only solution," "Combined electronic cards and software solutions," and "Personal money management."

1. Quicker time-to-market software only solution

Single-use number software installed on any mobile phone can help with securing card-not present transactions and can extend the idea initiated by Verified-By-VISA to all mobile phone users, thereby increasing the security of e&m-commerce transactions almost immediately. Various software embodiments of the present invention, along with already existing mobile infrastructure such as cameras on phones, SMS & MMS, and GPRS may be used effectively to increase e-commerce, and m-commerce.

2. Combined electronic cards and software solutions

Various embodiments of the present invention that include electronic stripe cards or smartcards may be used for the following:

A. Customers can inform his/her bank of a certain charge limit, beyond which the user would have to provide additional security through SMS message before the transaction can be completed.

B. A service provider may locate a customer by identifying the phone through the current network it is operating in. Since the card is integrated into the phone, a card being used outside its typical usage area can be readily identified. If it is being used in a "negative list" area, for example, the bank can confirm user authenticity with the user using SMS or mobile call. As an added value, once user authenticity is confirmed, locations of ATMs and merchant promotions can be sent directly to the user at his/her request.

IPR2025-01150
Apple EX1071 Page 569

C. To recharge stored-value/prepaid cards on the fly, by extending m-banking to the payment transaction level.

D. Be a money exchange mechanism between individuals by using the VISA or MasterCard authentication networks, i.e. replace services like Western Union with more convenient m-banking, m-cashing networks. Where POS installations are in their infancy, card issuing banks and merchant banks can reap value from mobile-to-mobile transactions while not compromising the integrity of their existing transaction mechanisms.

E. Provide more convenience and control to VisaBuxx customer segments by allowing users transparency to their secondary and tertiary cards, provide limits to transactions beyond which the primary card-holder needs to approve and have the ability to recharge the secondary and tertiary cards when pre-determined levels are reached.

F. Provide entry level prepaid cards/phones to "Teens" while employing budgetary controls (as in debit cards).

G. Use camera, fingerprint, and voice for authentication of card-present transactions.

H. Where appropriate, combine loyalty/incentive programs with cards, minutes used thereby align interest with the SmartCard program.

I. Where appropriate, use Infra-red, Bluetooth, or other wireless payments schemas to help banks get direct control of contactless payment paradigms.

3. Personal Money Management

Voice modules on phones can be used to record transactions and where pertinent, the transactions can be downloaded into money management software. This eliminates the hassle of having to type out all transactions and, as bandwidth improves, allows the customer to compare transactions with bank statements.

Figure 3 shows a block diagram of a programmable card. Programmable card 300 may be utilized as removable and reprogrammable card 205 (Figure 2). Programmable card 300 includes thin profile battery 302, power management circuitry 304, microcontroller with flash 306, Bluetooth front end 310, Bluetooth

IPR2025-01150
Apple EX1071 Page 570

antenna 312, universal serial bus (USB) and power supply connector 322, and display driver 320.

Figure 4 shows a block diagram of a secondary wireless device. Secondary wireless device 400 may be utilized as secondary wireless device 130 (Figures 1, 2). Secondary wireless device 400 includes thin profile battery 402, power management circuitry 404, microcontroller 406, read only memory (ROM) 420, FLASH memory 408, Bluetooth front end 410, Bluetooth antenna 412, and USB and power supply connector 422.

Figure 5 shows a computer and base station. Computer 510 may be any type of computer or computing device capable of being operated by a user and being coupled to base station 520. For example, computer 510 may be a personal computer, a handheld computer, or the like. Computer 510 may include software to drive the base station and its components, and may also include graphical user interface (GUI) front end software for step-by-step user instructions for programming a reprogrammable card. As described above, programming a reprogrammable card may include selection of rolling numbers and associated maximum transaction amounts.

As shown in Figure 5, base station 520 includes universal serial bus (USB) interface 528, card reader 522, secondary wireless device slot 526, and a reprogrammable card slot 524. Base station 520 may communicate with computer 510 over a cable coupled to USB interface 528. Although interface 528 is shown as a USB interface, this is not a limitation of the present invention. Any suitable interface may be used without departing from the scope of the present invention.

Base station 520 provides an interface between computer 510 and one or more other items. For example, in some embodiments, a reprogrammable card may be placed in slot 524 for communications with computer 510, or for programming by computer 510. Further, in some embodiments, a secondary wireless device may be placed in slot 536 for communications with computer 510, or for programming by computer 510. Also in some embodiments, base station 520 may be used for charging a reprogrammable card and secondary wireless device.

IPR2025-01150
Apple EX1071 Page 571

Base station 520 may also be used for reading standard magnetic cards to store information into a reprogrammable card. For example, a reprogrammable card may be placed in slot 524, and one or more standard magnetic cards may be swiped through card reader 522. Base station 520 may include circuitry to program a reprogrammable card directly from swiped magnetic cards, or may program a reprogrammable card under the control of computer 510.

Figure 6 shows usage models for various embodiments of the present invention. Figure 6 shows user icons to represent users in various stages of use, and arrows to indicate actions. The various usage models are now described. At 602, an un-programmed reprogrammable card, a secondary wireless device, and a base station are shipped to a user. Software on CD-ROM and an optional travel kit may also be shipped to the user. At 604, the user 612 installs the software and connects the base station to a home personal computer (PC). The software is run to initiate programming, and the user scans a fingerprint into the reprogrammable card. The user plugs the reprogrammable card and the secondary wireless device into the base station.

At 614, the software communicates with a server 622 to activate the reprogrammable card and secondary wireless device. Server 622 may be held at a secure location separate from the user and from a card issuing bank 660. For example, server 622 may be held by a company that provides reprogrammable cards and secondary wireless devices. Further, information may be stored on the server 622 for retrieval in case of loss of the reprogrammable card or secondary wireless device. The user 612 may then scan one credit card at a time into the base station. This may be repeated any number of times. The user 612 is shown at a PC performing the actions just described.

At 618, the user 642 has completed the setup, and has a reprogrammable card available for use. The user 642 carries both the reprogrammable card and the secondary wireless device. It is best to keep the secondary wireless card separate from the reprogrammable card. The secondary wireless device never has to be accessed by user 642 to initiate a transaction. At the end of the day, the user 642 plugs the reprogrammable card and the secondary wireless device into the base station for charging and account summary.

IPR2025-01150
Apple EX1071 Page 572

At 644, user 670 initiates a transaction with merchant 672. To initiate the transaction, user 670 activates the reprogrammable card using a fingerprint scan and selects the credit card to use. The reprogrammable card authenticates only in the presence of the appropriate secondary wireless device. Information programmed on the reprogrammable card's electronic stripe will get erased automatically after a predetermined timeout. For example, the information may get erased after five minutes. To prevent multiple swipes, the information in the reprogrammable card may be erased after one swipe. An alternative is to provide a rolling account number that the credit card company can map to the actual account number. The account number may then roll to a new number for each fingerprint scan.

If a user 652 loses one of the reprogrammable card or secondary wireless device, shown by 654, the company will mail a preprogrammed reprogrammable card or secondary wireless device to the user 652 at 624. If a user 632 loses both the reprogrammable card and secondary wireless device, shown by 616, the company will help deactivate all user credit card accounts and start the process again at 634.

As described above, reprogrammable cards may take any suitable form. For example, reprogrammable cards may be magnetic stripe cards, electronically programmable cards, smart cards, or any combination. Various embodiments are now described under headings relating to magnetic cards, electrically programmable cards, and smart cards. It should be noted that nothing in these embodiments should be considered essential.

Magnetic stripe cards

Embodiments that include magnetic stripe cards are now described with reference to Figures 1-6. Various embodiments of the present invention include: (i) an intelligent (memory, computational power) electronic device that has magnetic stripe reading / writing capability, and a wireless link such as Bluetooth; (ii) a fingerprint scanner on the intelligent electronic device; (iii) electronic device such as a key that has memory and wireless connection such as Bluetooth; and (iii) an empty generic three track magnetic stripe card that can be programmed by the intelligent electronic device on a per transaction basis. For

IPR2025-01150
Apple EX1071 Page 573

example, Figures 1 and 2 show portable transaction devices 102 and 202 that may be used as intelligent electronic devices. Further, portable transaction devices 102 and 202 are shown having wireless links and fingerprint scanners. Portable transaction device 202 is shown having a magnetic stripe reader/writer to program reprogrammable card 205.

The use of an intelligent electronic device with a fingerprint scanner or the use of an intelligent electronic device and the key (secondary wireless device) constitutes a two-factor authentication solution while the use of all three (intelligent electronic device with the fingerprint scanner and the key) constitutes a three-factor authentication solution.

The user first installs interface software in the intelligent electronic device. Using the installed software the user scans his/her portfolio of standard financial cards using the integrated magnetic stripe card reader. The user may also enter information necessary for financial card transactions that may not be present in the magnetic stripe such as a security code. The user also scans a fingerprint to associate the cards with the user. The financial card information is stored in the intelligent electronic device in encrypted form. The decryption code for the information stored in the intelligent electronic device may be stored in the key. Each intelligent electronic device may have an associated key that is unique. Once all the relevant information is stored in the intelligent electronic device, the user may slide the generic card into the integrated magnetic stripe reader/writer.

When the user is ready to use a financial card for a transaction s/he logs into the intelligent electronic device using the fingerprint scanning device or by entering a password. In the two-factor solution, the card user can proceed with initiating the transaction. In the case where the user opts for a three-factor solution, the intelligent electronic device will let the login occur only if it is able to establish a wireless link with its associated key. The user then selects the type of card to use. After log in using either approach, the intelligent electronic device receives the decryption code from the key to access the information about the selected card, if key based authentication is used. If fingerprint scan based authentication is used for two-factor then the decryption code is stored in the intelligent electronic device itself, which will be provided after the

IPR2025-01150
Apple EX1071 Page 574

authentication. The user then pulls out the generic card, during which the card is programmed by the magnetic writer. At this point the intelligent electronic device deletes the decryption key information that it received from the key. Once programmed, the generic card can be used like any other magnetic stripe financial card. Once the transaction is completed the user inserts the card back into the intelligent electronic device during which the information stored in the magnetic stripe is erased.

Further embodiments may be generated by combining various feature of magnetic card embodiments with electronically programmable embodiments and smart card embodiments, described below. The use of magnetic cards as reprogrammable cards may obviate the need for a power supply in the card, and provides a mechanism to use traditional three track magnetic stripe cards and hence does not require development of a card that has an alternate programming medium.

Note that the need for having access to the intelligent electronic device along with fingerprint scanning and the presence of a key provides a three-factor authentication. The same can be implemented without the key in which case the security of the information stored in the intelligent electronic device may be achieved with two-factor authentication through fingerprint scanning. The key can also be replaced with a PIN input + fingerprint scanning; however, without the key the decryption code is physically stored in the same device as that of the information. A key along with the intelligent electronic device can be used as two-factor authentication.

Electronically programmed cards

Embodiments that include electronically programmable cards are now described with reference to Figures 1-6. Various embodiments of the present invention include: (i) a base station having the ability to scan a user's card information; (ii) an electronic card that has an electronically programmable region that has identical dimensions as that of a magnetic stripe (henceforth referred to as the electronic stripe), a wireless link such as Bluetooth and a fingerprint scanner; (iii) an electronic device such as a key that has memory and a wireless link such as Bluetooth. For example, Figures 1 and 2 show portable

IPR2025-01150
Apple EX1071 Page 575

transaction devices 102 and 202 that may be used as intelligent electronic devices. Further, stripe 104 (Figure 1) may be a reprogrammable electronic stripe, and stripe 204 (Figure 2) may be a reprogrammable electronic stripe. Note that the electronic programming may be done using electric currents. The direction of current travel will change the magnetic field and hence can be used to code for a digital "1" or a digital "0". This information can then be read by a traditional magnetic stripe reader present in point-of-sale.

The electronic card may come preprogrammed with software that will allow users to input card information or the users may first install interface software in the intelligent electronic device or in the base station. Using the installed software the user will then enter standard financial card information. An optional card reader can be used to read most of the information present in a financial card. The financial card information will be stored in the intelligent electronic device in encrypted form. The decryption code for the information stored in the intelligent electronic device will be stored in the key. Each intelligent electronic device will have an associated key that is unique.

When the user is ready to use a financial card for a transaction s/he logs into the intelligent electronic device using a fingerprint scanning device or by entering a password. In the two-factor solution, the card user can proceed with initiating the transaction. In the case where the user opts for a three-factor solution, the intelligent electronic device will let the login occur only if it is able to establish a wireless link with its associated key. The user then selects the card to use through a card selection button on the face of the intelligent electronic device. The intelligent electronic device receives the decryption code from the key to access the information about the selected card. The intelligent electronic device programs the electronic stripe. At this point the intelligent electronic device deletes the decryption key information that it received from the key. Once programmed the intelligent electronic device can be used like any other magnetic stripe financial card. Once the transaction is completed, the intelligent electronic device erases the information stored in the electronic stripe. The electronic stripe can be programmed to time out after a certain length of time or after a specified number of swipes.

IPR2025-01150
Apple EX1071 Page 576

In some embodiments, the key may store all critical information from the intelligent electronic device as backup in encrypted format. The decryption code for information stored in the key may be present in its associated intelligent electronic device. Also in some embodiments, an intelligent electronic device may include software having the ability for the intelligent electronic device to either limit to one swipe after programming or record how many times a card was swiped between magnetic stripe programming and erasing. In further embodiments, the intelligent electronic device may include software and/or voice recognition that tracks the expenses based on user input every time the card is used or when the user makes any expense transaction to provide categorized expense summary. In further embodiments, the intelligent electronic device may include the ability to communicate to the point-of-sale the amount entered by the user for transaction – this however will require change to the point-of-sale. In still further embodiments, the intelligent electronic device may include the ability to generate one account number from a set of account numbers. These numbers will be generated in a predetermined sequence (or one time use numbers) that will expire at the end of every transaction to eliminate card cloning and counterfeiting operations. In some embodiments, this may be achieved by either using the 19 digit PAN Field and/or Discretionary Data character fields allocated in the magnetic stripe standards. For example, the way the variable number (required for off-line transactions) would work is that a card holder may be assigned let us say 100 account numbers. The account numbers will revolve in a pre-determined order. The issuing bank will know what order will be used and so will the intelligent electronic device. For each authentication the intelligent electronic device will activate one number in the pre-determined order. The variable number also applies for on-line transactions and can either replace or work with the one time use numbers.

In some embodiments, the programmed magnetic stripe may be detached from the main unit for use in transactions where the card is swallowed in whole to complete the transaction (such as in an ATM machine or at a gasoline pump). Also in some embodiments, a fixed base station may be connected to a desktop PC or a standalone base station and can be used for charging the intelligent electronic device and key. The base station may also be used to retrieve

IPR2025-01150
Apple EX1071 Page 577

financial card information for the desktop PC from the intelligent electronic device for electronic transactions. The transaction will occur only if both the intelligent electronic device and key are present. The fixed base station may also be used to include the optional magnetic card reader to initially download the information into the intelligent electronic device. In some embodiments, an organic light emitting diode (LED) display and flexible printed circuit board (PCB) may be used to design an intelligent electronic device that has the form factor and mechanical flexibility of a plastic card so that it can be carried inside a wallet. The intelligent electronic device may also act as an agent that holds other secure information such as user ID and password for access by the user after two or three factor authentications. Further, an intelligent electronic device that is enabled with wireless may be used to show on-demand advertisement and coupons on its display. The information displayed can depend on the card holder's usage pattern, if available.

For card-not-present on-line transactions, the mode of operation may be one of the following: (a) base station will verify the presence of the intelligent electronic device along with two or three factor authentication, explained above, or (b) if random or one-time use numbers are used, then with two or three factor authentication the intelligent electronic device will provide the correct number to use for card-not-present transactions similar to card present transactions.

In electronically programmable embodiments, the user does not have to deal with a third component, the generic card, unlike the magnetic card options described above. Further, the erasing of the information stored in the electronic stripe may be automatic, whereas in the magnetic card embodiments, erasing may depend on the user sliding the generic card back into the intelligent electronic device.

Note that the need for having access to the intelligent electronic device along with fingerprint scanning and the presence of the key provides a three-factor authentication. The same can be implemented without the key in which case the security of the information stored in the intelligent electronic device is achieved with two-factor authentication through fingerprint scanning. The key can also be replaced with a PIN input + fingerprint scanning to result in three-factor authentication. However, without the key the decryption code is

IPR2025-01150
Apple EX1071 Page 578

physically stored in the same device as that of the information and therefore susceptible to theft by hacking. The key along with the intelligent electronic device may be used as two-factor authentication.

Although the various embodiments of the present invention are described above using an intelligent electronic device and key, other devices may be utilized. For example, an intelligent electronic device may be a self powered smart card device that includes a display, fingerprint reader, and Bluetooth. Further, PIN entry or other biometric authentication can be used instead of fingerprint authentication.

Smart cards

Embodiments that include smart cards are now described with reference to Figures 1-6. Various embodiments of the present invention include: (i) an electronic device such as a personal digital assistant or an intelligent electronic device with smart card interface and wireless link such as Bluetooth; (ii) an electronic device such as a key that has memory and wireless link such as Bluetooth; (iii) the ability to generate predefined card numbers at random that will expire at the end of every transaction to eliminate card cloning and counterfeiting operations; and (iv) an empty generic smart card that can be programmed by the intelligent electronic device. The assumption here is that the point-of-sale uses smart cards.

The usage model is similar to that described above with reference to magnetic stripe cards, except the Intelligent Electronic Device programs the smart card instead of the magnetic stripe card.

In some embodiments, the intelligent electronic device and the smart card may be integrated into one device. This will result in a device similar to devices described above with reference to electronically programmed cards, except it is to be used for smart card point-of-sale.

Further, in some embodiments, a standalone smart card may be utilized without the intelligent electronic device. Each smart card will have an associated key. The smart card point-of-sale will verify if the associated key is present before approving the transaction. One feature of these embodiments is

IPR2025-01150
Apple EX1071 Page 579

that the smart card is not programmable to act as one of several cards and will require change in the point-of-sale.

Although the various embodiments of the present invention are described above using an intelligent electronic device and key, other devices may be utilized. Further, PIN entry or other biometric authentication can be used instead of fingerprint authentication.

Various embodiments described thus far include "programmable" financial cards, where "programmable" refers to the fact that the information for the card's stripe is programmable to represent one of several cards held by the card holder. Embodiments are now described that are applicable to authentication for bank checks.

Authentication for bank checks

Figure 7 shows an intelligent electronic device capable of printing checks. Intelligent electronic device 700 includes storage 744 for "blank" paper checks without account information, a wireless interface to support a wireless link 732 such as Bluetooth, a fingerprint scanner 712, a display screen 710, account selection and function buttons 708, and a miniature printer 742 to print checks. Also shown in Figure 7 is a key 730 that has memory and a wireless link such as Bluetooth.

The intelligent electronic device 700 will be preprogrammed with relevant account (or accounts) information including account holder name, mailing address, account number, and bank routing number. When the user is ready to use the check book s/he will power up the intelligent electronic device. The device will authenticate the user by verifying the presence of the key and/or fingerprint ID. Once authenticated, the user will pick the account of choice and optionally enter memo along with the transaction amount information. The printer then will print the account and transaction information on the blank paper check to produce a printed check 740. Any features discussed above with reference to programmable card embodiments may utilized with intelligent electronic device 700 without departing from the scope of the present invention. Further, PIN entry or other biometric authentication can be used instead of fingerprint authentication.

IPR2025-01150
Apple EX1071 Page 580

Financial Card Transaction Verification

Figures 8-10 show various methods for financial card transaction verification in accordance with various embodiments of the present invention. Figure 8 shows an example of "real time push verification," Figure 9 shows an example of "offline push verification," and Figure 10 shows an example of "offline pull verification." The embodiments represented by Figures 8-10 are applicable for all programmable financial card embodiments described herein and for all other standard cards.

When a transaction is initiated from the point-of-sale, credit card and transaction information is transferred to an acquirer 802 and a card issuing bank 804. These transfers are shown at 812 and 822 in Figures 8-10. The card issuing bank 804 transfers an approval or denial of the transaction to the acquirer 802 and ultimately to the point-of-sale. The transfers are shown at 824 and 814 in Figures 8-10. The acquirer 802 typically pays the merchant after verification. The card issuing bank 804 then pays the acquirer 802.

In various embodiments of the invention, an additional step is added either during information processing at the acquirer or at the card issuing bank. This additional step involves instant messaging to the card holder's phone/email with the necessary transaction details, which then when approved by the card holder is recorded to be a legitimate transaction. The phone 806 can be a mobile phone running special software that indicates to the user that a new transaction has arrived for approval. If the approval is not completed within a prescribed time the transaction is marked as a possible suspect and further defensive actions can be taken. The transaction records on the mobile device 806 can be downloaded onto PC financial software for record keeping. This transfer is shown at 840. Access to mobile device instant messaging can be restricted via PIN entry, voice recognition, or other biometric authentication such as fingerprint.

Figure 8 shows a real time push verification where the issuing bank 804 sends a real time message 832 to the mobile device 806 and waits for approval or denial at 834 before approving the transaction at 824. Figure 9 shows an offline push verification where the issuing bank 804 sends a message 832, but does not

IPR2025-01150
Apple EX1071 Page 581

wait for real time approval. Instead, a user may provide later notification of approval or denial at 934, and if necessary, the issuing bank 804 may take defensive action.

In other embodiments, instead of the information being pushed via automated mobile phone instant message, it can be an information pull based implementation, such as that shown in Figure 10. In information pull implementations, the transaction details are logged on a secure web site 1008 where the user visits periodically to approve the transactions at 1034.

Figure 11 show a flexible form factor for a programmable financial card. Programmable financial card 1100 has a flexible printed circuit board (PCB) that may include embedded integrated circuit components such as memory, processing, display driver, and wireless front end. In addition, programmable financial card 1100 may include a fingerprint reader, input buttons, organic LED display, and flexible battery power.

Figure 12 shows a perspective exploded view of the programmable financial card of Figure 11. Programmable financial card 1100 includes flexible PCB 1202, programmable stripe 1204, organic LED display 1216, and fingerprint input device 1214. Flexible PCB 1202 includes flexible battery 1208, battery charging by contactless coupling 1206, memory, processing, and display driver integrated circuits 1210, and wireless front end integrated circuit and antenna 1212.

Figure 13 shows usage models for a secondary wireless device in card-present transactions and card-not-present transactions. Usage models for card-not-present transactions are show in the top portion of Figure 13, shown generally at 1302. In these embodiments, secondary wireless device 1310 communicates with various types of electronic devices that in turn communicate with point-of-sale terminals or merchants without a reprogrammable card present. For example, secondary wireless device 1310 may provide user transparent automated authentication with a home computer and base station 1320, laptop computer 1330, personal digital assistant (PDA) 1340, or cellular telephone 1350. These devices may then in turn communicate with merchants using one or more secure protocols such as: Secure Electronic Transaction

IPR2025-01150
Apple EX1071 Page 582

(SET), Mobile electronic Transaction (MeT); M-payments; or other emerging standards.

Usage models for card-present transactions are show in the bottom portion of Figure 13, shown generally at 1304. In these embodiments, secondary wireless device 1310 provides user transparent automated authentication with one or more of a reprogrammable card 1360 and portable transaction device 1370. Reprogrammable card 1360 may then communicate with point-of-sale terminals or merchants.

Multi-factor authentication may be utilized in both card-present and card-not-present transactions. For example, two factor or three factor authentication may be provided as described above with reference to Figures 1-6.

Figure 14 shows an architecture diagram for a transaction system with multi-factor authentication. Architecture 1400 is a layered architecture that represents any of the transaction systems described herein. For example, architecture 1400 may represent a portable transaction device in combination with a programmable stripe or a reprogrammable card such as those shown in Figures 1 and 2.

Architecture 1400 includes an application layer 1410, a first virtual layer 1420, a standards layer 1430, a second virtual layer 1440, and a physical layer 1450. Architecture 1400 may include more layers than those shown in Figure 14, and further, no layer shown is meant to be essential.

Application layer 1410 includes original equipment manufacturer (OEM) software (SW) 1412 and value added software 1414. OEM SW 1412 may include any software provided by a manufacturer of a portable transaction device. For example, OEM SW 1412 may include a phone book, contacts, and other software. Value added SW 1414 may include any software that directly or indirectly supports the transaction system. For example, value added SW 1414 may include a graphical user interface (GUI) for card information download, authentication, card selection, voice component, single use account number generation, e-wallet applications, or the like. Value added SW 1414 may also include a voice recognition component to record transactions for download to money management software. The foregoing list is not meant to be exhaustive, and no portion of the list is meant to be essential.

IPR2025-01150
Apple EX1071 Page 583

Virtual layer 1420 provides an application programming interface (API). The API in virtual layer 1420 may be provided by an OEM, or by a value added business, or both. For example, an OEM API may provide an interface for third party developers to develop applications for the portable transaction device. Also for example, a value added API may provide an interface for third party developers to develop applications for the combination of portable transaction device and programmable stripe or reprogrammable card.

Standards layer 1430 provides operation in compliance with one or more standards. As shown in Figure 14, standards layer 1430 provides operation in compliance with at least multimedia and communications standards. Example standards include, but are not limited to: telephony standards, TCP/IP, GPRS, USB, Bluetooth, IrDA, SMS, MMS, ECML, SSL, TLS, JPEG, MPEG, and MP3.

Virtual layer 1440 includes operating system (OS) and device drivers. Example operating systems include, but are not limited to: Symbian, Microsoft Mobile, PalmOS, and Linux. Device drivers may include drivers to provide an interface to hardware in physical layer 1450.

Physical layer 1450 includes OEM hardware 1452 and value added hardware 1454. OEM hardware 1452 may include any hardware provided by a manufacturer. For example, in embodiments where the portable transaction device is a mobile phone, OEM hardware 1452 includes the phone and any accessories provided by the OEM. Value added hardware 1454 may a reprogrammable card or stripe. In some embodiments the card or stripe may be tightly coupled to the OEM hardware and in other embodiments, the card or stripe may be insertable and removable. Physical layer 1450 may also include a voice component, image component, fingerprint capture component, a link to a secondary wireless device, or the like.

Figure 15 shows usage models for electronic money transfer. The usage model shown in Figure 15 represents the electronic transfer of money from portable transaction device 1 (1504) to portable transaction device 2 (1524). Portable transaction device 2 is also shown at 1550 ready to perform a transaction after authentication.

IPR2025-01150
Apple EX1071 Page 584

Money may be transferred electronically from portable transaction device 1 may be under a new debit card account or other account. Portable transaction device 1 requests a transfer from bank 1502 at 1503, and portable transaction device 2 may receive the electronic transfer either directly from portable transaction device 1 at 1507 or through a mobile network at 1513. For example, a direct transfer at 1507 may include communications via Infrared (IrDA), Bluetooth, cabling, or other interface. Also for example, a transfer using a mobile network may include portable transaction device 2 communicating over a data network at 1513 to receive the electronic transfer.

After the transfer, portable transaction device 2 may be used in a financial transaction. For example, a user may authenticate, shown generally at 1540, and then portable transaction device 2 may be used at 1550. A user may authenticate using any type of single or multi-factor authentication described herein. After authentication, device 1550 may be used in a financial transaction such as a merchant transaction at a point-of-sale, an ATM machine, or another transfer into a different account.

The transaction may be a card-present or card-not-present transaction. For example, a card present transaction may be performed using stripe 1560, and a card-not-present transaction may be performed using a card number that represents the account to which the money has been transferred. The card number may be a static number or may be a one time use number.

Figure 16 shows usage models for pre-paid card recharge. The usage model shown in Figure 16 represents the recharge of a stored value card or pre-paid card. For example, the holder of portable transaction device 1 may authorize a pre-paid card increase at 1634, and bank 1602 may increase the value of a pre-paid card at 1636. Portable transaction devices 1 and 2 may communicate either directly or indirectly through a mobile network at 1607. Communications 1607 may include portable electronic device 2 requesting an increase in value, and portable transaction device 1 either granting or denying a change in value.

When portable transaction device 2 receives an increase in value of a stored value or pre-paid card, and a user has authenticated, a card-present or card-not-present transaction may be performed as described above.

IPR2025-01150
Apple EX1071 Page 585

Figure 17 shows business methods. Business 1710 is a business that profits from use of the transactions systems described herein. Figure 17 is shown in the context of cellular phones being used as portable transaction devices in the transaction systems described herein, but this is not a limitation of the present invention. For example, other business methods utilize personal digital assistants (PDAs) or handheld computers as portable transaction devices.

Business 1710 may or may not manufacture value added hardware such as devices having programmable stripes, and may or may not produce value added software. In some embodiments, business 1710 owns intellectual property relating to value added hardware and software, and licenses that intellectual property. In other embodiments, business 1710 also produces value added hardware and/or software, and income is derived from those activities.

As shown in Figure 17, business 1710 may receive fees from many potential sources, including card-issuing banks 1720, phone manufacturers 1730, phone service operators 1740, customers, and third parties.

The following numbered paragraphs provide further disclosure of the systems and methods of the present description:

1. A financial transaction authentication system, including a mobile telephone (or handheld computer or other portable electronic device) having a biometric scanner and a transaction stripe that may be operatively engaged with a point-of-sale stripe reader, where the financial transaction authentication system is configured to combine biometric information with one or more additional authentication factors to secure financial transactions.

2. The system of paragraph 1, where the stripe is attached to the mobile telephone.

3. The system of paragraph 1, where the stripe is provided on a separate structure (e.g., a structure shaped and sized like a traditional financial card) that may be selectively inserted into and removed from the mobile telephone.

4. The system of paragraph 1, further comprising software configured to control financial transaction communication between the mobile telephone and various external systems involved in financial transaction, and

IPR2025-01150
Apple EX1071 Page 586

configured to control communications between the mobile telephone and access controls implemented in buildings, cars etc.

5. The system of paragraph 1, further comprising software configured to implement and apply one-time use numbers on to the transaction stripe, wherein this may include local generation of the one-time use numbers or download of one-time use numbers via a mobile telephone network.

6. The system of paragraph 1, where the information is encoded onto the transaction stripe via electrical voltage pulses that generate magnetic fields to mimic magnetic stripe tracks in standard financial transaction cards. The sequence of pulses of time duration T and 2T may be used to code for 1 and 0. Since the pulse train is not stored magnetically the stripe length can be much smaller than that of a standard card. The card substrate can thus be much smaller than a traditional financial card. The card may include the transaction stripe, optional memory and optional energy storage to support complete detaching from the mobile telephone. The detachable card may also include wireless capability to communicate to the mobile telephone.

7. The system of paragraph 1, where in multi-factor authentication, biometric data (e.g., fingerprint) is used to access the mobile phone device and PIN entry is required to access account information.

8. The system of paragraph 1, further comprising a secondary wireless device, such as a key fob, that is used to provide an additional authentication factor, namely that the mobile telephone will not allow access to the financial card account information unless the secondary wireless device is in the vicinity. Wireless key can be implemented via bluetooth protocol as an example.

9. The system of paragraph 1, where the mobile telephone is employed as a wireless authentication key for two factor authentication in accessing other electronic systems such as laptops, PCs, cars etc.

10. The system of paragraph 1, where the mobile telephone is used for card consolidation, in that information for multiple accounts is stored within a memory in the mobile telephone, and where the user may select a particular account and after proper authentication, the account information for the selected account is applied to the transaction stripe.

IPR2025-01150
Apple EX1071 Page 587

11. The system of paragraph 1, where since the system may be configured to require two or more factor authentication for gaining access to account information, the system may be employed for secure card present and card not present transactions. Also, since the one-time use number generation is integrated into the mobile telephone, card present or card not present solutions can take advantage of this security feature.

12. The system of paragraph 1, where since the information on the electronic stripe is not coded in physical locations on the magnetic stripe more bits can be conveyed to the POS between the start and the stop sentinels. These additional bits can be used to have unique ID independent of any account information. This will ensure that even if account information is stolen without this unique ID in the stripe the transaction will not be valid. So a cloned card based on known account information will not make the transaction valid without this unique ID.

13. The system of paragraph 1, where since the mobile telephone device is connected to a mobile phone network, the account holder can set a per-transaction amount limit and if a transaction exceeds that limit the user will receive a secure SMS message (or a message via any other mobile network-based messaging service) requesting validation of the transaction; the transaction will be authenticated only after the user replies the SMS with an 'overlimit' password; the password will be independent of other passwords. Note that the per-transaction limit could be zero, which will require secure SMS authentication every transaction; also, if the mobile phone is not in a cell then the financial card issuing bank will note it as a 'risky' transaction and take appropriate action, such as invalidate the account for future transaction.

14. The system of paragraph 1, where since the mobile telephone device is connected to the mobile phone network, the account activation may happen via the mobile network after 2- or 3-factor authentication. Authentication may also happen via the mobile phone network; for example, a user will have to make a phone call and the system will verify the user's voice; once the voiceprint is verified, the mobile network will be used to download the financial card information onto the mobile telephone device.

IPR2025-01150
Apple EX1071 Page 588

15. The system of paragraph 1, where the mobile telephone device will also use the voice recording component in the mobile phones to record user voice keywords. The keywords will include the type of transaction and the amount of transaction. The keywords can then be downloaded into a PC with voice recognition for automated data entry into software such as Microsoft Money or Quicken. The mobile telephone device can have two directional microphones, one for recording background noise and one for recording voice and background noise. This will improve voice recognition by canceling out background noise.

16. The system of paragraph 1, where the mobile phone network can also be used to upload account summary automatically from the card issuing bank. This can then be downloaded into a PC. All connections to the PC will be via an optional base station. The base station will also be used to charge the phone.

17. The system of paragraph 1, where the mobile phone network can also be used to update the cell phone service provider of the financial transaction details. This can be used to consolidate the mobile phone bill with the credit card transaction bill.

18. The system of paragraph 1, where since the mobile telephone device is connected to the mobile phone network, if the device is stolen the mobile phone network can be used to call the phone to delete all account information. Also, the network can be used to track a delinquent account holder.

19. The system of paragraph 1, where since the mobile telephone device is connected to the mobile phone network, gift cards and other stored value cards can be directly transmitted to a recipient if his/her telephone number is known.

20. The system of paragraph 1, where the mobile phone network can be used to upload user-specific ads/coupons into the mobile telephone device. This can also involve using Bluetooth or Infrared network to upload user specific ads/coupons.

21. The system of paragraph 1, where messages sent via the mobile phone network to and from the mobile telephone will be encrypted. Each mobile

IPR2025-01150
Apple EX1071 Page 589

telephone device will have a unique private and public key which will be used for sending secure information.

22. The system of paragraph 1, where since the mobile telephone device provides secure storage of information, it can be extended to store not such financial data but also other user information such as login IDs and passwords, account numbers for building access, user ID for access to cars, etc.

23. The system of paragraph 1, where the portable electronic device is configured to take photographs, and where a photograph of a user is taken during initial activation, and where such photograph is later employed to increase the security of a financial transaction (e.g., by providing an additional authentication factor).

24. The system of paragraph 1, where the portable electronic device is voice-activated.

25. The system of paragraph 1, where the transaction stripe is magnetically encoded via a magnetic head of the portable electronic device.

26. The system of paragraph 1, where the system is implemented using open technologies and specifications, such as ECML (electronic commerce modeling language).

27. The system of paragraph 1, where communications are secured via secure protocols such as TLS and SSL.

28. The system of paragraph 1, where the mobile telephone (or other electronic device) may be operatively interfaced with another such device to perform a peer-to-peer value transfer.

29. The system of paragraph 1, where the system may be employed to refresh value in a stored value card or like device.

30. The system of paragraph 29, where the stored value is refreshed via a mobile telephone network.

31. The system of paragraph 1, where financial card information is stored in a SIM device associated with and operatively engaged with the mobile telephone.

Although the present invention has been described in conjunction with certain embodiments, it is to be understood that modifications and variations may be resorted to without departing from the spirit and scope of the invention

IPR2025-01150
Apple EX1071 Page 590

as those skilled in the art readily understand. Such modifications and variations are considered to be within the scope of the invention and the appended claims.

IPR2025-01150
Apple EX1071 Page 591

What is claimed is:

1. A portable transaction device comprising:
memory to hold information regarding a financial card;
a slot to interface with a reprogrammable card; and
software to generate single use transaction numbers.

2. The portable transaction device of claim 1 further comprising a biometric scanner where the portable transaction device is configured to combine biometric information with one or more additional authentication factors to secure financial transactions.

3. The portable transaction device of claim 1 further comprising a wireless interface to communicate with a secondary wireless device for an additional authentication factor.

4. The portable transaction device of claim 1 further comprising controls to allow a user to select one of a plurality of financial cards with which to program the transaction stripe.

5. A portable transaction device comprising:
means for interacting with a user to provide a first authentication factor;
means for interacting with a secondary wireless device to provide a second authentication factor; and
software to request a change in value of a pre-paid card.

6. The portable transaction device of claim 5 wherein the means for interacting with a user comprises a biometric input device.

7. The portable transaction device of claim 6 wherein the biometric input device comprises a fingerprint scanner.

IPR2025-01150
Apple EX1071 Page 592

8. The portable transaction device of claim 5 wherein the portable transaction device comprises a cellular phone.

9. The portable transaction device of claim 8 wherein the software to request a change in the value of a pre-paid card comprises software on the cellular phone to communicate with a mobile network.

10. The portable transaction device of claim 8 wherein the software to request a change in the value of a pre-paid card comprises software on the cellular phone to communicate with another portable transaction device.

11. The portable transaction device of claim 5 further comprising a slot to receive the pre-paid card.

12. A portable transaction device comprising:

a user authentication component to allow a user to authenticate to the portable transaction device;

a cellular telephone component; and

a value transfer component to operatively interface to another portable transaction device to refresh value in a stored value card.

13. The portable transaction device of claim 12 wherein the value transfer component operatively interfaces with another portable transaction device using the cellular telephone component.

14. The portable transaction device of claim 12 wherein the value transfer component operatively interfaces with another portable transaction device using an Infra-red signal.

15. The portable transaction device of claim 12 wherein the user authentication component includes a biometric input device.

16. The portable transaction device of claim 15 wherein the user

IPR2025-01150
Apple EX1071 Page 593

authentication component further includes a wireless interface to communicate with a secondary wireless device.

17. A financial transaction system comprising:

a reprogrammable financial card; and

a cellular telephone having an interface to communicate with the reprogrammable card, wherein the cellular telephone includes a software component to request a change in value of a financial account.

18. The financial transaction system of claim 17 wherein the financial account represents a stored value card, and the reprogrammable card may be programmed to operate as the stored value card.

19. the financial transaction system of claim 17 wherein the financial account is accessible using a debit card, and the reprogrammable card may be programmed to operate as the debit card.

20. The financial transaction system of claim 17 further comprising a wireless interface to communicate with a secondary wireless device for authentication.

IPR2025-01150
Apple EX1071 Page 594

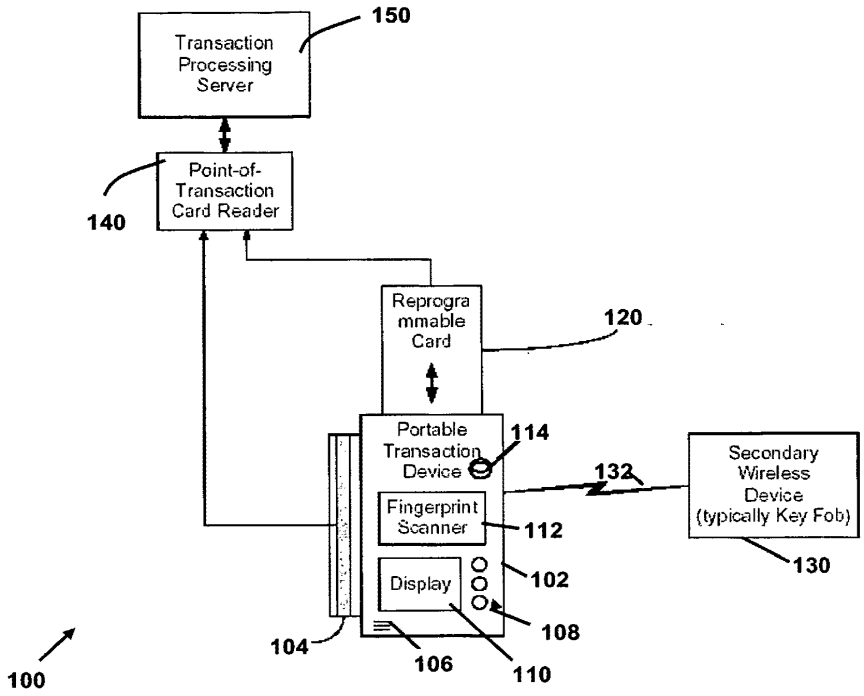

Transaction Processing Server
150
Point-of-Transaction Card Reader
140
Reprogramable Card
120
Portable Transaction Device
114
Fingerprint Scanner
112
Display
102
132
Secondary Wireless Device (typically Key Fob)
130
108
104
106
110
100

Fig. 1

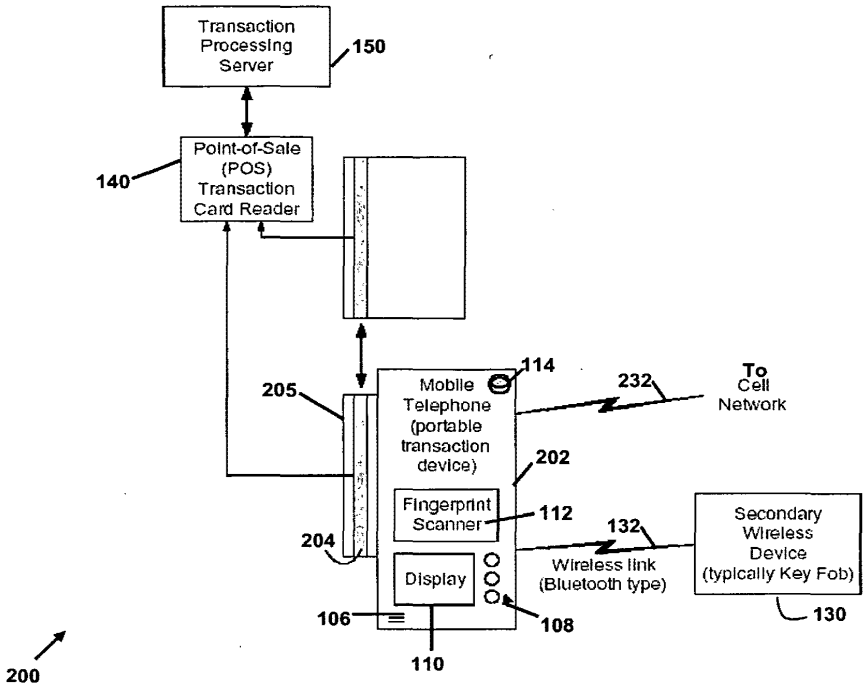

Transaction Processing Server
150
Point-of-Sale (POS) Transaction Card Reader
140
205
Mobile Telephone (portable transaction device)
114
232
To Cell Network
202
Fingerprint Scanner
112
132
Secondary Wireless Device (typically Key Fob)
204
Wireless link (Bluetooth type)
Display
106
108
130
110
200

Fig. 2

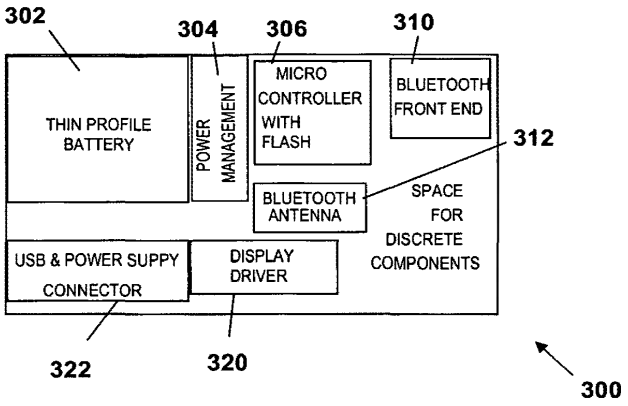

302
304
306
310
THIN PROFILE BATTERY
POWER MANAGEMENT
MICRO CONTROLLER WITH FLASH
BLUETOOTH FRONT END
312
BLUETOOTH ANTENNA
SPACE FOR DISCRETE COMPONENTS
USB & POWER SUPPY CONNECTOR
DISPLAY DRIVER
322
320
300

Fig. 3

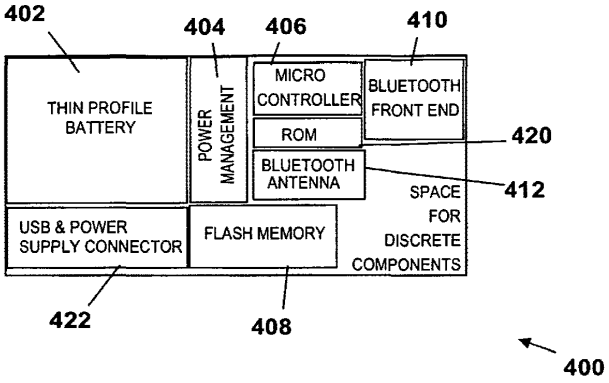

402
404
406
410
THIN PROFILE BATTERY
POWER MANAGEMENT
MICRO CONTROLLER
BLUETOOTH FRONT END
ROM
420
BLUETOOTH ANTENNA
412
SPACE FOR DISCRETE COMPONENTS
USB & POWER SUPPLY CONNECTOR
FLASH MEMORY
422
408
400

Fig. 4

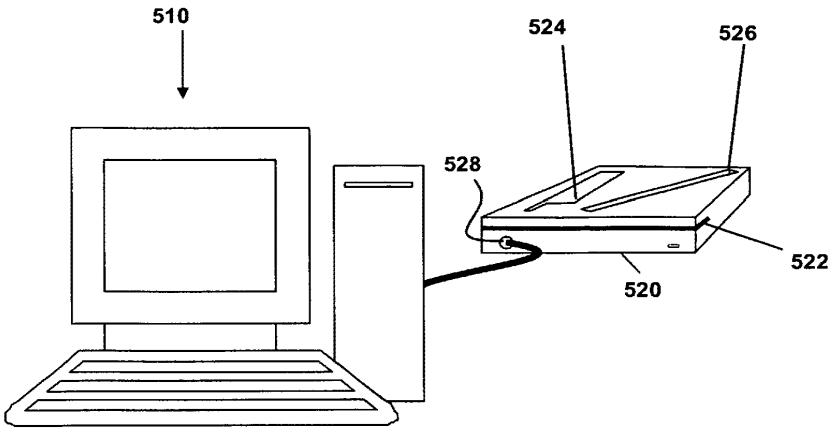


Fig. 5

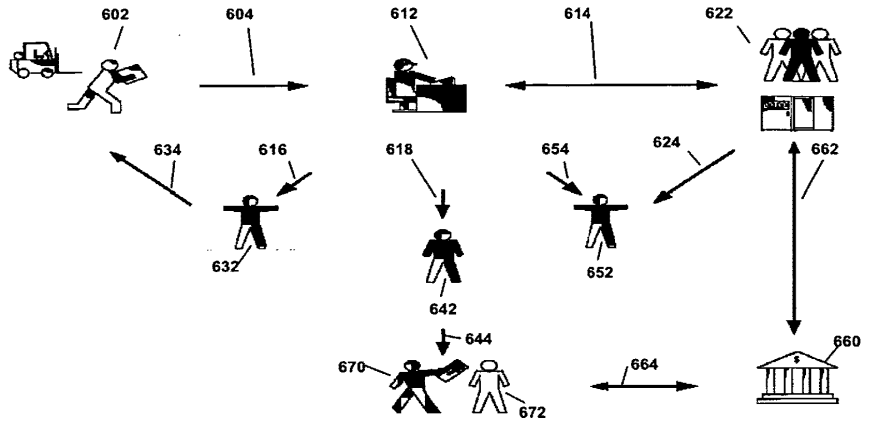

602
604
612
614
622
634
616
618
654
624
662
632
642
652
644
660
670
664
672

Fig. 6

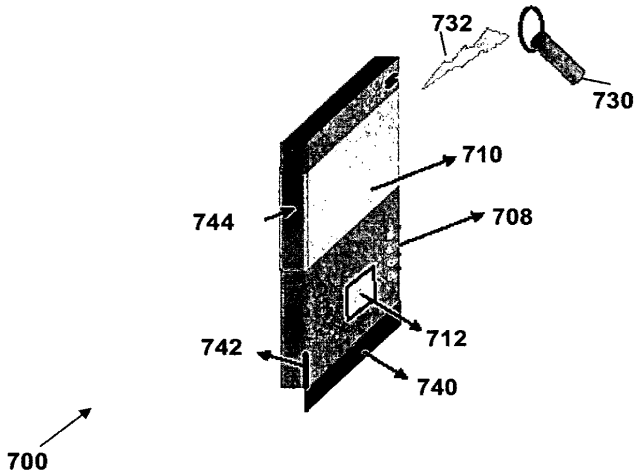


Fig. 7

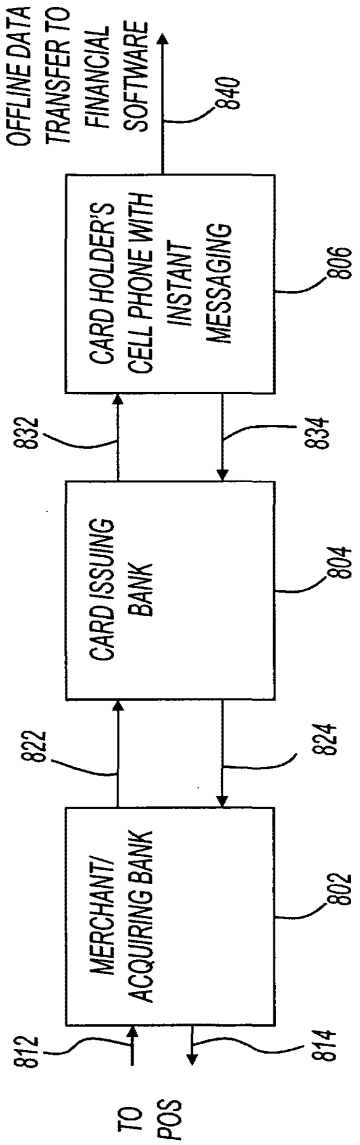

OFFLINE DATA TRANSFER TO FINANCIAL SOFTWARE
840
CARD HOLDER'S CELL PHONE WITH INSTANT MESSAGING
806
832
834
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 8

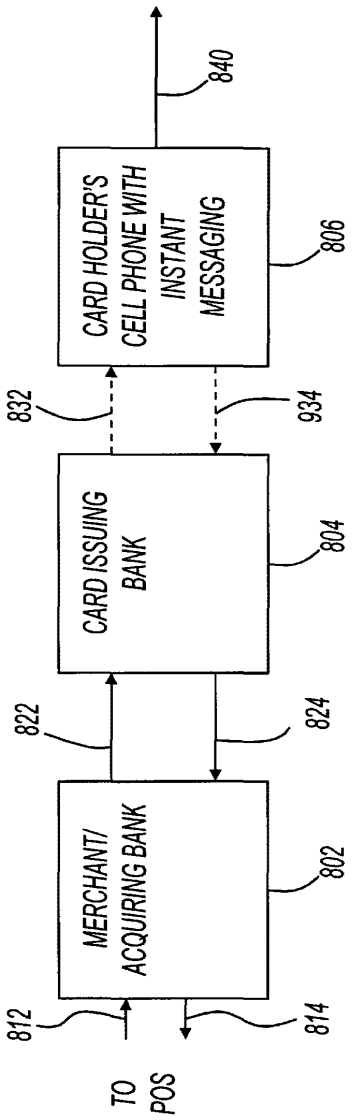

840
CARD HOLDER'S CELL PHONE WITH INSTANT MESSAGING
806
832
934
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 9

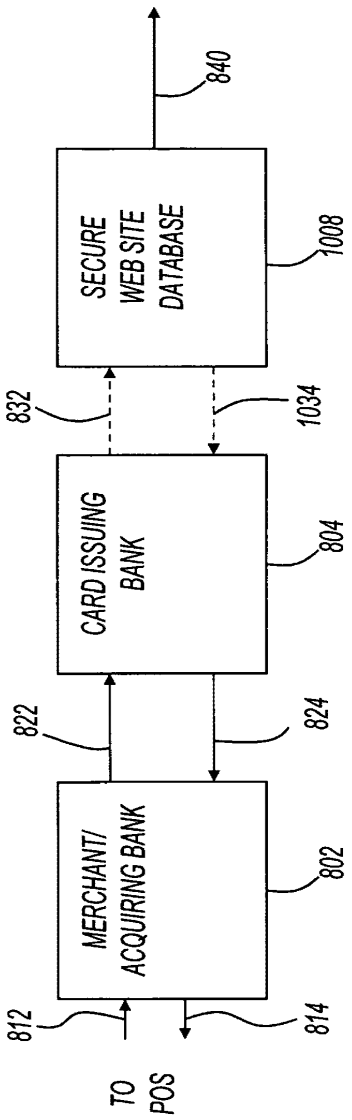

840
SECURE WEB SITE DATABASE
1008
832
1034
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 10

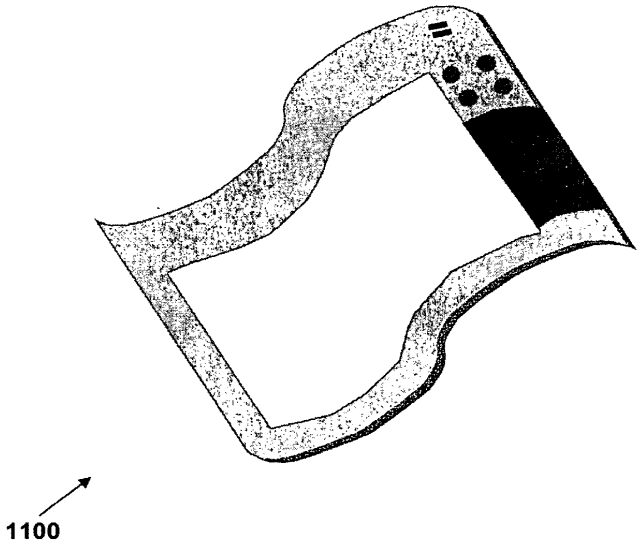


Fig. 11

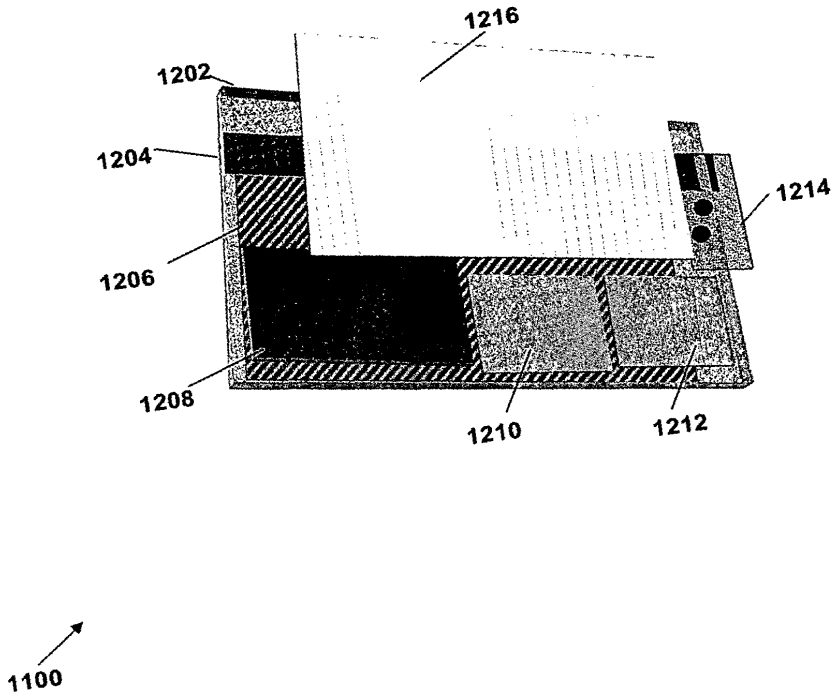


Fig. 12

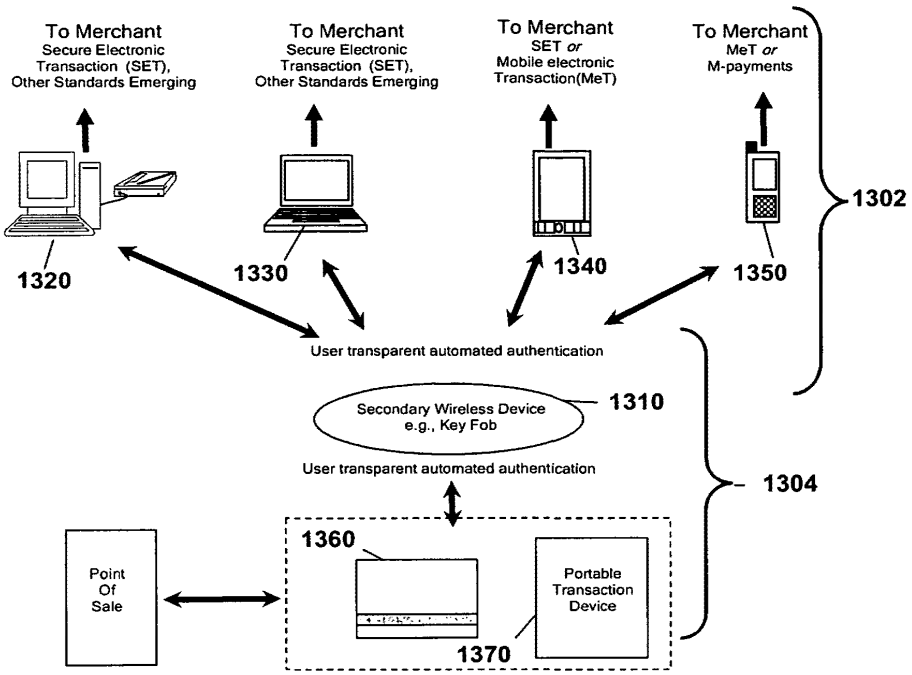

To Merchant
Secure Electronic Transaction (SET), Other Standards Emerging
To Merchant
Secure Electronic Transaction (SET), Other Standards Emerging
To Merchant
SET or Mobile electronic Transaction(MeT)
To Merchant
MeT or M-payments
1320
1330
1340
1350
1302
User transparent automated authentication
Secondary Wireless Device e.g., Key Fob
1310
User transparent automated authentication
1304
Point Of Sale
1360
Portable Transaction Device
1370

Fig. 13

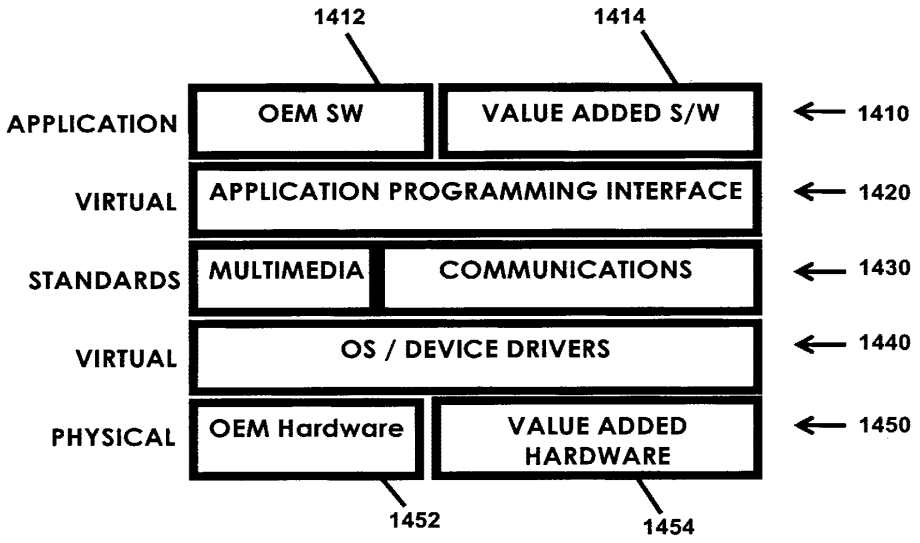

1412
1414
APPLICATION
OEM SW
VALUE ADDED S/W
1410
VIRTUAL
APPLICATION PROGRAMMING INTERFACE
1420
STANDARDS
MULTIMEDIA
COMMUNICATIONS
1430
VIRTUAL
OS / DEVICE DRIVERS
1440
PHYSICAL
OEM Hardware
VALUE ADDED HARDWARE
1450
1452
1454

Fig. 14

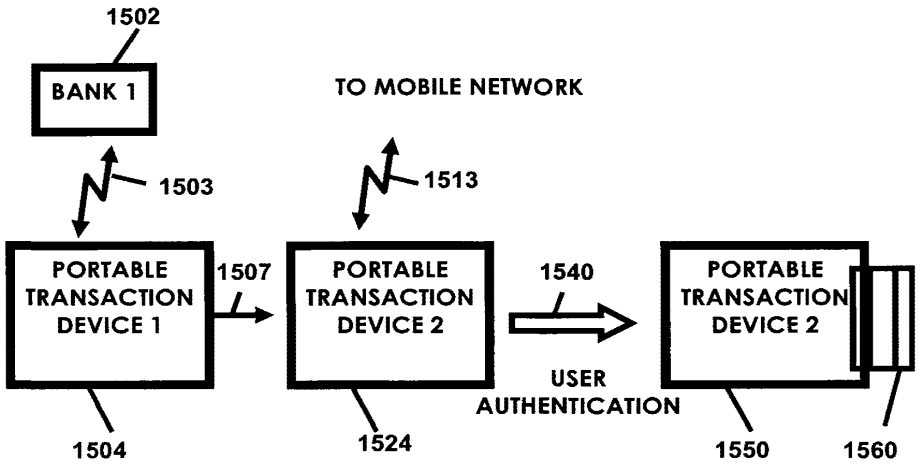

1502
BANK 1
TO MOBILE NETWORK
1503
1513
PORTABLE TRANSACTION DEVICE 1
1507
PORTABLE TRANSACTION DEVICE 2
1540
PORTABLE TRANSACTION DEVICE 2
USER AUTHENTICATION
1504
1524
1550
1560

Fig. 15

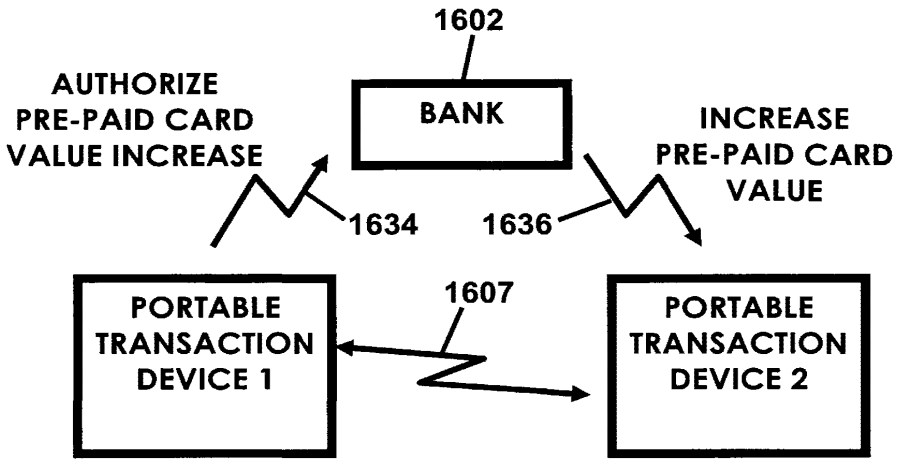

1602
BANK
AUTHORIZE
PRE-PAID CARD
VALUE INCREASE
INCREASE
PRE-PAID CARD
VALUE
1634
1636
1607
PORTABLE
TRANSACTION
DEVICE 1
PORTABLE
TRANSACTION
DEVICE 2

Fig. 16

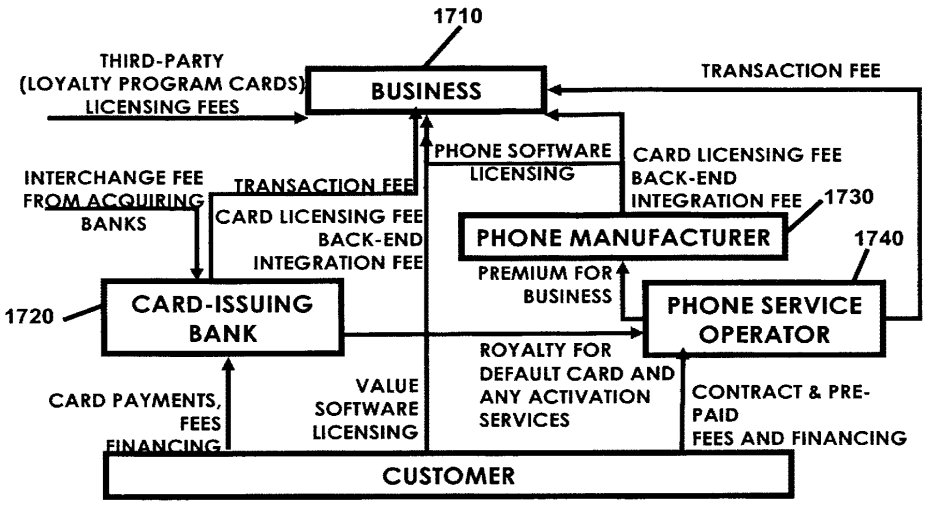

1710
THIRD-PARTY
(LOYALTY PROGRAM CARDS)
LICENSING FEES
BUSINESS
TRANSACTION FEE
PHONE SOFTWARE
LICENSING
CARD LICENSING FEE
BACK-END
INTEGRATION FEE
1730
INTERCHANGE FEE
FROM ACQUIRING
BANKS
TRANSACTION FEE
CARD LICENSING FEE
BACK-END
INTEGRATION FEE
PHONE MANUFACTURER
1740
PREMIUM FOR
BUSINESS
1720
CARD-ISSUING
BANK
PHONE SERVICE
OPERATOR
ROYALTY FOR
DEFAULT CARD AND
ANY ACTIVATION
SERVICES
CARD PAYMENTS,
FEES
FINANCING
VALUE
SOFTWARE
LICENSING
CONTRACT & PRE-
PAID
FEES AND FINANCING
CUSTOMER

Fig. 17

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9600808		2017-03-21	Gomez, Sr.; William et al.	
	2	9098846		2015-08-04	Gill; Sara et al.	
	3	7690580		2010-04-06	Shoemaker; Austin William	
	4	8499334		2013-07-30	Doughty; Ralph O. et al.	
	5	11100431		2021-08-24	Mullen; Jeffrey D. et al.	
	6	8255323		2012-08-28	Casey; Brandon J et al.	
	7	8423462		2013-04-16	Amacker; Matthew W. et al.	
	8	10460314		2019-10-29	Hird; Geoffrey R. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	9	9846866		2017-12-19	Royyuru; Vijay	
	10	6736322		2004-05-18	Gobburu; Venkata T. et al.	
	11	7967211		2011-06-28	Challa; Nagesh et al.	
	12	8628012		2014-01-14	Wallner; George	
	13	8690059		2014-04-08	Wallner; George	
	14	8814046		2014-08-26	Wallner; George	
	15	9361613		2016-06-07	Wallner; George	
	16	9454679		2016-09-27	Wallner; George	
	17	9652642		2017-05-16	Wallner; George	
	18	9864994		2018-01-09	Huang; Enyang et al.	
	19	10044510		2018-08-07	Kwon; Eun Young et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	20	10269005		2019-04-23	Lee; Woo-Sup et al.	
	21	10275761		2019-04-30	Lee; Woo-Sup et al.	
	22	10402811		2019-09-03	Park; Yong Man et al.	
	23	10423942		2019-09-24	Lee; Woosup et al.	
	24	10454728		2019-10-22	Huang; Enyang	
	25	10505277		2019-12-10	Lee; Woosup et al.	
	26	10516208		2019-12-24	Lee; Woo-Sup et al.	
	27	10540647		2020-01-21	Park; Yong Man et al.	
	28	10546291		2020-01-28	Kim; Eun Jik et al.	
	29	10592893		2020-03-17	Lee; Hee-Dong et al.	
	30	10680322		2020-06-09	Lee; Woosup et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	31	10699266		2020-06-30	Lee; Hee-Dong et al.	
	32	10713646		2020-07-14	Lee; Hee-Dong et al.	
	33	10796299		2020-10-06	Lee; Woo-Sup et al.	
	34	10803452		2020-10-13	Kim; Eun Jik et al.	
	35	10862718		2020-12-08	Huang; Enyang	
	36	10902390		2021-01-26	Lee; Woosup et al.	
	37	10929851		2021-02-23	Kang; Minkoo et al.	
	38	10990954		2021-04-27	Park; Yong Man et al.	
	39	10990959		2021-04-27	Lee; Woo-Sup et al.	
	40	10998620		2021-05-04	Lee; Woosup et al.	
	41	11004075		2021-05-11	Lee; Je Min et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	42	11017399		2021-05-25	Park; Yong Seok et al.	
	43	11042855		2021-06-22	Kim; Yu Hwan et al.	
	44	11061698		2021-07-13	Rhee; Injong et al.	
	45	11074581		2021-07-27	Kim; In Ho et al.	
	46	11107047		2021-08-31	Kim; Kibong et al.	
	47	11127010		2021-09-21	Cho; Boo Hyun et al.	
	48	11129018		2021-09-21	Kim; Ki Bong et al.	
	49	11227278		2022-01-18	Choi; Hoon et al.	
	50	11232339		2022-01-25	Lee; Woosup et al.	
	51	11321701		2022-05-03	Lee; Hee-Dong et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

EFS Web 2.1.18

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20130124410		2013-05-16	KAY; Christopher Erin et al.	
	2	20080319905		2008-12-25	CARLSON; Mark	
	3	20100185545		2010-07-22	Royyuru; Vijay K. et al.	
	4	20130262305		2013-10-03	Jones; Andrew R. et al.	
	5	20060089171		2006-04-27	Yoo; Kyung-Min et al.	
	6	20090048971		2009-02-19	Hathaway; Matthew et al.	
	7	20130232083		2013-09-05	SMITH; Theresa L. et al.	
	8	20080126260		2008-05-29	Cox; Mark A. et al.	
	9	20080222047		2008-09-11	Boalt; Adam	
	10	20080172317		2008-07-17	Deibert; Doug et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	11	20090159701		2009-06-25	Mullen; Jeffrey D. et al.	
	12	20120317035		2012-12-13	Royyuru; Vijay K. et al.	
	13	20130166441		2013-06-27	Kobylkin; Egor et al.	
	14	20120310760		2012-12-06	Phillips; Simon et al.	
	15	20080302876		2008-12-11	Mullen; Jeffrey D.	
	16	20110186626		2011-08-04	Manessis; Thomas et al.	
	17	20150147065		2015-05-28	Civelli; Jay Pierre et al.	
	18	20140143785		2014-05-22	Mistry; Pranav et al.	
	19	20050043997		2005-02-24	Sahota, Jagdeep Singh et al.	
	20	20150178724		2015-06-25	Ngo; Hao et al.	
	21	20160132881		2016-05-12	LEE; Yang-Soo et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	22	20160253652		2016-09-01	JE; Seong-Min et al.	
	23	20160253657		2016-09-01	SOHN; Se Chang et al.	
	24	20190026725		2019-01-24	PARK; Yong Seok et al.	
	25	20190172051		2019-06-06	LEE; Hui Jae et al.	
	26	20190173290		2019-06-06	HA; Min Cheol et al.	
	27	20210311752		2021-10-07	Rhee; Injong et al.	
	28	20220005046		2022-01-06	KIM; Inho et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2478712	GB		2011-09-21	JACKSON, DAVID		
	2	2485442	GB		2012-05-16	CUBIC CORP		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	3	00/62214	WO		2000-10-19	CLEARTOGO.COM et al.		
	4	01/57620	WO		2001-08-09	COMSENSE TECHNOLOGIES LTD et al.		
	5	2007145687	WO		2007-12-21	WEISS, KENNETH P.		
	6	2010043974	WO		2010-04-22	RICHARD, CHRISTIAN		
	7	2012154915	WO		2012-11-15	DYNAMICS INC et al.		
	8	2005119607	WO		2005-12-15	TYFONE INC et al.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 August 2001 (09.08.2001)

PCT

(10) International Publication Number
WO 01/57620 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US01/03882

(22) International Filing Date: 6 February 2001 (06.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/180,530	7 February 2000 (07.02.2000)	US
09/570,399	12 May 2000 (12.05.2000)	US

(71) Applicant *(for all designated States except US)*: **COMSENSE TECHNOLOGIES, LTD.** [IL/IL]; 3 Azrieli Center, 67023 Tel-Aviv (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ATSMON, Alon** [IL/IL]; 131/2 Ben Guryon Street, Yahud (IL). **ANTEBI, Amit** [IL/IL]; 64 Marganit Street, Ramat-Gan (IL). **LEV, Tsvi** [—/IL]; Lisin Street 11, 62997 Tel-Aviv (IL). **COHEN, Moshe** [IL/IL]; Chovevey 47, Tsivon, Tel-Aviv (IL). **SPEYER, Gavriel** [US/US]; 11358 Chalon Road, Los Angeles, CA 90049 (US). **SEGE, Alan** [US/US]; Apartment #5, 1518 Euclid Street, Santa Monica, CA 90404 (US). **ALTIMAN, Nathan** [IL/IL]; Hachashmonaym Street 39, Tel Aviv (IL). **ANATI, Rami** [IL/IL]; Haetrog Street 16, 38244 Kfar Brandes Haders (IL).

(74) Agents: **CHOU, Chien-Wei, (Chris)** et al.; Oppenheimer Wolff & Donnelly LLP, 1400 Page Mill Road, Palo Alto, CA 94304 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/57620 A2

(54) Title: PHYSICAL PRESENCE DIGITAL AUTHENTICATION SYSTEM (TRANSMISSION AND ROUTINE)

(57) Abstract: The interactive authentication system allows a consumer to interact with a base station, such as broadcast media (e.g., television and radio) or PC, to receive coupons, special sales offers, and other information with an electronic card. The electronic card can also be used to transmit a signal that can be received by the base station to perform a wide variety of tasks. These tasks can include launching an application, authenticating a user at a website, and completing a sales transaction at a website (e.g., by filling out a form automatically). The interaction between the base station and the electronic card is accomplished by using the conventional sound system in the base station so that a special reader hardware need not be installed to interact with the electronic card. The user is equipped with an electronic card that can receive and transmit data via sound waves. In the various embodiments, the sound waves can be audible or ultrasonic (which can be slightly audible to some groups of people).

IPR2025-01150
Apple EX1071 Page 624

PHYSICAL PRESENCE DIGITAL AUTHENTICATION SYSTEM (TRANSMISSION AND ROUTINE)

BACKGROUND OF THE INVENTION

RELATED APPLICATIONS

This application is a continuation-in-part of PCT application PCT/IL99/00525 titled "Card for Interaction with a Computer," filed October 4, 1999, which is a 35 USC 119(e) application based on U.S. provisional applications 60/115,231 filed January 8, 1999, 60/122,687 filed March 3, 1999, 60/143,220 filed July 9, 1999, 60/145,342 filed July 23, 1999, and 60/153,858 filed September 14, 1999. This application is also a continuation-in-part of U.S. provisional application 60/180,530 filed February 7, 2000. This application is also a continuation-in-part of PCT applications PCT/IL98/00450 filed September 16, 1998, PCT/IL99/00470 filed August 27, 1999, PCT/IL99/00506 filed September 16, 1999, and PCT/IL99/00521 filed October 1, 1999, all filed in the Israel receiving office by applicant ComSense Technologies Ltd. and designating the United States, and PCT/IB99/02110 filed November 16, 1999 with the International Bureau. All of these applications benefit from a priority date of July 6, 1998. Reference is further made to and priority claimed from U.S. Patent Application Serial No. 09/570,399, filed May 12, 2000, entitled, "Physical Presence Digital Authentication System." The disclosures of all of these applications are incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates generally to electronic cards or device for interaction with another electronic card or device such as a computer and, in particular, to electronic cards that use acoustic signals for such communications.

DESCRIPTION OF RELATED ART

The Internet, and the World Wide Web (WWW) in particular, has grown in popularity in recent years. In addition to news and information, merchants and consumers alike have come to view the web as a virtually unlimited source for conducting business, in the form of sales of products, services, and information. Nevertheless, many computer users are still somewhat leery of conducting sales transactions over the web especially because credit cards are involved, along with the associated fear of widespread and unchecked dissemination of the credit card numbers. These same users may also be leery of conducting non-Internet related sales transactions using credit cards. After all, anyone can swipe a credit card number and use it later for unauthorized purchases. Assurances from well-meaning web (and non-web) merchants do not alleviate these concerns because the user would have to carry a credit card in his person, which can be easily stolen or lost (and thus found by an unscrupulous thief). What is needed is a secure purchasing mechanism that provides users with the peace of mind to make a purchase on the web (or any other form of electronic purchase or other secure

information access) without the fear of having his credit card number stolen by an interloper at any point in the transaction.

Typically, systems that provide security to such online users do so to the detriment of user convenience. Because the Internet is a mass-medium, the success of online services depends largely on preserving user convenience. Without such conveniences, users would become decreasingly tolerant resulting in a loss of business and social opportunities for both web merchants and users alike.

Traditional microprocessor credit cards, also known as "smart cards" or "chip cards," provide security. But while smart cards that work in conjunction with dedicated smart card readers have become prevalent (i.e., bank cards in Europe), they are ill-suited for deployment as widespread Internet access control devices. Deploying smart card readers to users in their homes, for example, and educating users on their installation and use, are cumbersome, expensive, and inconvenient.

The prior art smart card systems largely were developed for a disconnected world; that is, maintaining a constant connection between the smart card and some other entity was considered expensive, inconvenient, and largely unnecessary. Indeed, the telephone charge itself was significant enough in cost to warrant minimizing such connection times.

In the prior art smart card, a small computer apparatus was embedded into a credit card plastic. At the very minimum, that apparatus would authenticate a user's secret personal identification number that was manually entered by the user on an in-store keypad every time a card is swiped. This authentication process did not require the intervention of any other authentication network. One aim of the present invention is to provide authentication that is as secure as ordinary bank cards, but in a manner where the functionality associated with the card is accessed via a public network such as the Internet. Ideally, such cards that send a one-way authentication signal can be used anywhere the Internet is available.

Computer network components that communicate using radio frequency (RF), infrared (IR), and wires are well known. In addition, some home appliances are controlled using acoustic remote control. However, these networks and appliances needed dedicated hardware components to realize the communication protocol; that is, specific and specialized hardware whose sole purpose was to effectuate the communication was installed therein. If such communication were not needed, the specific and specialized hardware would not be needed at all. Installing such hardware on an existing computer, TV, or radio may be expensive and/or problematic. Further, some electronic and/or computer embedded devices, for example cellular telephones may be "sealed" products, to which it is impossible to add internal components. What is needed is an electronic device that communicates with existing infrastructure equipment without the need to further equip these infrastructure equipment with any special hardware such as a smart card reader.

PCT publications WO96/10880, WO94/17498, WO93/21720 and WO93/11619, the disclosures of which are incorporated herein by reference describe an electronic device which transmits coded information to a microphone of a telephone using a DTMF-like encoding scheme. A WWW page addressed "http://www.encotone.com/html/tech_def.html", suggests using such a device to transmit audible DTMF-like tones to a personal computer using the computer's sound card.

IPR2025-01150
Apple EX1071 Page 626

Two way communications using audible DTMF-like tones, between an electronic card and a telephone communication system is described in US patent 5,583,933, the disclosure of which is incorporated herein by reference. Thus, what is needed is a communication mechanism that allows the electronic card to communicate with a transmitter/receiver without the need for dedicated or special hardware. Use of existing components would facilitate the wide acceptance of this communication mechanism, particularly in the purchasing context.

The present invention provides such a system and method and provides solutions to the problems described above.

SUMMARY OF THE INVENTION

One object of the present invention is to provide an electronic system which allows users to easily interact with a merchant (web-based or otherwise) or some other entity.

Still another object of the present invention is to provide a credit card-sized electronic card that can interact with various electronic devices (e.g., computer) to transmit information as well as receive information.

Another object of the present invention is to provide such an interactive electronic system without the use of dedicated hardware; that is, existing hardware will be utilized resulting in little, if any, changes for the television, radio, and stereo system manufacturers.

A further object of the present invention is to require little or no change to the content (as opposed to the infrastructure equipment itself) generated by the existing infrastructure. Sound is an essential element of human communications. Therefore, the present invention is relatively immune from changing communications standards, and is mass scalable. Strictly speaking, implementing those two-way methods requires little or no infrastructure change or modification of existing sound content. Two-way implementations under the current invention provide widespread utility in situations removed from a network. For example, some embodiments described here enable users to "bookmark" sound content, and later use those sound bookmarks to retrieve desired content from a network or other receiving apparatus.

In accordance with one embodiment of the present invention, the interactive electronic system includes an electronic card. In one embodiment, the electronic card is a one-way card that has a transducer, receiver circuitry and software (i.e., DSP and operating system) to process the incoming data. In another embodiment, the electronic card is a two-way card with both transmission and reception circuitry. In a further embodiment, the electronic card is a one-way transmit-only card. In any of these embodiments, the electronic card also includes a display, such as a liquid crystal display (LCD) panel. Memory (ROM, EEPROM, and RAM), a bus system, and power source are also provided. Electronic card contacts may also be provided to allow the electronic card to interface with standard electronic card readers. One or more physical buttons are also provided on the electronic card itself to perform any of a number of functions: (1) transmit data from the electronic card, (2) transmit data followed by a short period in receive mode, or (3) turn on the power to receive data for a short period.

Generally, the electronic card works with the existing infrastructure; that is, no special dedicated reader is necessary for the electronic card to communicate with existing base stations. For example, one such base

IPR2025-01150
Apple EX1071 Page 627

station is a personal computer. The personal computer typically has sound devices installed therein and the electronic card of the present invention can communicate with the computer using this already existing sound system. However, in another embodiment, special readers can be used to provide various functionality -- from reading the contents of the card (for those systems without a sound device) to adding bidirectional support for an otherwise one-way card to recharging the battery(ies) in the card. So, if the computer system is not equipped with a sound system, a special reader is provided to allow the electronic card to communicate with the computer system. As another example, the special reader can be an electronic device with a microphone to allow an otherwise transmit-only one-way electronic card to have two-way capability.

Without trading off security, the present invention provides substantially enhanced user convenience. For example, reader-free authentication devices are disclosed that enable "one-button" triggering of complex tasks such as connecting to a network and logging in securely to personalized network services. The software that enables the reader-free communication can be stored permanently on the base station for enhanced functionality. But for enhanced portability, methods are described for outsourcing that communications software to a remote computer, so that the devices can be used at a broader array of base stations.

The spectrum of applications enabled by the electronic card is broad. For the various embodiments of the present invention, the applications can be grouped into seven different categories – (1) One-way Infrastructure-to-Card, (2) One-way Card-to-Infrastructure, (3) Two-way, (4) Card-to-Card, (5) Client Software Applications, (6) Card Distribution, and (7) Dedicated Systems.

BRIEF DESCRIPTION OF THE FIGURES

The above objects and description of the present invention may be better understood with the aid of the following text and accompanying drawings.

FIG. 1 shows a system level diagram of the various components of the interactive media system in accordance with one embodiment of the present invention.

FIG. 2 shows a high level view of the one-way transmit-only electronic card.

FIGS. 3(A) and 3(B) show high level views of a two-way electronic card.

FIGS. 4(A) and 4(B) show high level views of the receiver portion of the electronic card.

FIG. 5(A) shows the data stream format for the card-to-PC communication direction. FIG. 5(B) shows the data stream format for the PC-to-card communication direction.

FIG. 6(A) shows a flow chart of the transmission routine of the electronic card in accordance with one embodiment of the present invention. FIG. 6(B) shows a detailed flowchart of the transmission portion of the transmission routine of FIG. 6(A).

FIG. 7 shows a low level view of the circuitry surrounding the microcontroller in accordance with one embodiment of the present invention.

FIG. 8 shows a low level view of the voltage doubler circuitry in accordance with one embodiment of the present invention.

FIG. 9 shows a low level view of the power and switching circuitry in accordance with one embodiment of the present invention.

IPR2025-01150
Apple EX1071 Page 628

FIG. 10 shows a low level view of the electronic card connector.

FIG. 11 shows the key components of the client computer system, including the speaker/microphone, sound card driver, special client remote access software, and the web browser in accordance with one embodiment of the present invention. Note that the browser is optional and that the present invention is operational with just the special client remote access software.

FIG. 12 shows a high level block diagram of the electronic card's reception software in accordance with one embodiment of the present invention.

FIG. 13 shows a flow chart of the reception software in a personal computer.

FIG. 14 shows a signal decoder in accordance with one embodiment of the present invention.

FIG. 15 shows a signal detector in accordance with one embodiment of the present invention.

FIG. 16 shows an exemplary graph of the received signal and the sampled points therein to illustrate the moving average concept in accordance with one embodiment of the present invention.

FIG. 17 shows an alternative embodiment of the one-way Transmit card. This circuit can also be applied to two-way cards for the transmit portion.

FIG. 18 shows a detailed analog front end portion of the receiver circuitry for the electronic card in accordance with one embodiment of the present invention.

FIG. 19 shows a detailed digital core portion of the two-way electronic card in accordance with one embodiment of the present invention.

FIG. 20 shows a block diagram of the card architecture which implements analog recording in accordance with one embodiment of the present invention.

FIG. 21 shows a server architecture which implements the pattern recognition search engine and various databases including an account database, coupon database, incentive points database, merchandise database, and soundtrack database in accordance with one embodiment of the present invention.

FIG. 22 shows a high level block diagram of the pattern recognition search functionality in the pattern recognition search engine in accordance with one embodiment of the present invention.

FIG. 23 shows a high level diagram of a cable TV infrastructure and the manner in which the merchant data is mixed with normal programming.

FIG. 24 shows a high level diagram of a broadcast TV/radio infrastructure and the manner in which the merchant data is mixed with normal programming.

FIGS. 25(A), 25(B), and 25(C) show three embodiments of the component layouts for the electronic card.

FIG. 26 shows the layers of materials that make up the electronic card in accordance with one embodiment of the present invention.

FIGS. 27(A), 27(B), and 27(C) illustrate the transducer construction in accordance with three embodiments of the present invention.

FIG. 28 shows a state diagram of the multi-mode switch software in the electronic card.

FIG. 29 shows a system diagram for the E-Wallet system in accordance with one embodiment of the

IPR2025-01150
Apple EX1071 Page 629

present invention.

FIG. 30 shows a flow chart of the operation of the E-Wallet system in accordance with one embodiment of the present invention.

FIG. 31 shows a high level block diagram of the various entities that involved in credit card transactions.

FIG. 32 shows a flow chart of the on-line authentication operation in accordance with one embodiment of the present invention.

FIG. 33 shows the sequence of steps taken by the electronic card, PC, and the web merchant when the customer is attempting to check the trustworthiness of the web merchant via a challenge-response technique in accordance with one embodiment of the present invention.

FIG. 34 shows the sequence of steps taken by the electronic card, PC, and the web merchant when the web merchant is attempting to check the trustworthiness of the electronic card (and hence user) via a challenge-response technique in accordance with one embodiment of the present invention.

FIG. 35 shows the sequence of steps taken by the electronic card, PC, and the web merchant when both the web merchant and the customer are attempting to check each other's respective trustworthiness via a challenge-response technique in accordance with one embodiment of the present invention.

FIG. 36 shows a crypto service provider (CSP) scheme, the entities, and the sequence of steps taken by these entities in accordance with one embodiment of the present invention.

FIG. 37 shows one embodiment of the electronic card decoder when RF signals are used for the PC-to-electronic card communication path.

FIG. 38 shows another embodiment of the electronic card decoder when RF signals are used for the PC-to-electronic card communication path.

FIG. 39 shows another embodiment of the electronic card decoder when magnetic signals are used for the PC-to-electronic card communication path.

FIG. 40 shows another embodiment of the present invention where a hardware PLL technique is used in the electronic card for processing acoustic signals.

FIG. 41 shows another embodiment of the present invention where a software PLL/FLL technique is used in the electronic card for processing acoustic signals.

FIG. 42 shows another embodiment of the present invention where a mixer is used for baseband processing in the electronic card for processing acoustic signals.

FIG. 43 shows an embodiment of the present invention where a special driver is placed between the Windows Mulimedia interface and the default sound card driver so that multiple applications can run concurrently in the computer system.

FIG. 44 shows an alternative embodiment from the system described an shown in FIG. 43 where a special driver is placed between the Windows Mulimedia interface and the default sound card driver so that multiple applications can run concurrently in the computer system.

FIG. 45 shows a diagram of a secure purchasing mechanism in accordance with one embodiment of the

IPR2025-01150
Apple EX1071 Page 630

present invention where incentive points/mileage instead of cash can be used to purchase products.

FIG. 46 shows a high level abstracted view of some of the many applications that are enabled by the present invention.

FIG. 47 shows a high level view of another application where benefits are achieved using the versatile electronic card with the conventional magnetic stripe in a system that utilizes a central account database.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

At a high level, this patent specification provides detailed information on the system, the electronic card itself, the base station (e.g., personal computer), and various applications (which may involve various web servers). In particular, the patent specification is organized as follows:

1.0 SYSTEM SUMMARY
2.0 FREQUENCY RANGE
3.0 ELECTRONIC CARD
- 3.1 TWO-WAY CARD
- 3.2 CARD TRANSMISSION HARDWARE
- 3.3 CARD TRANSMISSION SOFTWARE
  - 3.3.1 DATA STREAM
  - 3.3.2 TRANSMISSION ROUTINE
  - 3.3.3 MULTI-MODE SWITCH
- 3.4 CARD RECEPTION HARDWARE
- 3.5 CARD RECEPTION SOFTWARE
- 3.6 CARD MECHANICAL CONSTRUCTION
  - 3.6.1 SHEETS-LEVEL CARD FABRICATION
  - 3.6.2 COMPONENT LAYOUT
  - 3.6.3 CARD LAYERS
  - 3.6.4 TRANSDUCER CONSTRUCTION

4.0 BASE STATION
- 4.1 CLIENT COMPUTER SYSTEM
- 4.2 INSTALLATION AND INITIALIZATION
- 4.3 BASE STATION TRANSMISSION SOFTWARE
- 4.4 BASE STATION RECEPTION SOFTWARE
- 4.5 CONCURRENT OPERATION OF MULTIPLE RECORDING SOFTWARE
- 4.6 SERVER-BASED PROCESSING

5.0 APPLICATIONS
- 5.1 BROADCAST MEDIA
  - 5.1.1 BROADCAST MEDIA INFRASTRUCTURE
  - 5.1.2 BROADCAST MEDIA COUPON TRANSMISSION
  - 5.1.3 BROADCAST MEDIA COUPON REDEMPTION

IPR2025-01150
Apple EX1071 Page 631

5.1.3.1 Password-based Internet Manual Redemption
5.1.3.2 Internet Automatic Redemption
5.1.3.3 Store Redemption
5.1.4 INTERACTIVE TV AUCTION
5.1.5 CONTENT RECORDING FOR SEARCH/REDIRECTION
5.1.5.1 Electronic card Hardware
5.1.5.2 Server Architecture
5.1.5.3 System Operation
5.1.6 BOOKMARKS FOR BROADCAST MEDIA
5.2 SMART E-WALLET SYSTEM
5.2.1 INSTALLATION
5.2.2 OPERATION
5.2.3 SECURITY
5.3 WEB TRANSACTIONS AND AUTHENTICATION
5.3.1 CREDIT CARD INFRASTRUCTURE
5.3.2 ON-LINE AUTHENTICATION
5.3.3 OFF-LINE AUTHENTICATION
5.3.4 PASSWORD GENERATOR
5.3.5 CHALLENGE-RESPONSE
5.3.6 CRYPTO SERVICE PROVIDER (CSP)
5.4 PLUG-INS
5.4.1 PLUG-IN SUBSERVIENT
5.4.2 PLUG-IN DOMINANT
5.5 POINTS/CASH PURCHASING MECHANISM
5.6 BAR CODE READER
5.7 CARD-TO-CARD INFORMATION EXCHANGE
5.8 WEBPAGE-DEPENDENT ACTIVATION
5.9 ELECTRONIC LOYALTY SYSTEM
5.10 ADDITIONAL SYNERGIES WITH VOICE
6.0 NON-ACOUSTIC EMBODIMENTS
6.1 RADIO FREQUENCY (RF)
6.2 MAGNETIC FIELD

1.0 SYSTEM SUMMARY

One embodiment of the present invention provides for a system that allows a user to interact with merchants and other entities via an electronic device, such as television, radio, or personal computer, to conduct transactions of various kinds (e.g., consumer purchase of products/services, security check). The transactions can involve transmitting information of various kinds (e.g., membership information, personal information) and

IPR2025-01150
Apple EX1071 Page 632

receiving information of various kinds (e.g., account statements, coupons, special sales offers, other sales information). The user is equipped with an electronic card that can receive and transmit data via sound waves. The interaction is accomplished by using sound from the electronic device's speakers when receiving data and emitting sound from the electronic card to the electronic device's microphone when transmitting data. In the various embodiments, the sound waves can be audible or ultrasonic (which can be slightly audible to some groups of people).

Note that in addition to the electronic card, the client software, and the various applications, the communications protocol itself also contains various unique aspects. The communications scheme can be between cards and between the card and the base station. The direction of the transmission can be one-way or two-way.

FIG. 1 provides a high level view of the interactive system in accordance with one embodiment of the present invention. At the core of the system is an electronic card 10 (or electronic card 10). As discussed in greater detail below, the electronic card 10 is a card that complies with standard credit card form factor requirements while containing some electronic circuitry and transducer(s) for processing data, storing data, transmitting data, and receiving data. In some embodiments, the electronic card 10 also contains an LCD display. The transmitted and received data are in the form of sound waves that are either audible or ultrasonic.

Although this embodiment requires the electronic card to adhere to ISO-compliant credit card form factor specifications, other embodiments do not require such compliance. Indeed, other embodiments involve large electronic devices that contain the logic and functionality described herein in this patent specification. Although a major advantage of the electronic card in accordance with one embodiment is its credit card form factor size, the spirit and scope of this patent application extends to any electronic device regardless of physical form factor.

In one embodiment, as illustrated in the general diagram of FIG. 1, the electronic card 10 can be used by the user to interact with almost any infrastructure electronic device, so long as the infrastructure electronic device is equipped with hardware that is not necessarily dedicated to interact with the electronic card 10 and supporting software. Thus, the electronic card 10 can transmit data to a radio 11 via sound waves 19a, television 12 via sound waves 19b, a computer 14 via sound waves 19c, and some electronic device in conventional store 13 via sound waves 19d. Of course, each of these infrastructure electronic devices must have corresponding microphones to receive the sound waves (e.g., microphone 14c for computer 14). In the case of the radio 11 and television 12, the electronic card 10 can emit infrared, RF, or magnetic signals, instead of sound waves if these devices do not contain a microphone. Also, the electronic card 10 is equipped with transmission circuitry, microprocessor circuitry, memory, and a transducer to generate the sound waves.

Conversely, the infrastructure devices can deliver data to the electronic card 10. Thus, the electronic card 10 can receive data from radio 11 via sound waves 19w, television 12 via sound waves 19x, computer 14 via sound waves 19y, and some electronic device in conventional store 13 via sound waves 19z. Each of these infrastructure electronic devices must have corresponding speakers to emit the sound waves (e.g., speakers 14a

IPR2025-01150
Apple EX1071 Page 633

and 14b for computer 14). The electronic card 10 is equipped with reception circuitry, microprocessor circuitry, memory, and a microphone to receive and process the sound waves.

When the electronic card 10 is used with a personal computer 14, other commercial opportunities open up. For example, the user could use the electronic card to interact with a web merchant 17 and a web portal 18 via the Internet 16. Of course, the average consumer would need access to the Internet via some Internet Service Provider (ISP) 15. The electronic card 10 could be used to facilitate the sales transaction between the web merchant 17 and the user. Furthermore, the electronic card 10 could provide a greater sense of security to various web players (i.e., web merchants, credit card issuers, acquiring banks, consumers themselves). These and other applications of the electronic card-based interactive system are detailed below.

The following is a sampling of the system specifications.

System Feature	Specification Description
Card transmission speed	Card-to-PC: 200 bps
EDAC mechanisms	Bytes transmitted with parity, with on-the-fly error correction and detection
Card lifespan	Up to 10,000 key presses
Card dimensions	0.76 mm x 85 mm x 54 mm
Robustness	Sustains bending and torsion; highly resistant to electromagnetic radiation
Range	1-2 feet from microphone
PC Operating System	Windows 95/98
System Requirements	Pentium 100 MHz; 32 MB RAM; 1MB free space on hard disk; sound card
Browsers	Internet Explorer 4.0 and higher; Netscape Communicator 4.0 and higher; AOL

The transmission technique is frequency shift keying (FSK), as described in more detail below. In other embodiments, the transmission technique is n-ary phase shift keying (PSK). However, in contrast to the FSK technique where magnitude was used in the DFT banks to select the two relevant frequency channels, nPSK relies on selecting a particular channel for detection and then determine phase drift and offset by examining the I and Q channels.

The spectrum of applications enabled by the electronic card is broad. From a complexity point of view, the applications may include, at one extreme, the simple task of providing information to a web merchant or store (i.e., "I am present.") to a medium complexity task of automating the process of filling out a form and, at the other extreme, performing a complicated series of tasks involving security, context sensitivity actions, and multiple modes. For the various embodiments of the present invention, the applications can be grouped into seven different categories – (1) One-way Infrastructure-to-Card, (2) One-way Card-to-Infrastructure, (3) Two-way, (4) Card-to-Card, (5) Client Software Applications, (6) Card Distribution, and (7) Dedicated Systems. Each of these categories of applications will be described in greater detail below.

2.0 FREQUENCY RANGE

In one embodiment of the present invention, the interactive system uses acoustic waves. Preferably, acoustic signals in the ultrasonic frequency band are used. In one embodiment of the present invention, acoustic waves in the ultrasound frequency range will be used. Ultrasound is in the 15-28 kHz frequency range,

IPR2025-01150
Apple EX1071 Page 634

and typically higher. Of course, the reader should realize that ultrasound has no fixed upper limit. In the preferred embodiment, the frequency range of 17-20 KHz has been selected for the ultrasonic acoustic signals. In particular, one embodiment uses 17.5 kHz for one FSK frequency and 18.5 kHz for the other FSK frequency. These numbers were selected because half (for Nyquist sampling) of the 44.1 KHz recording rate for CD-quality audio is 22.05 KHz. The upper limit of 20 KHz was selected because in most sound systems, sound above 20 KHz is filtered out sharply. Thus, this embodiment uses sounds in the frequency range that can be supported by the current sound systems that are installed in today's computer systems. In another embodiment, the sound waves can go down to 10 kHz while still retaining the benefits of the ultrasonic frequency signals.

Ultrasound has certain benefits over the audible frequency range. First, most people cannot hear ultrasound and when they do hear it, it is not noticeably loud. Normally, young people can hear in sounds in the frequency range of 0-20 kHz, adults can hear in the 0-18 kHz range, and the older senior citizens can hear in the 0-16 kHz range. Some animals, such as dogs, can hear sounds at much higher frequencies.

Second, ultrasound is less subject to interference. Most ambient noise is audible and audible sounds are omnidirectional. Thus, using audible frequencies would subject the electronic card to all sorts of unwanted interference. As the sound is at a higher frequency range (such as ultrasound), it also becomes more directional. In addition to the directionality, the higher frequency sounds travel shorter distances. Thus, ultrasonic noise sources, if any, need to be generally pointing directly at the microphone and be reasonably close to the ultrasonic electronic card to cause any interference.

Third, the bandwidth is greater at the higher frequencies. Therefore, more information can be transmitted per unit of time. This is important because the data transfer should not occur over an extended period of time.

Fourth, to implement ultrasound, the transducers are smaller than conventional sound transducers. Because the electronic card will comply with the major credit card standards, this small size is particularly important. The smaller size transducers will take up less space and if placed strategically in the card, the user will be able to bend the electronic card without any damage to the components therein.

Fifth, the ultrasonic electronic card can be used with existing non-dedicated base station infrastructure equipment. For example, the sound device (e.g., "Sound Blaster" sound card) in a personal computer supports the ultrasound frequency band. Accordingly, with no hardware modifications, additions, or subtractions of any kind, the electronic card of the present invention can interface with the existing base station infrastructure.

When ultrasound is used, the electronic card has a range of approximately 1-3 feet. Other frequency ranges, such as the audible frequency range, provide greater distances. Thus, the particular acoustics that the electronic card uses determines the transmission distance. Typically, the user (and hence the card) would be fairly close to a microphone to pick up the acoustic signals transmitted by the electronic card. This also applies to the reception of the acoustic signals by the electronic card.

Of course, the selection of the frequency range for the acoustic signal depends on the application. If the base station that communicates with the acoustic electronic card is a conventional telephone, for example, audible acoustic signals should be used since filters in the telephone network remove signals in the ultrasound

IPR2025-01150
Apple EX1071 Page 635

range. Thus, in one embodiment, the electronic card emits acoustic signals in the non-ultrasonic audible frequency range so that it can communicate with band-limited sound systems. In another embodiment, the particular audible frequencies that are used are based on the DTMF system.

3.0 ELECTRONIC CARD

The electronic card 10 (see FIG. 1) will now be discussed. Initially, a two-way card will be described, followed by individual transmission and reception components. Note that some embodiments require a two-way card, while other embodiments require a transmit-only one-way card or a receive-only one-way card. In all of these embodiments, at least one switch that is physically activatable by the user is provided on the card. In some embodiments, multiple switches are provided to provide additional functionality.

3.1 TWO-WAY CARD

A high level block diagram of a two-way electronic card will now be described with respect to FIGS. 3(A) and 3(B). For one-way transmit-only cards, the transmission portion of the two-way card is used. For one-way receive-only cards, the receiver portion of the two-card is used.

FIG. 3(A) shows one embodiment where a receive transducer and a separate transmit transducer are provided. In FIG. 3(A), memory unit 30 is coupled to processing unit 31, which is in turn coupled to reception unit 32 and transmission unit 33. The received signals in the reception unit 32 are provided to the processing unit 31. Also, the processing unit 31 determines what data to transmit with the transmission unit 33. The reception unit 32 is coupled to the receive transducer 36, while the transmission unit 33 is coupled to the transmit transducer 37. A power and switching unit that is identical to unit 24 of FIG. 2 is also provided but not shown in FIG. 3(A).

In contrast, FIG. 3(B) shows another embodiment where a single transducer is provided for both reception and transmission. Again, the memory unit 30 is coupled to the processing unit 31. The processing unit 31 is coupled to an input/output unit 35. The input/output unit 35 includes a reception unit 32, a transmission unit 33, and a switchable transducer 34. The switchable transducer 34 is under the control of the processing unit 31 since the processing unit 31 knows when the electronic card should transmit and receive. Any received signals detected by the switchable transducer 34 are provided to the reception unit 32, while any signals that need to be transmitted are provided by the transmission unit 33 to the switchable transducer 34.

Further details of the card's transmission and reception hardware units will be provided below. Also, the software in the microcontroller 31 includes:

(1) transmission software
(2) reception software
(3) encryption software
(4) memory retrieval and storage

These four parts of the card's software will be discussed further below.

3.2 CARD TRANSMISSION HARDWARE

The transmission hardware will now be discussed. In particular, the transmission hardware will be discussed in the context of a one-way transmit-only electronic card 10 as shown in FIG. 2. The electronic card

IPR2025-01150
Apple EX1071 Page 636

10 is essentially a portable device with a processing unit 21, memory unit 22, output unit 23, and power and switching unit 24. The processing unit 21 provides the computation and control necessary for operating system functionality, cryptography, communication, memory management, and code updates. This unit comprises a dedicated chip microcontroller, DSP functionality, a smartcard chip, and a bus system. Preferably, the processing unit used has sufficient power (a few MIPS), and includes some on-chip or off-chip memory for storing and/or generating a cryptographic signature. A Microchip 12C508, 12C672 or higher processing unit is preferred. In one embodiment, a Microchip PIC16F84 is used which uses an on-chip EEPROM.

Preferably, the microcontroller should satisfy the following requirements:

(1) working voltage of 2.2 V depending on the battery. Although 2.2 V is adequate for standard batteries, 2.0 V is preferable. A voltage of 3.0 V also works.
(2) low supply current of approximately 2 mA
(3) MIPS: at least 0.5
(4) Program memory of 2KBytes, although 2 K instructions is preferable
(5) EEPROM of 8 Bytes
(6) Data memory of 100 Bytes (although the Microchip PIC16F84 has 68 Bytes)
(7) Timer is desirable
(8) RC input for clock source in one embodiment, but an external frequency source can be used for some ASIC implementations
(9) Die
(10) Temperature tolerance of 0-50 degrees Celsius for working conditions and –10 to 70 degrees Celsius for storage
(11) Watchdog functionality to add reliability to the microcontroller (resets the microcontroller if it starts to malfunction)
(12) I/O: at least 4 I/O pins are needed with 2 spares.
(13) Sleep mode for reducing current after card operation has been executed
(14) Low cost

The memory unit 22 is used to store data relevant for the card user. The memory unit 22 comprises read only memory (ROM), random access memory (which may also be incorporated in the processing unit 21), and an EEPROM to permanently store externally received data. Specifically, the memory unit can contain data for security encryption, personal details, electronic coupons, and upgradeable software. In one embodiment, the memory unit 22 is a non-volatile memory. The digital ID stored therein is 8 bits long in one embodiment and after encryption, it becomes 32 bits (for main digital ID bits, checksum, CRC, header, etc.).

The output unit 23 physically creates the transmitted signal. It is preferably made from a metal plate with a piezo material (e.g., piezo ceramic material with a small thin metal plate) on it. Being very thin, these transducers produce the required intensity at the ultrasonic frequencies. It also comprises driver circuitry and amplification circuitry connected between it and the processing unit 21.

IPR2025-01150
Apple EX1071 Page 637

The power and switching unit 24 comprises a very thin battery with enough capacity and drain ability, or with recharge capabilities. A switch is provided for turning the card on or off and for changing states (or modes) of the card. Aside from a mechanical switch, the processing unit can also automatically turn the power and switching unit 24 off. The card may be programmed so that the system wakes up at the occurrence of certain wake-up events. Power supply amplification and filtration are also provided.

Referring now to FIGS. 7-10, a detailed low level description of the one-way card will now be provided. FIG. 7 shows the Microchip PIC16F84 microcontroller and surrounding circuitry. The processor is a PIC 16F84, which is fast and contains on-chip data EEPROM. The PIC 16F84 also provides for three options to provide the clock source – (1) external crystal oscillator, (2) external oscillator circuit, and (3) external RC circuit. Because of the size constraint of the electronic card, a crystal clock source could not be used. Also, an external oscillator circuit, while feasible, contains too many components. Accordingly, an RC circuit (R2 and C2) is provided at the OSC1/CLKIN input. With the particular values shown in FIG. 7, the clock frequency selected is 4MHz. Reset is provided at the MCLR input.

At the VDD input, the microcontroller is coupled to Vdd3, capacitor C1, and VDD-. The power supply, which is discussed later in conjunction with FIG. 9, provides 2-3 volts. The microcontroller however needs 4-6 volts the transmission circuitry and also because the microcontroller can operate faster with higher input voltage. A voltage doubler circuit of FIG. 8 provides the doubling needed to effectively operate the microcontroller.

The RA0 pin is used as an output pin. The voltage provided at this pin mirrors the voltage doubled input VDD- and is also provided to the power and switch unit which is described below in FIG. 9. Essentially, the RA0 prevents the operation of the electronic card during transient states (turning on or turning off).

The output at RB1 is coupled to buzzer LS1, which generates the acoustic signal. In one embodiment, this buzzer is an FT12-T.

Pins RB5-RB7 are used for programming and testing the microcontroller. In addition, the electronic card connector of FIG. 10 is used for programming and debugging.

The voltage doubler circuit will now be described with respect to FIG. 8. The voltage doubler is a high efficiency device. A charge pump scheme is used because of the big physical size of the needed inductors in other schemes. However, in other embodiments, the use of such inductors is feasible in the credit card-sized electronic card 10 of FIG. 1. The Maxim voltage converter MAX861 takes as its input at Vdd and outputs a doubled voltage VDD- at pin Out. The VDD- is provided to the VDD input of the microcontroller in FIG. 7. The additional circuitry of C4, C5, and Motorola diode MBR0503T1 provides protection to the chip from overvoltage at the input Vdd.

The power and switching circuit will now be described with respect to FIG. 9. The power source is a Varta LPF25 battery which is small, has low current drain, and provides just enough voltage for the rest of the card's circuits. In one embodiment, it outputs 2-3 volts.

A switch SW1 is provided. The switch is used by the user to enable the transmission of data in the electronic card. The user should keep the switch pressed for as long as the transmission requires, which is

IPR2025-01150
Apple EX1071 Page 638

usually a short period of time since the data transmission is relatively fast at 200 bits per second. However, sufficient protection circuitry is provided so that if the user releases the switch prematurely, the proper operational voltage is delivered to the processor so that the data can be transmitted without fail. When the switch SW1 is pressed, transistors Q1 (Fairchild Semiconductor MMBT2907A) and Q2 (Fairchild Semiconductor MMBT2222A) provides a smart switch function. After turning on, these transistors Q1 and Q2 are turned off by the Microchip processor of FIG. 7. Transistor Q1 passes the voltage from the battery to the voltage doubler circuit of FIG. 8 as voltage Vdd1. The capacitors C9 and C10 allow for the power to ramp up smoothly and to hold the Vdd1 voltage for some time period. The transistor Q2 receives a digital command from the processor and shifts voltage levels for transistor Q1 as needed. The discrete bipolar transistors are used because of their low leakage current, which can be as low as a few nAmps.

The combination of Q1, Q2, micro power voltage reference D2 (National Semiconductor LM385-2.5/SO), and their resistors are provided to confirm the validity of the signal. This circuit ensures that any signal above 4 volts from the processor via RA0 will deliver power to the power and switching circuit for its effective operation. However, any signal below 3 volts will be ignored so that latch-up of the circuit will be prevented during transient states (turning off or turning on). This circuit consumes less than 10 nA in the off state. An alternative circuitry for the LM385-2.5 can be a reset supervisor which will reset the microcontroller when the voltage drops below the allowed threshold. Such IC's can be the equivalent of MAX821 or MAX6326.

An electronic card connector J1 is also provided as shown in FIG. 10. The electronic card connector is used to program, test, and debug the electronic card. In alternative embodiments, however, the electronic card connector is not provided. Instead, the electronic card is programmed by the manufacturer of the microcontroller. In another embodiment, the card is programmed using the electronic card connector and then the circuits including the electronic card connector are laminated over with suitable material, including printed PVC.

An alternative embodiment of the card transmission hardware provides for two added benefits – lower power consumption and greater power output. With the lower power consumption, battery life is extended. With the greater power output, reliability is increased with lower bit error rate. A high level block diagram of this alternative embodiment is shown in FIG. 17.

In FIG. 17, a battery 190 is provided. This battery supplies 2-3 volts nominal voltage. In one embodiment, the battery is a single Varta LPF-25 battery that provides 2.7V nominal at 1 mA discharge (25 mAH).

A mechanical switch 191 provides the circuit connection when it is closed. In one embodiment, the mechanical switch is a dome switch. A silicon switch 192 is also provided for maintaining power after the user has activated the mechanical switch 191. The silicon switch 192 makes sure that the rest of the transmission circuitry in the card has enough power to function properly for a period of time after the user has activated the mechanical switch 191 in the event that the user lifts the mechanical switch 191 prematurely.

IPR2025-01150
Apple EX1071 Page 639

A voltage regulator 193 is coupled to the battery 190 via the mechanical switch 191 and the silicon switch 192. The voltage regulator 193 stabilizes the frequency of the microprocessor 194 and lowers the current consumption of the battery 190. The voltage regulator 193 is an LDO with low decoupling capacitors and low current. The output voltage is 2.2V. This IC can also be omitted in expanse to a lesser frequency stability. The voltage is provided to the microprocessor 194, which in one embodiment is a Microchip PIC16F84. An electronic card connector 197 allows for the microprocessor 194 to be programmed. Additional contacts are provided for factory testing and debugging.

A voltage multiplier and driver 195 receives signals from the microprocessor 194 and provides an output at 6Vpp to the transducer 196. An alternative circuit can double the battery voltage to 5Vpp, with fewer components. The voltage multiplier and driver 195 doubles the input voltage to generate a square of the power out. At the very least, the transducer needs twice the battery voltage to be driven. The transducer 196 exhibits approximately 5 nF of capacitance.

In contrast to the above embodiment where a single channel is used to transmit either f0 or f1 for this FSK scheme, two channels can be implemented to increase the bit rate. In one embodiment, the two frequencies to be transmitted are summed in the electronic card where the single transducer transmits the summed signal to the PC. In another embodiment, each frequency to be transmitted is associated with a transducer in the electronic card, where after being transmitted, the transmission medium (e.g., air) adds the two frequency components before being received by the PC. In a further embodiment, one transducer is associated with frequencies f1 and f2, while another transducer is associated with f3 and f4. At any moment in time during a transmission, each transducer transmits one bit so that the electronic card with two transducer essentially transmits two bits at the same time.

Accidental activation of the TX switch in the electronic card can potentially drain the power from the battery supply unless appropriate safeguards are taken. In one embodiment, circuitry is provided such that if the switch is pressed for more than a threshold amount of time (e.g., 1 sec), then the electronic card will turn itself off. No transmission will be possible unless the switch is deactivated first. In another embodiment, the microprocessor is programmed with a time-out logic so that if the TX is pressed for more than a threshold amount of time, then the microprocessor unit will turn off the power.

3.3 CARD TRANSMISSION SOFTWARE

The software in the electronic card primarily performs the following routines:

(1) read data (e.g., ID, sync byte) from memory
(2) write data (e.g., increment counter value) to memory
(3) perform DES3 encryption to calculate Series
(4) calculate checksum
(5) beep audible feedback to user
(6) initialization
(7) transmit data
(8) receive data

IPR2025-01150
Apple EX1071 Page 640

These and other related features of the card software will be described further below.

3.3.1 DATA STREAM

The software for the card resides in the microcontroller and is written in Assembly language. On activation of the card (i.e., press of the switch), the card transmits a data stream that comprises a header, data, a footer, and start/stop bits. The header, footer, and start/stop bits are fixed. However, the software calculates the data portion.

Referring now to FIG. 5(A), the data stream includes f0 (approximately 100 msec long or 24 bits), f1 (approximately 20 msec long or 5 bits), a synchronization byte, a known byte, the data portion (96 bits), and a checksum (CRC) byte. The portion of the data stream beginning with the synchronization byte to the checksum byte is divided up into bytes of data with start and stop bits inserted between the bytes. Thus, at the beginning of a byte is a start bit (e.g., logic 1) and the end of that same byte is a stop bit (e.g., logic 0).

The f0 and f1 portions of the data stream represent the two FSK frequencies employed by the system. The f0 and f1 portions are pure sinusoids of the base FSK frequencies and are transmitted first to allow the receiver to enable detection.

The sync byte is a sequence of alternating bits with some pattern (e.g., 01010101) that enables synchronization of the receiver with the received data stream. The known byte is a byte known to both the receiver and transmitter of the system. It assures the receiver that this signal is indeed a signal and not noise.

The data portion is the major part of the data stream where each bit is translated to a wave of frequency f0 or frequency f1 with a length of T msecs that determine the raw bit rate. The discussion below details how one embodiment calculates the data portion, which is denoted by the variable DataOut. In other embodiments, DataOut is calculated differently and can be any desired length depending on the functionality desired by the press of the TX switch.

The checksum (CRC Code 32) byte is transmitted to ensure no errors in the received data stream. Also, as mentioned above, start/stop bits are inserted into the portion of the data stream beginning with the synchronization byte to the checksum byte. This portion is divided up into bytes of data. Start and stop bits are inserted between the bytes. Thus, at the beginning of a byte is a start bit (e.g., logic 1) and the end of that same byte is a stop bit (e.g., logic 0). The start and stop bits are utilized for resynchronization. Because of the clock source in the card has errors, the transmitted signal drifts in frequency which results in missing a sampling point (or sampling the wrong point). The resynchronization provides for this correction.

Returning now to the data portion of the data stream, the software makes use of certain algorithms along with some numerical attributes of the card. Each card is associated with a group ID, individual ID, and a key. The group ID identifies this card with other similarly situated cards; that is, if ABC Corporation distributed the card to its members, the card would have ABC Corporation's group ID number. All cards distributed by XYZ Inc.'s web portal would be associated XYZ's group ID number. The individual ID is essentially the card's serial number and is unique to that card. The key is a secret private key. Note that the terms "private/public key" are from asymmetric crypto systems, but in the current embodiment, only one key is used and is usually referred to in the literature as "the key" or "the secret key". The microcontroller also

IPR2025-01150
Apple EX1071 Page 641

manages a counter in non-volatile memory, which in one embodiment, increments by one each time the card's TX switch is pressed. In one embodiment, the size of these card numerical attributes are:

Group ID: 32 bits

Individual ID: 32 bits (in another embodiment, 16 bits)

Key: 16 Bytes

Counter: 32 bits

Based on these numerical attributes, the microcontroller in the card creates a complex numeric series that is not easy to predict. One preferred series is:

Series = DES3(Key, Msg), where Msg = [Group ID, Counter]

DES3 represents the Data Encryption Standard (DES) cryptographic algorithm as defined by the U.S. Bureau of Standards (FIPS PUB 46-2, 1993 and FIPS PUB 74, 1981). Msg is the concatenation of the 32-bit Group ID and the 32 bit Counter value, which results in a 64-bit number. The Series is a 64-bit number. The microcontroller employs the algorithm in the encryption portion of the software to calculate this Series. However, what is actually transmitted for the data portion of the signal is:

DataOut = [Series, Individual ID]

Here, DataOut represents the concatenation of the 64-bit Series which is a DES3 encrypted number and the unencrypted 32-bit Individual ID, which results in a 96-bit number. On every activation of the card, the counter is incremented and the next code in the series is used.

In an alternative embodiment, security can be assured by storing identical sets of random numbers both on a memory unit in the card, and on the authentication server. That random number takes the place of the DES3 encrypted number element of the DataOut series described above. The advantages of such an embodiment are twofold. First, it clears processing resources on the card, or reduces the complexity of the processor needed, since the encryption algorithm no longer is practiced. Also, theoretically, a random number scheme is virtually impossible to decrypt.

3.3.2 TRANSMISSION ROUTINE

A high level description of the transmission routine in the electronic card will now be provided with respect to FIG. 6(A). The transmission routine begins at step 50. At step 51, the parameters Known Byte, Sync Byte, Series, Individual ID, and Checksum are placed in the send buffer. To perform this step, some of these parameters are either retrieved from memory (Known Byte, Sync Byte, Individual ID, checksum, and also the counter value) as well as calculated (Series). Step 52 requires that the base frequencies f0 and f1 in FSK are selected. Step 53 transmits the data. The transmission routine ends at step 54.

FIG. 6(B) illustrates a more detailed flowchart of the transmission process. This flowchart provides more details for steps 51 and 53 of the FIG. 6(A). The flowchart begins at step 60. At step 61, the microcontroller reads the counter value. At step 62, the microcontroller calculates the Series based on the Key and the Msg, as described above. For each press of the TX switch, the microcontroller increments the counter

IPR2025-01150
Apple EX1071 Page 642

value by one. At step 63, the microcontroller determines DataOut as the concatenation of the encrypted Series and the unencrypted Individual ID. Having calculated the data portion of the data stream, the microcontroller is now ready to transmit the data stream.

At step 64, the microcontroller transmits f0 for approximately 120 ms (or 24 bits) and f1 for approximately 20 ms (or 5 bits). At step 65, the start bit (logic 1) is transmitted. A byte of a portion of the data stream beginning with the synchronization byte and ending with the CRC bytes are then transmitted at step 66. The stop bit is transmitted at step 67. If any more data from the sync byte...CRC portion of the data stream is remaining, then the microcontroller goes back up to step 65 to transmit the start bit. It then transmits another byte of data, followed by the stop bit. If no more data is remaining to be transmitted, the process ends at step 69.

After the data has been transmitted, the card turns itself off to conserve battery power. In another embodiment, the card goes into receive mode for a few seconds after the transmission steps in anticipation of receiving data. Thereafter, the card turns itself off to conserve power. In still another embodiment, the card provides an audible feedback (e.g., beep) to alert the user that the data has been successfully transmitted. Some delay is provided after the beep to compensate for the case where the CPU turns off the power before the user lifts his finger off the switch. Then, the card turns itself off, or alternatively, goes into receive mode followed by power off.

Note that the system uses FSK to transmit the signals. In one embodiment, the system is capable of being modified so that the base frequencies (f0 and f1) are adjustable. This modification can occur in realtime and in automated fashion to ensure that the receiver receives a good signal. Similarly, automatic retransmission is also provided as a feature of the electronic card. For example, if the user presses the switch on the card longer than expected, this may imply that the transmission is bad because the user did not see the appropriate response from the PC (e.g., an audible beep from the PC to indicate that the signal was properly received). In this case, the card will, after some delay, retransmit the data stream possibly using a different set of FSK frequencies.

Some other design considerations should be taken into account. The program code necessary to execute the above process is relatively small to fit into the small microcontroller. The timing is very exact so as not to introduce errors and audible noise to the communication. Since a low cost processor is used (e.g., Microchip PIC16F84), PWM or DTOA units are not available; therefore, the digital output pins of the processor will be used for transmitting the signal.

In one embodiment, the bit rate for the transmitted data is 200-600 bits per second.

3.3.3 MULTI-MODE SWITCH

In accordance with one embodiment of the present invention, the electronic card contains one switch. To provide multiple functionality for the electronic card (and the client base station, such as a personal computer), the electronic card is equipped with multiple modes. Each mode is associated with some unique function apart from the other modes. In one embodiment, the mode of the card depends on the length of time that the switch is pressed by the user. To assist the user in determining what mode he has invoked, or

IPR2025-01150
Apple EX1071 Page 643

conversely, how long he has pressed the switch, an audible feedback such as a beep sound is generated by the electronic card. Thus, for every T seconds that the switch is pressed, a single audible beep is generated. In one embodiment, T is 0.25 seconds. A single beep indicates that the electronic card is in one mode, while two beeps indicate that the electronic card is in another mode.

Referring to FIG. 28, a state diagram is provided. At state 280, the electronic card is turned off. So long as the switch is not pressed, the electronic card is not operating.

When the switch is pressed, the power of the card is turned on. This is represented by state 281. The card may require the switch to be pressed for some minimum amount of time before it is recognized as a valid switch press. In one embodiment, this minimum amount of time is 0.25 seconds. When the switch is pressed for this minimum amount of time, the electronic card will provide an audible beep every T seconds (e.g., 0.25 seconds) so long as the switch is depressed. The number of beeps indicates to the user the mode of the electronic card. Of course, the user would already know what mode he wants to place the electronic card in and he holds down the switch until the desired number of beeps is produced.

When the user finally releases the switch, the number of beeps is temporarily stored in memory in the electronic card in state 282. This beep number can then be used by the electronic card to perform its function in accordance with the mode selected by the user. Alternatively, the number of beeps along with the card authentication data (e.g., Series, checksum, Individual ID) are transmitted to the client base station. The client base station can then receive the number of beeps and interprets the mode of the communication. At state 283, the CPU in the electronic card turns off the power to conserve battery power.

Some exemplary modes are as follows. A single beep indicates that the electronic card is in transmit mode. Whatever data that needs to be transmitted will be transmitted shortly. After the data has been transmitted, the electronic card turns itself off. In another embodiment, a reception period (e.g., 1 second) follows immediately after the transmission of data. This is then followed by power off.

A double beep indicates that the electronic card is in receive mode only for a short time period. In another embodiment, the electronic card sends the two beep indication to the client base station. The software in the client base station interprets the two beep indication as displaying a drop-down menu list of actions. The user can then select one of the listed actions. In one embodiment, these listed actions can be: (1) launch the browser, (2) launch the browser, if it is not already launched, and go to the user's designated home page (or the home page of the company sponsoring the electronic card); (3) launch the browser, if it is not already launched, and go to some designated website; (4) launch the user's email application, if it has not already been launched; (5) send email in the user's outbox and receive email from the user's mail server; (6) perform simple diagnostics by sending data to the electronic card, followed by receiving some data from the electronic card; and (7) perform any other series of actions (predefined or assigned by the user).

In another embodiment, the list of actions that are displayed on the client base station's monitor is context-sensitive. Thus, if the user's browser is already opened and displays the home page, one of the actions listed will not be to launch the web browser and go to the user's home page. Typically, one of the actions listed will be to fill out a form. So, if a user was shopping on the web and found some merchandise he would like to

IPR2025-01150
Apple EX1071 Page 644

purchase, he proceeds to the checkout line on the website where he encounters a form. The user presses the switch on his electronic card and waits for two beeps to sound before releasing the switch. The client base station receives the two-beep indication and proceeds to list action items in menu form. One of the action items is to "fill out a form." When the user selects this action on the list, the client base station proceeds to fill out the form on that web page to automate the purchasing process for the user. The client base station would have all the information necessary to fill out such a simple purchase form – name, billing address, shipping address, phone number, credit card number, credit card expiration date, etc. Once this form has been filled out, the user can use the browser in the conventional manner to complete the sales transaction. Form filling functionality details are provided below.

In another embodiment, three beeps indicate that the electronic card should reset. Similarly, three beeps could indicate that the electronic card should erase the contents of its battery backed-up RAM. If the RAM is used to store downloaded data off the Internet or some broadcast media device (e.g., TV or radio), this data is then erased.

In a further embodiment, a text-to-speech conversion feature is provided in the electronic card. An audio file is also stored in the electronic card. Each audio file is associated with one of the beep numbers; that is, an audio file is associated with a single beep and another audio file is associated with two beeps. Thus, the user need not remember what function corresponds to how many beeps. When the user has released the switch after N number of beeps, the electronic card plays the audio associated with the N beeps. For example, if the user selected two beeps, the played audio file says, "On-screen menu? One beep for YES and two beeps for NO." If the user did indeed want an on-screen menu list of actions to be displayed on the client base station monitor, he would press the electronic card switch until one beep sounds. Otherwise, he would press the switch until two beeps sound.

As described above, the electronic card can have one switch or multiple switches. Similarly, the audible feedback can vary from a single beep to multiple beeps. Based on the context or the action taken by the user, the audible feedback or alert can have different sounds (e.g., beep, buzz, ring). Additionally, the audible sound can be provided at the beginning or at the end of the action taken by the user. In other words, to use the example above, the beep can sound at the beginning of every T seconds instead of at the expiration of every T seconds.

One attractive application of either a multi-mode switch or of multiple switches on a single card relates to using the same card at base stations with diverse reception/transmission capabilities. For example, certain base stations, such as ordinary phones in a "Plain Old Telephone" ("POTS") network, are capable of receiving and passing on sounds in the audible, but not in the ultrasonic range. Where it is desirable to have a single card use audible transmissions in that environment, but ultrasound in other environments, a multiple switch or multi-mode switch as described above can be used. Specifically, in a multimode embodiment, a single press of the switch would activate an ultrasonic transmission terminated by an audible beep for user feedback. A longer press could result in (i) either the ultrasonic transmission or a simple pause, followed by (ii) either a terminating

IPR2025-01150
Apple EX1071 Page 645

"beep" for user feedback or none; and (iii) by an audible transmission for use over the phone or another similarly limited device.

There are a number of examples of the types of cards that would be attractive when implemented as cards tailored for use with highly functional acoustic base stations like computers or base stations that are more acoustically limited. For example, when implemented as a credit card, this multimode card would offer the cardholder the security of knowing that even a customer service representative does not get access to their credit card number, since it will sound like modem noise, which is actually transmitting a one-time code that cannot be reused (Described below). Just a few examples include frequent flyer or loyalty cards that can be used on the phone or via an Internet computer to accrue or spend points, car reservation services, and membership cards of all sorts.

3.4 CARD RECEPTION HARDWARE

The reception unit 32 will now be described in greater detail with respect to FIGS. 4(A) and 4(B). The primary objective of the analog front end of the reception unit is to detect the transducer's response to audio signals, amplify the transduced signals, filter them, and pass them to the microcontroller's A/D for digital processing. FIG. 4(A) shows a transducer 40 receiving the audio signal, transducing the acoustic signal to an electrical signal such as a voltage change, and delivering the transduced electrical signal to a pre-amplifier 41. The transduced electrical signal is at level of tens of microvolts (e.g., 10 microvolts).

The pre-amplifier 41 is a high impedance amplifier that amplifies the transduced electrical signal. It amplifies the signal 100 or 200 times the input. Thus, the output of the pre-amplifier 41 is at 1,000 microvolts or 1 mV. The pre-amplifier 41 then sends the amplified signal to a band pass filter 42.

The bandpass filter 42 is a filter with a Q of approximately 8 to filter the signal. In one embodiment, it passes signals in the 17-20 kHz range for the ultrasonic frequencies. A high pass filter is also provided on top of the bandpass filter to further attenuate speech. The design of the bandpass filter 42 accounts for the limited gain margin of the op-amps at the center frequency. The classic computation of Q should also be altered for compensation. The bandpass filter 42 passes the filtered signal to an automatic gain control (AGC) circuit 43, which then delivers the signal to the microcontroller 44.

The combination of the pre-amplifier 41 and the bandpass filter 42 uses a non-inverting MFBF scheme as a compromise to obtain the high Q and high input impedance. The pre-amplifier 41 needs a high input impedance, but the bandpass filter 42 with a high Q has very low input impedance. The gain in the lower frequency ranges is 1 (instead of decaying in 20 dB/dec), but this still leaves more than 40 dB of attenuation compared to the center frequency. The next blocks with the high pass filter (see FIG. 4(B)) deal with the further attenuation at lower frequencies.

The AGC circuit 43 will now be discussed with respect to FIG. 4(B). The AGC 43 keeps a fixed level of amplitude on the microcontroller's input and is located after the bandpass filter 42 to maintain a stable output (i.e., low phase shifts inside the AGC loop). The output of the AGC 43 is a frequency shift keying (FSK)

IPR2025-01150
Apple EX1071 Page 646

signal. In one embodiment, the dynamic range of the AGC 43 should be approximately 40 dB. Also, the AGC 43 works with low current and low voltages (e.g., 2 volts) with low amplitude variance at the output (input to the microcontroller 44). The microcontroller 44 determines whether the FSK signal is a signal at one frequency f0 or another frequency f1.

In the AGC 43, the signal at the output of the band pass filter 42 is provided to a divider 45, which outputs a signal at a relatively constant amplitude and low level. This signal is delivered to a gain and high pass filter circuit 46. The gain circuit is a constant gain amplifier with a fixed gain of approximately 300 dB determined mainly be the feedback resistors ratio. The input of this block is approximately 3.3 mVp-p and the output is approximately 1 Vp-p. This gain is large compared to the amplifier's open loop gain, and the amplifier has a relatively small gain margin at the desired frequency. This results in a reduced gain (compared to the lower frequency with the same resistors ratio), and a phase shift. However, the signal is not distorted. The high pass filter portion of the circuit 46 is realized by adding a capacitor to the feedback resistors. This high pass filter further attenuates speech frequencies. The output of the gain and high pass filter 46 is provided to the microcontroller 44 for further processing.

An amplitude estimator 47 is placed in a feedback loop from the output of the gain and high pass filter 46 to the input of the divider 45. The amplitude estimator 47 comprises two low end op-amps – an absolute value block and an integrator. The absolute value block estimates the output signal's amplitude. Other circuits (e.g., peak detector) may also be considered. The integrator locks the output amplitude on a predetermined value. This value is determined by the ratio of the resistors of the integrator. The gain of this integrator is determined by the multiplication of the feedback capacitor and the input resistor. This factor controls the speed of the loop and the ripple on the AGC's FET (the ripple is reduced by a LPF network after the integrator).

A tradeoff exists between the speed of the integrator and the signal distortion. When the gain is low, the FET receives a well-filtered signal that allows fine-tuning of the FET's resistance. When the gain is high, the output signal's final amplitude is reached quickly, but the signal will be distorted because of the fluctuations on the FET's gate. When Vgs/Vt is approximately 1, small fluctuations in Vgs result in large fluctuations in the FET's resistance. The ripple on the FET's gate is approximately 2 mV, based on a simulation.

Another tradeoff is between the time of settling and the final amplitude. The microcontroller prefers to have the largest amplitude possible (Vcc peak-to-peak). However, the integrator needs a spare of output amplitude in order to manufacture faster the error voltage for the FET. For now, the output signal is about a quarter (1/4) of the Vcc.

The constraints on the system include:

(1) low IC count

(2) low passive components count

(3) low current drain (< 2mA, not including the microcontroller)

(4) power supply is 4-6 volts, although the design works with 2-3 volts power supply with voltage multiplier circuitry

(5) low cost

IPR2025-01150
Apple EX1071 Page 647

(6) working temperature of 0-45 degrees Celsius

(7) robustness of design over device tolerances

(8) low noise level at the output

(9) input signal is tens of microvolts.

A more detailed view of the receiver in a two-way configuration is provided in FIGS. 18 and 19. FIG. 18 shows the analog front end and FIG. 19 shows the microcontroller unit. In FIG. 18, the power on switch block 198d provides for the batteries, where in this embodiment, two Varta batteries BT1 and BT2 are installed. These batteries provide power to the rest of the circuit via the switch SW1. The remainder of the circuitry provides for signal shaping and signal holding in a manner similar to the circuit of FIG. 9.

The transducer switch block 198a provides for both transmission and reception front end capabilities. The AnalogOn allows for the selection of input/output. The signal that should be transmitted is present on DigitalOut to pin 2 of the PI5A319A chip. If the transducer switch block 198a is in transmit mode, the signal is provided on pin 1 of the PI5A319A chip to the transducer pad TP1. If the transducer switch block 198a is in receive mode, the signal is provided to pin 1 of the PI5A319A chip from the transducer pad TP1. The received signal is then routed to pin 8 of the PI5A319A chip. The portion of the transducer switch block 198a that is associated with TP2 provides for noise immunity.

The received signal makes its way to the preamplifier and bandpass filter block 198b. After amplification and filtering, the received signal is provided to the high pass filter and AGC block 198c. The beginning portion of the circuit from resistor R2 to capacitor C7 provides for the divider function. The next portion of the circuit provides for the AGC function to generate the fixed amplitude. The bottom portion of the circuit provides for amplitude estimation. The processed signal is then provided to the microcontroller (e.g., Microchip PIC16F877 in a TQFP package) via AnalogIn.

The Vcc block 198e and Vref block 198f provide for the appropriate Vcc and Vref voltage sources that are used throughout the analog front end circuits. The additional circuitry 198g round out the analog front end.

FIG. 19 provides the pinouts and circuitry surrounding the digital core of the electronic card. The microcontroller/microprocessor 199a used in this embodiment is a Microchip PIC16F877 in a TQFP package. AnalogIn is the received signal to be processed. Conversely, DigitalOut is digital signal to be transmitted out of the card. The additional components like the connectors 199b and test point block 199c allow for programming and debugging of the microprocessor 199a.

Additional embodiments use different techniques for decoding the received signal in the electronic card. In one embodiment, a hardware phase-locked loop technique is employed. Referring to FIG. 40, transducer 400 receives the acoustic signal and makes the appropriate voltage conversions. The bandpass filter portion of unit 401 filters the signal in order to attenuate speech (or noise) signals. The preamplifier portion of unit 401 amplifies the signal to a minimum amplitude of a few milli-Volts. At this amplitude, most PLLs can lock onto the input signal. An AGC block 404 can be realized before the PLL 402 to increase the SNR.

IPR2025-01150
Apple EX1071 Page 648

In this embodiment, the PLL 402 is an XR215, XR2211, LMC568, or the like. The PLL 402 demodulates the audio signal as known to those ordinarily skilled in the art. The output of the PLL 402 can be a digital square wave of the decoded FSK signal. Alternatively, the output can be an analog voltage whose level is correlated to the input signal frequency. The microprocessor unit 403 accepts either of these forms of signals for further processing.

In another embodiment, software PLL/FLL decoding technique is employed to implement the locking of the input signal. Referring now to FIG. 41, the transducer 410 receives the acoustic signal and provides the necessary conversions. The bandpass filter portion of unit 411 filters the signal in order to attenuate speech (or noise) signals. The preamplifier portion of unit 411 amplifies the signal to a minimum amplitude of a few milli-Volts. The hard limiter block 412 produces a square wave from the analog output. The microprocessor unit 413 uses this digital input signal to implement the decoding. To increase the SNR, an AGC block 414, under the control of the microprocessor unit 413, can be realized before the hard limiter block 412.

In another embodiment, a mixer is used for baseband processing. Referring to FIG. 42, the components are similar to the above two embodiments corresponding to FIGS. 40 and 41 with the exception of a mixer 422. In this technique, the mixer 422 shifts the ultrasonic acoustic signal from around 20 kHz to baseband. Baseband processing is much easier to implement. An exemplary decoding method is squaring the analog output and processing the digital data. Another equally applicable method is conventional DSP algorithms for processing analog data.

3.5 CARD RECEPTION SOFTWARE

The goal of the receiver, whether hardware or software, is to detect and decode the FSK signal in real-time in a very simple processor with an erroneous clock. The receiver hardware received the acoustic signal, transduced it to an electrical signal, amplified it, and cleaned it before presenting it to the microcontroller. The receiver software in the microcontroller then processes the cleaned-up analog signal and attempts to decode it to extract the actual data therein.

The data stream transmitted by a base station (e.g., PC) comprises a header, data, a footer, and start/stop bits therein. The header, footer, and start/stop bits are fixed. The footer includes the checksum (CRC) byte. Referring to FIG. 5(B), the header includes an energy detector bit (1 bit) which includes contributions from two frequencies (sin(2*pi*f0*t) + sin(2*pi*f1*t)), a pure sinusoid with frequency (f0+f1)/2 (3 bits), a pure sinusoid with frequency f0 (3 bits), a pure sinusoid with frequency f1 (3 bits), and a known byte.

The data portion includes the actual data that the base station is trying to deliver to the card. This includes instructions, flags, and pure data for storage (e.g., coupons). The length of the data portion varies from one application to another.

Like the card-to-PC transmissions, start and stop bits are also used for this PC-to-card transmissions for resynchronization. The portion of the data stream from the known byte to the CRC byte is divided into bytes. Each byte is preceded by a start bit (logic 1) and appended by a stop bit (logic 0).

Referring to FIG. 12, the receiver downsamples the signal so that it could handle the otherwise large number of computations in real-time. This downsampling can be achieved in hardware with a bandpass filter

IPR2025-01150
Apple EX1071 Page 649

and an analog-to-digital (A/D) converter 120. For example, if the signals are between 18 kHz and 20 kHz, this portion of the spectrum can be prefiltered with the bandpass filter and then sampled at approximately 5 kHz (or 4900 Hz which is CD audio quality 44.1 kHz divided by downsampling factor 9). After the sampling, the signal will have moved to the 0-2 kHz band.

The energy detector 121 in the software then looks for a sharp rise in the signal energy. This energy detector 121 is used to determine whether an actual signal is present for processing. This can be accomplished by averaging the absolute power of the first bit (energy detector bit in FIG. 5(B)) of the received signal using a first order IIR filter of the form:

y[n] = a*abs(x[n])+(1-a)*y[n], where 0<a<1 and x[n] is the input signal

As mentioned previously, the signal comprising the energy detector bit is the addition of two sinusoids, where one sinusoid is at frequency f0 and the other sinusoid is at frequency f1. The reason why both FSK base frequencies are used is because there's a chance that one or the other frequency component will be DC after aliasing from the downsampling operation. If so, the high pass filter will remove it and the energy detector 121 will miss the beginning of the signal.

The receiver software samples one point. If the energy detector detects a high enough signal, then it's a signal. If not, the energy detector examines the next sample.

The next two blocks 122 and 123 correct for the card's clock errors. In contrast to the clock source in the card, the PC's clock source is more precise. Thus, the PC sends a constant and known frequency for the card to lock onto. The algorithm used by the card is a Least Mean Squared (LMS) on the following equation.

Any sine wave of the form x[n]=A*sin(2*pi*f0*n + phi) satisfies the difference equation:

x[n+1]*cos(2*pi*f0) = (x[n]+x[n+2])/2, for every n

Most notable about this difference equation is that it is second order, with at least one unknown parameter, b = cos(2*pi*f0), which can be interpreted as an unknown multiplicative constant. By defining an intermediate signal, b is determined by minimizing the mean squared error:

E{ (b *x[n] - s[n])^2 }

where E{} denotes statistical expectation. An LMS rule for determining the unknown coefficient b is given by the recursion

b[n+1] = b[n] - c*(b[n]*x[n]-s[n])

IPR2025-01150
Apple EX1071 Page 650

where c is a parameter that determines the rate of convergence ($0 < c < 2$), and the subtraction is used to implement the negative of the gradient (with respect to the parameter b) of the instantaneous cost C(b * x[n] - s[n]), as defined above. The frequency f0 can be estimated from b[n] by inverting the formula b[n] = cos(2*pi*f0[n]), most preferably in steady state (after convergence), and under the condition that -1 <= b[n] <= 1.

So, if the coefficent of x[n] is not known, an initial guess can be made and subsequently, the coefficient can be adaptively changed proportionally to the error as in any LMS algorithm. Here, the frequency adaptation bits are used. Referring briefly to FIG. 5(B), the 3 bits of (f1+f0)/2, the 3 bits of f1, and the 3 bits of f0 are used. For the first 3 adaptation bits, the average of f1 and f0 is used to minimize the risk that the correct frequency correction will be made. If only f1 or f0 is used, either f1 or f0 may flip over to the other side on the frequency spectrum during downsampling. When this happens, the receiver software will make a wrong correction of the frequency. By taking the average, the chance that the frequency will flip over is minimized and hence, the wrong correction will not be made.

After the frequency is adaptively selected in block 122, block 123 attempts to decode the first byte. If the decoding is bad, the receiver software returns to the A/D converter stage and starts over.

At block 124, the receiver software decodes the data to determine whether the received signal is a logic "1" or logic "0." Finally, block 125 checks for any errors using the checksum byte.

3.6 CARD MECHANICAL CONSTRUCTION

With respect to the mechanical construction of the electronic card, the electronic card complies with the credit card set of standards – ISO 7810, 7811-1 to 7811-6, 7813, 7816-1, and 7816-2. Some minor deviations from the standard are inevitable such as the location of the external switch and of course, the additional functionality provided by the card electronics. In other embodiments, no attempt is made to make the electronic card comply with the credit card standards. However, in the discussions below, the credit card standard-complying electronic card will be described.

The components in the card are miniaturized and placed on select locations in the card to optimize the use of such limited space. An external button is provided on the electronic card itself so that when it is pressed by the user, the electronic card encrypts the digital ID and transmits the encrypted digital ID via ultrasonic acoustic waves. The card also includes acoustic transduction elements, such as a microphone and a speaker, which serve as the acoustic antennae.

In a preferred embodiment of the invention, the card is thin (0.8 mm is a standard plastic card thickness), so the microphone should also be very thin. The acoustic receiver can be any microphone, such as a regular capsule microphone or an ultrasonic type microphone, which is possibly specific for a particular frequency or frequency range used. In some cases, special ultra-low power circuitry may be desirable. The acoustic transmitter can preferably generate a strong atmosphere wave. It is noted however, that only a small amount of power is required for short range transmissions.

The reception transducer is a capacitive microphone with two plates with a small air gap; that is, the distance between the two plates are small compared to conventional capacitive microphones. Any vibration on

IPR2025-01150
Apple EX1071 Page 651

the plate changes the capacitance which in turn changes the current to the reception circuitry. With a DC voltage applied across the plates, the resulting changing current signal is filtered, amplified, and then analyzed since the modulation of this signal is directly proportional to the information contained therein. The transmit transducer is a thin stainless steel/brass plate on a PCB with a piezo-ceramic material on top of it. The distance between the top surface of the piezo-ceramic material and the printed PVC layer is approximately 0.8 microns (micro-meters).

The electronic card's battery is small and is guaranteed to work in 0-60 degrees Celsius. Even if the electronic card is left inside a hot car, the battery will not be damaged. The battery also functions in temperatures down to –15 degrees Celsius. Up to 10,000 card activations (i.e., switch press) are possible for one embodiment of the present invention.

The electronic card is very robust to bending and has been designed to provide maximum bending protection. The electrical connection between the battery and the other components is soldered and subsequently covered with PVC, making the circuitry very resilient. Furthermore, components in the card have been placed in locations such that any bending of the card will not damage or otherwise impair the functionality of the electronic card.

With the current fabrication process, the electronic card can be laminated and embossed at 120 degrees for 10 minutes without damage to the card's circuitry or internal components. In other embodiments, the components, such as the transducer itself, are shielded so that hot lamination processes can be used.

The electronic card allows for conventional embossing in the area reserved for embossing cardholder information in compliance with ISO 7816. High pressure embossing is also possible in the card signature field since the electronic card does not have circuitry in this area.

Branding is also important for electronic card sponsors. The electronic card can be printed with any external features of the integrator's choice, including holograms and company logos.

3.6.1 SHEETS-LEVEL CARD FABRICATION

With current smart card fabrication techniques, the exposed nature of the smart card contacts complicates the assembly/lamination/printing process. Usually, assembly of the smart cards involves the manufacture of a plurality of smart cards in sheets. Each sheet is typically 7x12 cards (or 84 cards), although the exact dimensions of the matrix can vary depending on the type of smart card. However, for efficient and cost effective mass production, these smart cards are manufactured in large numbers to produce these sheets. Also, because these sheets contain smart cards, the smart card modules are exposed, which complicates the process. Also, sometime during this process of creating sheets, the individual smart cards are programmed. At some point, these sheets are cut into smart cards.

The current process for producing smart "bank" cards utilizes the conventional credit card fabrication more closely than that of the electronic card of the present invention. In fabricating smart cards, actual fully compliant "dumb" cards are produced in a credit card manufacturing operation. This includes the standard sheet printing/laminating/singulation processes. Once the "dumb" card is complete, it is further processed into a smart card. This is accomplished by machining a cavity into the body of the "dumb" credit cards and

IPR2025-01150
Apple EX1071 Page 652

implanting a smart card module into the body of the card. The subsequent personalization processes, therefore, do not represent a significant threat to the module.

During the lamination and printing stages, special machines (e.g., DataCard, Heidelberg) are needed to print the appropriate information (logos, numbers) around the exposed smart card modules. Heidleberg printing presses are used for the offset printing of the sheets, whereas the DataCard machines are for the personalization of individual cards, which can include thermal or dye sublimation printing. Without these special machines, the printing/lamination stage could potentially damage the exposed smart card modules and render the smart card useless. Also, special machines would also be needed to read and program the chips in the smart card. If additional personalization is needed (i.e., user name, user signature, user photo), these special machines would be needed again to print around the exposed modules as well as read and program the chips therein. Thus, the exposed modules in these smart cards complicate and otherwise makes costly the card fabrication process after the cards have been laid in sheets.

One embodiment of the present invention significantly improves this procedure. Not only do the electronic cards of the present invention contain "smarts," but these electronic cards do not expose the contacts or modules fabricated therein. The manufacturer programs these cards with the appropriate codes and IDs that are described throughout this patent specification. These cards are also laid out in sheets, where at some point, they are cut to produce the credit card-sized electronic cards. During the printing/lamination stage, standard credit card printing/lamination machines that are used on conventional United States-based "dumb" credit cards are utilized. No special machines are needed to print and laminate around the exposed smart card modules since the electronic cards of the present invention have no exposed modules. Also, since the electronic cards of the present invention have already been programmed, no additional machines are needed to read and program these cards. These cards are delivered directly to the user of the account.

To activate and personalize the card, the user would normally log into the card sponsor's website and press the button on the card. The website would process the data transmission and affiliate the card ID with the user's account. This is analogous to the user calling an 800 number to activate the card. In fact, the card can emit a signal usable over ordinary phone lines or cellular phones and thus, the cardholder's first activation of a card over that 800 number could also result in affiliating the card ID with the cardholder's account. Thus, the issuer need not worry about programming the electronic card since the affiliation of the electronic card with the user's account would occur at the backend after the user has activated the card by pressing the card button. The personalization of the card occurs upon the "first use" of the card in accordance with one embodiment of the present invention. In contrast, conventional technologies require some form of card-accepting device to be available and operational at the time of card registration or activation in order for personalization to occur.

Furthermore, according to the credit card standards, if smart card modules are exposed, the smart card must comply with the credit card standards organization's approved payment system. This involves additional components in the cards and additional programming to comply with the payment standard. By not exposing the modules in the electronic cards of the present invention, the manufacturer of these electronic cards need not

IPR2025-01150
Apple EX1071 Page 653

comply with this payment system standard. This allows the manufacturer to save on the cost of supplying, assembling, and programming the chips with the payment system standard-complying logic.

By preprogramming the electronic cards and not exposing any of the modules, the fabrication of these electronic cards provides efficiency improvements in fabrication (via the use of standard printing/lamination machines and no additional programming), cost (no additional logic needed to comply with payment system standard; no special machines needed to print/laminate around the exposed modules), and standards compliance (no separate payment system standard compliance issues). In essence, fabricating the electronic card of the present invention provides all the benefits of fabricating a standard credit card, in addition to the benefits described above.

3.6.2 COMPONENT LAYOUT

The component layout in the electronic card will now be discussed. Referring to FIG. 25(A), the substrate portion of the electronic card is shown. Here, the basic components and their placement in the substrate of the electronic card are illustrated. For the sake of clarity, trace conductors/interconnects are not shown; however, one ordinarily skilled in the art can determine the location and paths of trace lines based on the circuit diagrams described above.

Here, substrate 257 is shown superimposed on the outline of the final credit card form factor card 250. From this orientation, the magnetic stripe portion of a typical credit card is provided in region 258. On one side of the electronic card in this region is the magnetic stripe itself. On the other side of the electronic card in this region is the embossing area where credit card issuers normally place the name, social security number, expiration date, and other embossed information. On the same side is the logo of the credit card, and in some cases, the photo of the cardholder.

In this region 258, several components are also provided – switch 256 and transducers 254 and 255. The switch enables the electronics in the card to first transmit data in the electronic card and then followed by a short receive period. In other embodiments, of course, the single switch permits multiple modes where, for example, a single press indicates transmission and a double press indicates reception. In still other embodiments, multiple switches are provided on a single electronic card. Typically, the switch is a dome switch constructed of stainless steel material. A thin PVC layer also covers the switch. The switch is normally provided on the side opposite the printed PVC layer where the actual magnetic stripe is placed.

In this embodiment, two transducers are provided – one for transmit (e.g., speaker for acoustic signals) and the other for receive (e.g., microphone for acoustic signals). In other embodiments, only one transducer is used for both transmit and receive. Essentially, the transducer is piezo-ceramic disc on top of a small brass/steel plate. The entire structure is enclosed in a reverberation chamber. More details of this construction are provided below.

Outside of this magnetic stripe region 258, the battery 251, the chip and surface mount technology components 252, and electronic card connectors 253 are provided. In one embodiment, the battery is a Varta LPF-25. For smaller capacity, the battery is a Varta LPF-7. The chip and SMT components include the digital core (microprocessor and supporting circuits) as well as the analog front end.

IPR2025-01150
Apple EX1071 Page 654

Another embodiment of the component layout is shown in FIG. 25(B). Once again, the substrate 257 is shown superimposed on the outline of the electronic card 250. In this embodiment, two batteries 251a and 251b are provided. Part of the first battery 251a along with the chip/SMT 252 and the switch 256 are in the magnetic stripe region 258a. Outside of this region, the electronic card connectors 253, transducer 259 (which can provide both transmit and receive functions) and second battery 251b are provided.

In another embodiment, region 258b is the magnetic stripe area, instead of region 258a. In this embodiment, transducer 259 and part of the second battery 251b are placed in this region without affecting the magnetic stripe. Other components are outside this region 258b.

FIG. 25(C) shows a third embodiment of the component layout. In this embodiment, the switch 256 is the only component in the magnetic stripe region 258a. All other components including the two transducers 254, 255, the electronic card connectors 253, the digital core circuitry 252a, the analog front end circuitry 252b, and the battery 251 are placed outside this region 258a. Note that in this embodiment, the electronic card connectors 253 are placed below transducer 254. The magnetic stripe region 258a can also be used for embossing purposes.

In another embodiment, region 258b is used for the magnetic stripe. In this case, region 258a would be used for embossing,

As these three embodiments in FIGS. 25(A), 25(B), and 25(C) illustrate, the placement of the components in the electronic card is an important design criteria. Generally, the embossing area, which is also typically not the same area as the magnetic stripe region 258, should have as little components as possible. This allows embossing to be accomplished with relative ease while minimizing the concerns that credit card manufacturers may have on whether the embossing process might harm an electronic component. However, as components get smaller and smaller, the placement of some components (in whole or in part) should not affect the durability and reliability of the electronic card.

3.6.3 CARD LAYERS

The fabrication of the electronic card will now be discussed. FIG. 26 shows the various layers that make up the electronic card. At the heart of these layers is the substrate layer 260. This substrate layer includes a chip/SMT cavity 260a, battery cavity 260b, transducer cavity 260c, and switch cavity 260d, where the chip/SMT component 252, battery 251, transducer 254, and switch 256 are placed in these cavities, respectively. Some insulation material is used to cover the battery 251. Also, in some embodiments, the electronic card connectors (not shown in FIG. 26) are covered with PVC and other insulation material after the microprocessor in the electronic card has been programmed and debugged. In the portion of the substrate where silicon components are provided, some epoxy material is used to cover this area to prevent moisture from forming and to prevent this area from physically bending.

Surrounding the substrate layer 260 is the substrate "cap" layer 263 and the cavity layer 264. The substrate "cap" layer 263 is basically a very thin PCB where the underside (in the direction facing the substrate 260) has copper interconnects with special coating. The cavity layer 264 is a PVC material that is provided around the substrate 260 to artificially produce a fixed and constant height for the substrate 260 and its

IPR2025-01150
Apple EX1071 Page 655

components. Obviously, without the cavity layer 264, the placement of the various components in the substrate layer 260 results in different heights for the different regions of the substrate. This entire section which includes the substrate "cap" layer 263, the substrate layer 260 (with the components), and the cavity layer 264 are all filled with a material to fill in gaps to eventually even out the height of the entire section.

Above the substrate "cap" layer 263 is the printed PVC layer 262. The magnetic stripe is fabricated on this layer. Analogously, the other printed PVC layer 265 is provided below the cavity layer 264. The various images (e.g., credit card logo, bank logo), photos, and other information associated with credit cards are provided on this layer. Conversely, the magnetic stripe can be placed on printed PVC layer 265 and the other images and photos can be placed on PVC layer 262. A clear PVC outer layer 261, 266 are provided on the outer surface of each side of the electronic card.

3.6.4 TRANSDUCER CONSTRUCTION

The mechanical construction of the transducer will now be described with respect to FIGS. 27(A) to 27(C). FIG. 27(A) shows a cross-section of a circular transducer, like transducer 254 of FIG. 25(A), in accordance with one embodiment of the present invention. On the PCB 275, which is approximately 0.1 um (microns) in height of plastic, a brass/stainless steel plate 274 is provided. The brass/stainless steel plate 274 is approximately 0.1 um to 0.15 um in height. On top of the brass/stainless steel plate 274 is a small piezo-ceramic disc or element 273, which is approximately 0.15 um in height.

To provide some room for the vibration or movement of the piezo-ceramic element 273 to generate the acoustics, some space is provided around the piezo-ceramic element 273. Spaced apart from the piezo-ceramic element is the printed PVC layer 270. The distance from the top of the piezo-ceramic element 273 to the bottom of the printed PVC layer 270 is approximately 0.8 um. A wall 272 surrounds the piezo-ceramic element 273 and the brass/stainless steel plate 274 to create some enclosed chamber 271. The spacing of piezo-ceramic element 273 from the printed PVC layer 270 and the creation of a chamber 271 with the wall 272 also result in some form of a reverberation chamber for the acoustics. The acoustic signal is generally directed toward the PCB 275 (downward direction on FIG. 27(A)).

The resonant frequency of the acoustic signals generated by this transducer depends on the selection of the various parameters of the components in the transducer. The main parameters include the thickness of the piezo-ceramic element 273, and the thickness, stiffness, type of material, shape, and diameter of the brass/stainless steel plate 274.

FIG. 27(B) shows an alternative embodiment of the transducer construction. In this embodiment, the brass/stainless steel plate is not used. Instead, the piezo-ceramic element 273 rests on and uses the PCB layer 275 as a substitute plate. Additionally a portion of the printed PVC layer 270 protrudes into the chamber 271 so that the distance between the top of the piezo-ceramic element 273 and the bottom of the protruded printed PVC layer 270 remains at 0.8 um. In a variation of this embodiment, the piezo-ceramic element 273 can be made thicker so that the protruding portion of the printed PVC layer 270 would not be necessary. The additional thickness of the piezo-ceramic element 273 would be approximately 0.15 um (or the thickness of the

IPR2025-01150
Apple EX1071 Page 656

brass/stainless steel plate had such a plate been used). Thus, the distance between the top of the piezo-ceramic element 273 and the bottom of the unprotruding printed PVC layer 270 is 0.8 um.

The embodiments of FIGS. 27(A) and 27(B) show transducers which are fabricated as the entire electronic card is fabricated. In contrast, FIG. 27(C) shows a third embodiment of the transducer construction where the transducer is modular and not fabricated with the card. In this embodiment, the wall 276 also includes a cover portion 276a. The cover portion 276a and the wall 276 form the chamber or cavity 271. In one embodiment, the cover portion 276a and the wall 276 are made of either steel or plastic. In this configuration, the piezo-ceramic element 273 need not rely on the printed PVC layer to form the chamber. When this modular transducer is used in the fabrication process of the electronic card, other fabrication technology can be used. For example, the more widely available technique of hot lamination can be used in some of the fabrication steps. Without the modular transducer of FIG. 27(C), some components in the transducer cannot be heated too high without component failure.

4.0 BASE STATION

In one embodiment, the base station is a station that is part of a land-based infrastructure. Although it is usually part of some network, this is not a mandatory requirement. Thus, a personal computer, whether or not it is connected to a local area network or has access to the Internet, is a base station. Other exemplary base stations include televisions, radios, telephones, automated teller machines, card reader at the store checkout line, and the like. In one embodiment, the base station transmission software is similar to that of the electronic card.

In another embodiment, the base station is not necessarily part of the land-based infrastructure; rather, the base station can be portable. Thus, cellular phones, personal digital assistants (PDAs), portable radios, portable televisions, and the like can be base stations. Like the land-based base station, the electronic card in accordance with one embodiment of the present invention can communicate with the portable base station.

In either case, the frequencies for the acoustic signal are carefully selected to enable the electronic card to communicate with the base station. For example, if the base station is a personal computer with a sound system, the acoustic signals can be in the ultrasound range. If the base station is a telephone connected to the public telephone infrastructure, then the acoustic signals should be in the audible range so that they can pass through the filters effectively. Note that a single card can be equipped to emit either audible or ultrasonic transmissions as desired to send to a telephone, a computer, or other digital devices as needed. In another embodiment, the audible frequencies selected conform to the standard DTMF scheme.

4.1 CLIENT COMPUTER SYSTEM

Referring briefly to FIG. 1, in the client computer system 14, a special client remote access software in accordance with one embodiment of the present invention is installed and running. In addition, a standard microphone, speaker(s), and a web browser are utilized. Of course, a web browser is not absolutely essential so long as the computer system allows the user to access the Internet. This can be accomplished with a piece of communications software. At the web merchant or web portal side, a server is provided to handle the user's redemption needs. Thus, having downloaded the coupon from a TV 12 or radio 11, the user can take his card

IPR2025-01150
Apple EX1071 Page 657

to his computer 14, access the Internet 16, and redeem his coupon at the sponsoring web merchant's or web portal's website.

Referring now to FIG. 11, the client computer system will now be described. The client computer system includes a web browser (e.g., Microsoft Internet Explorer, Netscape Navigator) 115, a special client remote access software 114, at least one speaker 111, a microphone 112, and drivers 113 for the sound device(s) (e.g., speaker/microphone). The sound card and corresponding sound card software normally interfaces with the speaker and microphone. Most computers currently on sale include a sound system, usually a "Sound Blaster" sound card, connected to at least one microphone and at least one speaker.

Note that the sound devices that are necessary depend on the particular application of the electronic card. If the electronic card is one-way transmission only, only the microphone is needed in the computer system. If the electronic card is two-way, both the speaker and the microphone would be needed. If the electronic card is one-way receive only, then the speaker would be needed in the computer system.

In a preferred embodiment of the invention, client computer system 110 and electronic card 10 communicate using these standard computer components of client computer system 110, which are usually for human communication, not for computer communication. Some computers are provided with other types of sound systems, which also support the application of preferred embodiments of the invention, possibly with a variation in frequencies to account for different circuit or sampling characteristics. Typically, this sound system is designed for generating music and other audible sounds. In addition, many computers include an internal speaker and a modem speaker. Some computers use USB speakers which are connected directly to the USB (Universal Serial Bus).

In one preferred embodiment of the invention, a standard sound card, such as the popular "Sound-Blaster" is used to generate sonic and/or ultrasonic signals to (and to alternatively or additionally receive them from) an electronic card. The acoustic signal may be audible (in some applications) or inaudible (more preferable), for example having mainly ultrasonic or infrasonic frequencies. Preferably, frequencies of about 22 kHz and 24 kHz and 32 kHz are used, since a standard sound card provides these sampling rates (and/or their multiples, e.g., 44 kHz and 48kHz). Alternatively, lower frequencies, such as between 17 kHz and 21 kHz may be used. In other embodiments, the standard sound card receives sound waves from the electronic card 10 (see FIG. 1) for further processing.

In some preferred embodiments of the invention, a sound card is adapted to work in the near ultrasonic range, for example by increasing its sampling frequency. Generally, the microphone and loudspeaker used for a computer system can support low frequency ultrasound with sufficient fidelity without adaptation. However, in some embodiments of the invention, a special ultrasound-sensitive microphone or ultrasound-effective speaker may be used. In other cases, the sensitivity of a particular microphone and/or loudspeaker maybe determined by the user prior to or during communication with an electronic card.

To provide for software control of the speaker 111 and the microphone 112, the client computer system 110 includes drivers 113. Normally, the user can set playback volume and recording volume on the software control panel which are then set in hardware by the drivers.

IPR2025-01150
Apple EX1071 Page 658

A special client remote access software 114 is provided to interface with the speaker/microphone drivers 113 via communication line 116 and the web browser 115 (or communications application) via line 117. The special client remote access software 114 was written specifically for the various embodiments of the present invention. This software 114 is installed in the client computer system 110 and is normally loaded at all times because the user may use his electronic card 10 at any time. Of course, if the special client remote access software 114 is not loaded, the user simply opens the application whenever he is operating the card.

The special client remote access software 114 performs multiple tasks that are important to the various embodiments of the present invention. During the initial stages of the user's on-line purchase, the special client remote access software 114 processes the sound waves corresponding to the digital ID that have been emitted by the electronic card 10. After having been received by the microphone and processed by the sound card, the sound waves are processed further. The special client remote access software 114 checks the encrypted digital ID sound waves to make sure that the data is complete and corresponds to the appropriate user's electronic card 10. Thereafter, the received data is processed by special client remote access software 114 in different ways depending on the application.

4.2 INSTALLATION AND INITIALIZATION

As mentioned above, the special client remote access software 114 in the user's PC is needed to communicate with the electronic card and the web browser. At times, the special client remote access software 114 can access the Internet and communicate with web servers without the web browser. The installation of the special client remote access software 114 can be accomplished in many different ways. The installation may occur over the web as the software is downloaded from a web server and then subsequently installed in the user's PC. Alternatively, the software can be installed via CD-ROM or floppy disk. Furthermore, when the user buys a computer, the software may be bundled with the computer equipment so that installation is automatic.

In communicating with the web browser, the special client remote access software 114 uses Java applets. When the special software 114 needs to interact with a web page, the Java applet calls the appropriate ActiveX controls to perform basic functions associated with that web page. The deployment of ActiveX by the special software 114 is routine and is known to those ordinarily skilled in the art. In this manner, some aspects of the special client remote access software are found in various servers that can be downloaded to the local client as they are needed. The basic special client remote access software 114 however, is installed locally. Thus, as the user navigates from one webpage to another, different functions may be supported. As the user encounters these webpages, the user can download these different functions to extend the capabilities of his electronic card.

For example, assume that a user has encountered a shopping website. The shopping website requires some authentication to log in. The website indicates that it supports the electronic card. The user then downloads the authentication logic from this website's server. Once downloaded, the user can then press his electronic card to authenticate himself into the website and access his account. When he reaches the checkout line, he downloads the form fill logic from that website's server. When he presses the button on his electronic

IPR2025-01150
Apple EX1071 Page 659

card, the just recently downloaded form fill logic portion of the special client software recognizes the electronic card transmission as requesting a form fill. The special client software then fills out the form on that webpage to assist the user. Other functions can be supported in this manner. Thus, as the user navigates from one webpage to another, he can encounter webpages that support different electronic card functions. If desired, the user can download those functions to extend the usefulness of the electronic card at that website.

In other embodiments, the special client software does not need the web browser to communicate on the web. After all, the special client software can contain all functionality that is in the web browser in addition to the functions needed to communicate with the electronic card. In a further embodiment, the special client software is not needed as the web browser provides all the functions that the user will need. A Java applet downloaded via a Java VM can perform all the specialized electronic card-related tasks, while the web browser itself allows the user to communicate on the web.

Initialization primarily involves the sound system and its supporting equipment. Two main tasks are executed – (1) mixer settings, and (2) sound card memory allocation. When the special client software is launched or otherwise turned on, it initially stores the default mixer settings so that later, it can return the PC to the state before the special client software was activated. The special client software then checks and adjusts the mixer control settings so that the sound card is optimized to interact with the electronic card.

First, the recording setting must be on. If it is off, the special client software turns on the recording setting. In other embodiments, the special client software asks the user to turn on the recording setting.

The special client software then performs several tests, with and without the assistance of the user. These tests involve testing the speaker, the microphone, and the electronic card-PC communication, as detailed below. These tests need not be performed every time, though.

The special client software also checks the microphone. If the microphone is off, then the special client software enables the microphone to be turned on. Alternatively, the special client software may ask the user to turn on the microphone. The special client software may also ask the user to test the microphone by speaking into the microphone. Various threshold settings are stored – (1) silent mic, (2) non-receiving mic, and (3) receiving mic. Alternatively (or additionally), the special client software may ask the user to operate the electronic card. If the test fails, the special client software will ask the user to fix the electronic card by providing various tips, such as proper press of switch, proper distance of electronic card to microphone, proper orientation of the electronic card to the microphone, and the like.

Additionally, to avoid feedback problems, the special client software turns off the playback control. For those sound blasters with AGC, the special client software will turn on the AGC setting when appropriate, as well as other special settings (e.g., boost).

The special client software takes control of the volume control slider and moves it all the way up to maximum. In some cases, however, audio clipping may be a problem due to the presence of ambient noise. If so, the special client software may move down the volume control slider and then subsequently alert the user to retransmit the data from the electronic card. In one embodiment, a test may be performed with a sample audio file. During the initialization phase, the special client software asks the user to transmit a sample data. By

IPR2025-01150
Apple EX1071 Page 660

pressing the TX switch in the electronic card, a sample audio file is transmitted. Based on the reception quality of this sample audio file, the special client software adjusts the volume control setting that allows proper recording while minimizing the negative influence of ambient noise.

For the sound card memory allocation, the special client software sends a request to the sound card driver in the PC to allocate memory. The memory has to be substantial enough to hold the audio data. In a typical sound card, 8 MB are available in the buffer. Usually, not all of this memory is needed. However, in some applications, many seconds of audio need to be recorded. As an exemplary number for the amount of memory used, approximately 1 MB is needed to record 10 seconds of audio.

In one embodiment of the sound card, assume that the special client software needs about 1 MB of memory to record 9-10 total seconds of audio. The sound card driver divides the 1 MB of memory into 36 buffers, where each buffer holds approximately 250 ms of audio data. When any buffer is filled, the sound card driver sends the audio data in that buffer to the special client software.

For two-way embodiments, a test with a sample .wav file is done to determine whether the electronic card can receive data properly. The special client software includes a sample audio .wav file. After the memory is allocated by the sound card, the sound card driver sends a pointer to a buffer location. The special client software then sends the sample .wav file to the buffer location specified by the pointer. The sound card then plays the .wav file through its speaker(s) while the electronic card receives this audio sample. If the expected audio sample is received and properly decoded in the electronic card, then the electronic card generates an audible beep to indicate that the test was successful.

Typically, these initialization settings are made upon launch of the special client software. When the electronic card transmits the data to the PC, the special client software processes this data. After processing this data, one embodiment returns the PC back to the initialization state where it waits for additional data transmissions from the electronic card. Thus, the special client software is active (usually as a tray application on the desktop) and the sound card is optimized for electronic card-to-PC communications until the application is closed.

In another embodiment, however, the special client software restores the default mixer settings. As mentioned above, the special client software stored the mixer control settings prior to adjusting them for the electronic card. If the user needs to use the electronic card again, he enables the initialization routine to start over again for the mixer control settings and the sound card memory allocation.

4.3 BASE STATION TRANSMISSION SOFTWARE

The primary purpose of the base station transmission software is to generate the data stream shown in FIG. 5(B). The data portion of the data stream can be instructions, flags, and pure data for storage (e.g., coupons). For the most part, if sound is utilized, a conventional audio file (e.g., .wav file) is played by a software audio player as is known in the art.

In some cases, the data is transmitted from a computer system via the speakers. The special client software packages the data to be transmitted, whether the data is locally available or downloaded remotely from a website, and transmits them. The transmission involves the playing of the audio .wav file. Thus, the

IPR2025-01150
Apple EX1071 Page 661

packaging of the data to be transmitted can be as simple as locating the relevant audio file in memory and playing that audio file via the speakers.

In other cases, the data is transmitted from a TV or radio set. Today's television sets and radios are fairly passive and dumb devices; that is, they merely broadcast what they have received from the conventional TV/radio stations or the cable infrastructure. Accordingly, the transmission software is installed in the location where the coupon data is mixed with the programming. This may be the headend or even the network program source in the cable infrastructure. Once mixed, the coupon data (whether audible or ultrasonic) and the regular TV/radio program travel through the normal channels to the user's TV or radio set. Thereafter, if the TV or radio set is on, it transmits the data stream of FIG. 5(B) via acoustic waves, where the coupon data is found in the data portion of the data stream.

4.4 BASE STATION RECEPTION SOFTWARE

When any sound is emitted by some sound source, whether or not the sound source is the smart card of the present invention, the microphone on the computer (computer 14 of FIG. 1) may pick up that sound. If the sound complies with the data stream format of FIG. 5(A), the special client software 114 (FIG. 11) can process it and extract the data therein. If, however, the sound is unrecognizable (or is otherwise noise) to the special client software 114, it ignores it. Generally, the special client remote access software 114 in the PC receives a signal, determines whether the signal is proper, and if so, performs digital signal processing on the signal and decodes it. Based on the decoded signal, the special client software 114 can perform many functions such as open a web browser to a specific web page, fill out a form, redeem a coupon, and otherwise automate previously manual operations.

In one embodiment, the base station is a personal computer that is connected to the Internet. FIG. 13 shows a flow chart of one embodiment of the reception software portion of the special client software 114 (FIG. 11). In FIG. 13, the process begins at step 130. At step 131, the software initializes the sound device (e.g., "Sound Blaster" sound card) and optimizes the mixer settings. Here, the software allocates enough memory in the sound device to properly receive all the data. In one embodiment, it allocates 1 MB of memory, which allows for approximately 10 seconds of sound. It also checks to make sure the microphone is on (if it's off). The recording volume is initially set at the highest level. In some cases, however, if the recording volume is too high, signals will overflow the system and data may be lost. In other words, clipping may occur because of ambient noise. In this case, the software will readjust the recording volume slider to suitable levels. If the recording volume is too low, weak signals may not be detected. To avoid feedback, the playback mic control is turned off. In some sound devices, an automatic gain control (AGC) feature is provided. In this case, the software turns on the AGC.

After the initialization step, the PC is in a "waiting for signal" state at step 132. As mentioned before, in accordance with one embodiment of the present invention, the signal is in the form of a Frequency Shift Keying (FSK) signal. At step 133, the software performs the detection operation. The detection of the FSK signal involves two distinct operations – multi-rate processing and signal detection. In multi-rate processing, the signal from the A/D converter (from the sound device) is high pass filtered and downsampled while

IPR2025-01150
Apple EX1071 Page 662

preserving the range of frequencies in which the received signal is assumed to occupy. This stage is used to restrict the attention of the detector to a narrow band of frequencies in which the received signal may or may not be present.

The problem of detection is to determine whether a transmitted signal is present in a background noise environment. Assuming noise is gausian in nature, one technique is to correlate the received signal with the specific expected wave. The output of the correlator Z[n], can then be compared against a threshold to decide if signal is present. The test is

$$Z[n] = \sum_{m=0}^{\infty} h_{mf}[m] y[n-m] \underset{H0}{\overset{H1}{\gtrless}} \eta$$

y[n] is the received signal. $h_{mf}[n]$ is a matched filter (usually a sinusoid for FSK transmission). H1 is the alternate hypothesis (signal present), and H0 is the null hypothesis(no signal present). The test threshold η is a value determined to minimize the probability of false alarm, while maximizing the probability of detection. This maximization is determined directly from the distribution of the test statistic Z[n].

In practice, the frequencies and amplitudes of the FSK signals are not known a priori, with the result that a band of frequencies, corresponding to that band of frequencies defined by the range of error from the transmitting card, are scanned using Discrete Fourier Transform (DFT) banks and then subjected to Generalized Likelihood Ratio Tests (GLRTs), to establish the presence or absence of a signal given. A GLRT is used since the amplitude of the transmitted signal is unknown, and so is the estimated parameter in the test. The noise thresholds for the tests are generated from a delayed window of "noise only" data, where the decision "noise only" was made by the detector at an earlier time, or from the start-up default condition, where the noise statistics are estimated. Subsequent to statistical testing, the received signal is further established as valid if it contains the proper data format (see FIG. 5(A)) and spacing between frequencies f0 and f1.

Once the signal has been detected at step 133, step 134 decodes the signal. The decoding procedure considers each of the two FSK channels separately to draw conclusions about the transmitted data. Referring briefly to FIG. 14, the input detected signal is provided to two short term correlators – frequency f1 correlator 140 and frequency f0 correlator 141. Again, the notion of a test statistic is used, where the test statistics are generated by the two correlators. The hypothesis testing in this case is that between the alternate hypothesis (Signal present, power A0 in correlator 140 or A1 in correlator 141), and the null hypothesis (No signal present, power level E0 in correlator 140 or E1 for correlator 141). The testing between the two hypotheses in each channel can thus be understood to establish the received signal variance as being either A1 (or A0) over E1 (or E0) in correlator 140 (or 141) given a Gaussian distribution for each hypothesis and an equal probability that the received bit is a one or zero, that is, for correlator 140, the following test is used:

$$\frac{p\left(r/\sigma_{r/H_1}{}^2 = A1\right) \underset{H_0}{\overset{H_1}{\gtrless}} 1}{p\left(r/\sigma_{r/H_0}{}^2 = E1\right)}$$

IPR2025-01150
Apple EX1071 Page 663

This two-pronged approach for making bit decisions is necessary since the received FSK signal may be subject to echoes, a phenomenon that affects each channel differently. The advantage of making two decisions, one for each channel, as opposed to a single decision, based on a test statistic generated from testing the likelihood of one frequency (channel) over the other, is that when both channels disagree on the value of the received bit, one can use the ratios A1/E1 and A0/E0, as a means for favoring the decision of one channel over the other. That is, if one channel has a stronger echo, it is less reliable. It is also important to note that the quantities A0, A1, E0, and E1 are all time varying quantities, owing to the fact that card movement, even slight movement, can give rise to noticeable changes in echo and signal levels. As a result, these quantities must be tracked throughout the transmission. It should be clear that if the bit rate is Fb = 1/Tb, then the above procedure is performed exactly once every Tb seconds, where the optimal timing, that is, the point at which to sample in an interval Tb, is determined during synchronization and resynchronization.

The output of correlator 140 is provided to threshold 144, where the threshold is determined from the log-likelihood ratio test between zero mean Gaussian distributions having variances A1 or E1, under the alternate and null hypotheses, respectively. If the signal is greater than this threshold, then block 146 makes a decision that the signal is a logic "1" and updates A1 based on the the current output power from correlator 140, and using some averaging with the current value of A1. If the signal is less than this threshold, a "0" is established, and the value of E1 is updated based on the current output power from the correlator (140) and the current value of E1. Similarly, the output of correlator 141 is provided to threshold 145. If the signal is greater than the threshold determined from the likelihood ratio test that decides between the alternate hypothesis (variance = A0) and the null hypothesis (variance = E0), then block 146 makes a decision that the signal is a logic "0" and A0 is updated based on a weighted average between the current output from the f0 correlator (141) and the current value of A0. If the signal is not greater than this threshold, then a logic "1" is decided and E0 is updated. The signal is then provided to block 146 for the decision. Under most circumstances, we expect that the two LRTs (144 and 145) will make the same decision, agreeing that a "1" or "0" was received for a given symbol interval. In cases where the two disagree, then if this is due to echoes, we can establish the best decision based on that channel having less echoing, which is determined from the ratio E0/ A0 or E1/ A1. This final level of decision making is performed at step 146.

To summarize the decoding operation, each of the two channels is processed separately, with a threshold being both tested against and updated from the current observation. In the case where both channels make the same decision, a secondary test is provided which takes into account the signals when the channels are inactive.

Returning to FIG. 13, the decoded data is then stored and processed based on the application at step 135. The application may be simple form filling on a web page after the user purchases some merchandise. The application may be the automatic launching of the user's web browser and navigation to a particular home page. Also, the application may be the delivery of the data to a web site for processing at the server, such as when coupons are redeemed. The process ends at step 136. Normally, the special client software is always turned on in the background (i.e., application could be placed in the Windows "tray").

IPR2025-01150
Apple EX1071 Page 664

The detection operation will now be discussed in greater detail. One of the keys to implementing a recursive DFT rests on preserving the property of orthogonality between the frequencies in the DFT and ignoring the choice of phase, which itself is arbitrary. Phase is only significant in a relative sense; that is, phase exists between the frequency components in the received signal. If desired, this phase can be discerned in a recursive DFT scheme with a few additional operations. Accordingly, this allows for the extensions of this scheme to Phase Shift Keying (PSK) and Quarternary Phase Shift Keying (QPSK), as well as the generalizations of these procedures.

Referring now to FIG. 15, a portion of the digital signal processing scheme is shown. Several DFT banks 150 are provided to perform the DFT operation on the received signal y(t). The DFT banks are necessary because of the inherent inaccuracy (i.e., due to small clock error) of the smart card in generating the FSK signals. If one knew the FSK frequencies (e.g., f0 and f1), then the entire detection process would be one of correlating along f1 and f0 and searching for a particular pattern or bit stream on which to synchronize using some type of statistical test as a criterion for acceptance. Because of the lack of a precise knowledge of the transmitted frequencies, the data format of the smart card includes a preamble. Referring briefly to FIG. 5(A), the preamble includes the two frequencies f0 and f1, where these two transmission intervals are sufficiently long to estimate each of the two FSK frequencies precisely. The known bit pattern is then used for synchronization. The reception software in the computer identifies the correctness of the received frequencies by their spacing (f1-f0), durations, and energy relative to the ambient noise level.

Since the smart card's clock error is consistent, identifying one variable leads to the simple calculation of the other variables; that is, the variables f1, f0, and T (symbol duration) have one degree of freedom which is the specific clock error in the smart card.. Thus, assuming that the duration of each frequency is sufficiently long, and that the energy over the given interval exceeds the threshold specified by the GLRT, then the symbol interval T can be recovered from the F1 and F0 intervals, as depicted in FIG. 5(A). With the symbol interval in hand, synchronization can be performed by using the delay line 152 in FIG. 15 along each of the corresponding frequencies f1,f0, according to their respective indices in the DFT bank 150, and with the aid of the known bit stream FIG. 5(A).

After the highpass filtering and downsampling, the frequencies of interest are located in the narrow band of 0-2kHz. The bit rate for the signal in this system is 200 bps in one embodiment, which is a symbol period of 5 msec long (T_{symbol}=1/200 bps). The downsampled rate is approximately 5 kHz (4.9=44.1 kHz/9, where 44.1 kHz represents the sampling rate of the sound card in the PC and 9 represents the downsampling factor). At this downsampled rate, approximately 25 samples are taken in one period (5 msec) of the received signal.

For practical purposes, the 0-2kHz narrow band is divided into 13 (which is approximately 25/2) bands to assist the software in determining the actual frequency of the received signal. Accordingly, the DFT banks 150 include 13 separate banks, where each bank is focused on one of these narrow bands. In effect, each bank or bank channel determines how much of the received signal is directed along the frequency the bank channel is

IPR2025-01150
Apple EX1071 Page 665

associated with; that is, how much the given bank channel frequency (e.g., w_0) contributes to the received signal.

Because the bit rate for the system is 200 bps in one embodiment, the DFT window in the DFT banks is 5 msec long (T_{symbol}=1/200 bps). Referring briefly to FIG. 16, the DFT window 167 is 5 msec long. Within the DFT window 167 are several sampled points, such as samples 160, 161, 162, 163, and 164, although in FIG. 16, each DFT window is not associated with 25 sampled points for the sake of clarity in the illustration. The 25 points in DFT window 168 are used to generate the 13 DFT coefficients for the particular embodiment as specified by the 44.1kHz sampling rate, 200 bit per second transmission, and downsampling factor of 9. Since the signal being analyzed is real, the spectrum has conjugate symmetry, and it is therefore sufficient to analyze only half of the signal's total bandwidth. Having the DFT in window 167, we can proceed to compute the DFT in window 168 recursively in the following manner.

Fundamentally, recursively computing the DFT comprises the moving correlation between a given complex exponential $e^{jk\omega_0 n}$ with the received signal x[n]. This quantity is denoted by $\hat{a}_k[n]$ such that:

$$\hat{a}_k(n) = \frac{\sum_{m=n-N+1}^{n} e^{jk\omega_0 m} x[m]}{N}$$

Defining the intermediate variable $\hat{x}[n]$ such that $\hat{x}[n] = e^{jk\omega_0 n} x[n]$, the quantity $\hat{a}_k[n]$ is a moving average of the quantity $\hat{x}[n]$, and hence can be written in the form:

$$\hat{a}_k[n+1] = \hat{a}_k[n] + \frac{\hat{x}[n+1] - \hat{x}[n-N+1]}{N}$$

Note the change in lower bound from N to N+1, as in the lower bound on the sum defining ak[n], which is termed the sliding DFT coefficient. Note that the difference

$$\hat{x}[n+1] - \hat{x}[n-N+1] = x[n+1]e^{j\frac{2\pi k(n+1)}{N}} - x[n+1-N]e^{j\frac{2\pi k(n+1-N)}{N}}$$
$$= (x[n+1] - x[n+1-N])e^{j\frac{2\pi k(n+1)}{N}}$$

so that the DFT coefficient $a_k[n+1]$ is simply updated from $a_k[n]$ by generating the difference between the newest and oldest samples, and adding to the real part of $a_k[n]$ this difference times the cosine of 2π k/N.

IPR2025-01150
Apple EX1071 Page 666

Similarly, the imaginary part of $a_k[n]$ is updated by adding the product between the difference (x[n+1]-x[n+1-N]), scaled by the reciprocal of the window length N, and the sine of 2π k/N.

With this recursive formulation, the kth DFT coefficient $a_k[168]$ for DFT window 168 can be computed from the kth DFT coefficient $a_k[167]$ from DFT window 167 by determining the difference between sample 165 and sample 160, and updating the real part of $a_k[167]$ with this difference times the cosine of 2π k*168/N, and similarly updating the imaginary part of $a_k[167]$ by multiplying the difference between sample 165 and sample 160 with the sine of 2π k*168/N.

Another recursive form for DFT is given by expressing the DFT window as the impulse response

$$h_k[n] = \sum_{m=0}^{N-1} e^{j2\pi \frac{k(N-1-m)}{N}} \delta(n-m)$$

This representation has z-transform

$$H(z) = \sum_{m=0}^{N-1} e^{j2\pi \frac{k(N-1-m)}{N}} z^{-m}$$

$$= e^{-j2\pi \frac{k}{N}} \frac{1-z^{-N}}{1-e^{-j2\pi \frac{k}{N}} z^{-1}}$$

which yields the recursion formula

$$a_k[n] = e^{-j2\pi k/N}(a_k[n-1] + x[n] - x[n-N])$$

Note that this recursion formula requires twice as many operations as the first recursion.

Returning to FIG. 15, the output of the DFT banks 150 is a block 151 that calculates the magnitude of the received signals for each channel. These values are then provided to delay lines 152, which is slightly longer than the data stream by a factor of 3/2. The delay lines store the values output from the magnitude block 151.

Concurrently, an additional delay line 153 is provided. This delay line takes in input y(t) to make a calculation of the noise variance. The noise variance is actually calculated in the Auto-Regressive block 154. The delay through 153 of FIG. 15 is sufficiently long so that the variance estimated at the output of 153 in the AR block 154 is from a period of time considerably earlier than the data in the correlator bank 150 of FIG. 15 and the delay lines 152 of FIG. 15. This means that since the detector is currently searching for a signal, that

IPR2025-01150
Apple EX1071 Page 667

earlier period whose power is evaluated in 154 of FIG. 15 must be a period deemed 'noise only.' Hence, the statistics so computed are enough to specify the threshold η of the Neyman-Pearson test on Z[n], described earlier.

The bank channels having maximum energy are then found in the delay line 152, according to the F1-F0 format described in FIG. 5(A). Since the sequence F1-F0 is transmitted first, these signal are the oldest in the delay lines, or the furthest back in 152 in the direction of the arrows. These selected bank channels are then compared to the calculated noise threshold to decide whether they are signal or noise, and also to each other to make sure that the proper frequency separation is present. Once these tests are passed, the detector has now determined the two bank channels that correspond to f0 and f1, or certainly close enough for decoding purposes.

Once the f0 and f1 frequencies have been determined with the f0 and f1 signals, the detector can now focus on synchronization. For the synchronization bits, the detector is programmed to know the particular pattern. If the pattern is 01010101, then the detector starts at a column in the delay lines 152 of FIG. 15 (where the frequency index denotes a row in the delay line 152) that corresponds to the point immediately after the location of the frequency identification intervals, F0 and F1, and alternately sums the values from the two selected banks, corresponding to f0 and f1, in step sizes of T, corresponding to the estimated symbol interval as estimated from F0 and F1. For example, the detector starts with the first bit, "0", which is the first symbol received, and so is the oldest on the delay line. The detector takes the value from the selected bank channel assumed to correspond to f0. The detector then proceeds to the next bit, "1", with location offset from the point previously taken from f0 by T samples and in the direction of the most recent sample, or towards the DFT bank, and adds this value from the f1 bank to the previous value. The detector continues with this 01010101 pattern until it has summed, for each value in the bit stream, the corresponding channel magnitude, with each such element separated from the previous by symbol interval T. Since this sum is a function of the offset from zero time, where zero time denotes the point where the energy in the first synchronization bit exceeds that in the last frequency identification bit, as in FIG. 5(A), we construct a cost function C[m], where m denotes the offset in samples from the zero time, and we define this first sum as C[0]. We write

$$C[n] = \sum_{m=0}^{M} b[m] f1[D - n - mT] + (1 - b[m]) * f0[D - n - mT]$$

where b[n] is the known preamble sequence, D is the offset from the output of the Magnitude device 151 to the zero time in 152, f1 is the delay line associated with frequency f1, and similarly for f0. Note that the sum moves from the oldest recordings of the 151 ouput towards the newest, in agreement with our understanding that the first bit transmitted will be the oldest recorded.

The detector now evaluates the sum C[1], which determines the sum of the delayed f0 and f1 correlator outputs offset by 1 sample from the previous sum, with the offset in the direction of the most recent sample, or in the direction of the DFT banks (opposite the direction of the arrows in FIG. 15). As before, the cost function C[1] is generated by alternately summing the magnitudes stored in the delay lines 152 of FIG. 15, spaced apart

IPR2025-01150
Apple EX1071 Page 668

by T samples, with the choice of frequency index f0 or f1 in the delay line 152 given by the corresponding value of the bit in the known bit sequence "0101010101".The detector now evaluates C[2], C[3], etc.. until it has evaluated at least T points, which is sufficiently long to determine a synchronization point.. When all the elements of C[m] are then compared to each other, one of the points is the maximum; that is, when these sums are plotted, the plot forms an upside down V pattern. The sum corresponding to the peak of this upside down V pattern is the synchronization point. From this synchronization point, one can in turn evaluate A0, A1, E0, and E1, which are the powers in each channel for one or the other of the two frequencies transmitted. Knowing the synchronization point on the received synchronization pattern, these quantities are directly calculated by taking advantage of the known (synchronization) data sequence.

The final issue to address is resynchronization, which bears sharp resemblance to synchronization. Based on the timing synchronization point K established from the maximum of C[m], the decoder will sample every T samples at points K+nT until the decoder reaches the 'stop' bit framing a given received byte. Since the "start" and "stop" bits are known, these bits are used to resynchronize much in the same way as the known synchronization sequence assisted in establishing the synchronization point K. In this case, however, rather than having many bits, there are only two, but conceptually the process is the same. A cost function is constructed from a point corresponding to the middle of the coming "start" bit. In this way, knowing that we are probably not off by much in terms of synchronization loss, we can sum the magnitude of the delayed "stop" bit with the current "start" bit, generate a cost function C'[m], and use the maximum as the new synchronization point K'. In some applications, an AGC can be introduced to the DECODING stage at a point prior to the f0 and f1 correlators to ensure that the resynchronization cost C'[m] always has the correct maximum by correcting the received signal in the presence of fading or weak signals.

In another realization, one can replace the auto-regressive noise power estimator 154 of FIG. 15 with a bank of autoregressive (AR) estimators which separately track the power in each of the frequencies analyzed by the bank 150 of FIG. 15. In this case, the delay line 153 of FIG. 15 can be removed, and the input to the bank of AR power estimators can be placed at the end of 152 of FIG. 15, after the delay line length of 152 is extended from L to accommodate the time required for the preamble duration and the time for the AR buffers in the new frequency - power estimation unit to fill with noise.

Interference Suppression:

The utility of estimating the noise power as a function of frequency, which is called the periodogram estimate, is particularly useful in the case where the background noise environment is colored. Classically, detection in the presence of colored noise amounts to preceding the detection mechanism with a prewhitening filter. When detecting frequencies, however, a whitening filter would translate to an increased threshold for those frequencies where the noise power is higher, and a reduced threshold at those frequencies with little noise power. This is in fact exactly how the spectrogram is used – thresholds are set at a frequency by frequency basis, where out of band interference can then be ignored. The cumulative effect of the periodogram estimate is then simply to replace the previous estimate of the threshold, for a given frequency, with the corresponding periodogram noise estimate for that frequency.

IPR2025-01150
Apple EX1071 Page 669

The advantages of this digital signal processing scheme are primarily threefold:

(1) The received signal may have a low signal-to-noise ratio since the DFT bank used for detection is essentially a bank of narrowband filters, improving the SNR per channel as compared with simple energy tests on the received signal. This is particularly important since the acoustic signals that are detected have very low amplitudes.

(2) The detector is practical to implement because of the application of the moving average concept to the DFT banks.

(3) The accuracy of the detector is close to optimal. The detector is a true matched filter.

In another embodiment, n-ary phase shift keying (nPSK) technique is used to decode the signals instead of FSK. In this scheme, the delay lines or channels at the output of the DFT bank, select one of the channels based on magnitude. Having selected the best bank, estimate the phase shift by processing the I-phase component and the Q-phase component of this bank. The offset determines whether the transmitted data is a "1" or "0".

4.5 CONCURRENT OPERATION OF MULTIPLE RECORDING SOFTWARE

In some computer systems, the operating system does not allow more than one recording software to operate at any given time. One such group of operating systems is Windows 95/98/NT/2000. If Windows allocates resources in the sound card for a particular commercial recording software, the special client software 114 (in FIG. 11) in accordance of the present invention may not work properly. After all, the electronic card and the special client software need the sound card in the PC to capture the audio signals for electronic card-to-PC transmissions and to generate the audio signals for PC-to-electronic card transmissions.

Assuming that the commercial recording software was installed first, Windows dedicates resources for that software in the sound card. Any other recording software that is installed later may not be recognized by Windows. Of course, if the special client software 114 (in FIG. 11) in accordance with the present invention is installed first, then the electronic card-special client software will work properly. The later-installed commercial recording software may have some problems working properly.

Of course, the user could manually unlink the commercial recording software from Windows to make the special client software work properly, but this is a cumbersome and annoying task. Furthermore, if some bug in the first-installed commercial recording software is present, the sound card in the PC would be locked and the special client software 114 (in FIG. 11) cannot function.

In accordance with one embodiment of the present invention, a special driver would be written and placed between the current driver and the Windows Multimedia interface. Referring to FIG. 43, several applications 430, 431, 432 are installed in the computer station, which in this example is a PC with a Windows operating system. One of the applications is the special client software 114 that can communicate with the electronic card of the present invention.

In order to access the sound card 438, these applications use the Windows Multimedia interface 433. Normally, the Windows Multimedia interface 433 communicates directly to a driver 437 to access the sound card 438. In one embodiment of the present invention, a special driver 435 is written and is placed between the

IPR2025-01150
Apple EX1071 Page 670

Windows Multimedia interface 433 and the driver 437. The API 434 of the special driver 435 is a copy of the API 436 of the driver 437. This special driver 435 is installed instead of the current default driver 437. But the special driver 435 uses the default driver 437 for normal operation. The special driver 435 also changes some of the recording parameters for the special client software 114 to function properly. Note that some of the processing can be done in the driver level, where the invention's "driver" layer will perform the processing.

In operation, when an electronic card signal is detected by the sound card 438, the driver 437 presents the data to the special driver 435. Some byte of data in the electronic card transmission will be provided to let the special driver 435 know that this data is for the special client software 114 and not the other recording applications. Of course, some decoding logic would be provided in the special driver 435 to decode this byte in the electronic card transmission. Once decoded, the special driver 435 processes this data for the special client software 114, while preventing other applications (such as application 430) from taking control. In effect, the special driver 435 convinces Windows Multimedia interface 433 that the current recording channel is no longer valid. Then, the special client software 114 accesses Windows Multimedia interface 433 for its own needs. This way, the special client software takes control of the sound card 438 without crashing the other applications in the computer system.

In another embodiment, as shown in FIG. 44, the special client software 114 interfaces directly with the special driver 435 instead of indirectly through the Windows Multimedia interface. The special client software 114 "steals" the appropriate handles that are used by another application (e.g., application 431) so that the electronic card-special client software communication can take place via the sound card 438. As known to those ordinarily skilled in the art, Windows provides handles of Windows Multimedia interface 433 to the relevant application. The relevant application uses the handles to have Windows Multimedia interface 433 perform various tasks.

4.6 SERVER-BASED PROCESSING

In the above description of the base station, special client software is resident in the client to perform such tasks as digital signal processing, data processing, performing some web-related action, and communication with selected web servers. Typically, all the necessary functionality are found in the special client software. In some cases, however, the software needed to perform some functions is downloaded from a designated server on an as-needed basis. In other words, the special client software in conjunction with a particular supporting web server determines whether a particular functionality is available in the client. If so, then the user goes about his business to conduct any transaction or otherwise communicate with that web server. If not, the special client software downloads that functionality from that web server so that the user can employ this functionality with this web server.

In another embodiment, the server contains all the functionality described above for the base stations to process the acoustic signals and perform the designated action based on the data in the signals. The client contains only the necessary software to record sounds and deliver those recorded sounds to any designated server. The server would then playback the recorded sounds and digitally process the signals to extract the data therein (if any). Thus, instead of processing the signals and communicating the data to the web server, the

IPR2025-01150
Apple EX1071 Page 671

client merely records the sounds and delivers them to the server. The server itself performs the digital signal processing operation, data processing operation, and the requisite action.

In this embodiment, the client software contains two main features: (1) recording, and (2) communications. The first feature allows the user the record the acoustic signal that is emitted when the user presses the button on the electronic card. The second feature allows the recorded signal to be delivered to a default designated web server to process the signals for authentication. The default designated web server would be contacted if the user did not already launch his web browser or the web browser has accessed a web page that does not support the electronic card and its communications protocol in accordance with the present invention. If, however, the web browser has already been launched and the user has accessed a page that supports the communications protocol of the present invention, then the communications component of the client software would interface with the web browser to deliver the recorded sound to that particular web page's web server.

Typically, when the web browser accesses a web server (i.e., web page) that supports the communications protocol of the present invention, the web server would send a code (or embedded data in the header) along with the html data that only the client software can interpret. It functions like a flag. When this code is detected by the client software, the recorded audio file can be delivered to this web server. If the code is not detected (i.e., this web page does not support the communications protocol of the present invention), then client software sends the recorded audio file to the default server.

5.0 APPLICATIONS

The spectrum of applications covered by the various embodiments of the present invention is broad. Referring to FIG. 46, at the core of the various applications is the electronic card 460 itself, whether in one-way or two-way form. As a receiver of information, the electronic card 460 can receive all kinds of information from simple facts to coupons, discount offers, promotional offers, and incentive points. The reception of information occurs via some electronic device 461, such as a broadcast media (e.g., TV, radio) or a personal computer.

The received information can be in two forms -- (1) embedded information, or (2) actual content for later pattern recognition. The embedded information can be some code that complies with the communications protocol of the present invention. Exemplary embedded information can be actual synthesized sounds that are generated as part of the broadcast program, code that was mixed in later at some point in the distribution chain of the broadcast program, and an audio file that is played on a website.

For the reception and processing of actual content, no communications protocol need to be followed since the electronic card is recording the actual sounds (whatever they may be) that emanate from the speakers of the TV, radio, or computer system. Later, the user can playback his recording where some pattern recognition server will attempt to match that sound clip with one of the soundtracks stored in its database. When a match is found, the server will identify the sound clip, provide links associated with the sound clip, or automatically redirect the user to a relevant website associated with that sound clip. This pattern recognition feature is particularly valuable when the user has limited or no access to the Internet at the moment that the user

IPR2025-01150
Apple EX1071 Page 672

hears the sound. By recording that sound at that moment, he can later get more information related to that sound clip.

Based on the type of information received (and saved), the electronic card 460 can be used to exploit this information. Thus, if the information received is a coupon, the electronic card 460 can be used to redeem this coupon either online on the web or at a conventional bricks-and-mortar store.

As a source of information, the electronic card 460 allows the user to perform various acts with the mere press of a single button. The button press can launch applications or functions as represented by reference numeral 462, authenticate the user into a website or server as represented by reference numeral 463, or perform other acts 464 within a service once the user has successfully accessed and been authenticated into a service.

For the launching action 462, the press of the button initiates such things as launching an application (e.g., web browser), accessing a particular website (e.g., buying club, travel service (airline, car, hotel), online account service, online banking, and proprietary service such as America Online), or accessing some service that requires telephone dial-in. In this launching action, no authentication is necessary since the user is merely accessing services that are publicly available but in a way that is more efficient and user-friendly.

For the authentication action 463, the press of the button on the electronic card 460 enables the user to securely log into various services S_1, S_2, ... , S_N, whether these services are accessed over the web or via a telephone number. Thus, instead of arduously entering ID and password information, the electronic card 460 simplifies the process by performing the login functions for the user without compromising the security concerns of these services. Exemplary services include an online trading service, a private intranet, a proprietary database, a remote desktop, a remote hard drive service, a web-based email service, or a music collection service. The list of services, whether commercial or personal, is long and can be anything that requires some authentication action to allow the user to access the contents therein. The authentication would be needed because the service contains personal or otherwise private information that need to be securely protected, or the service is commercially motivated to limit access to paying users.

Once the user has successfully been logged into a service (accessed and authenticated), the user can use the electronic card 460 to perform other actions with the press of a button. These actions can be as simple as filling out a purchase form at the checkout line to purchase some merchandise at an online store. For more sophisticated operations, the press of the button on the electronic card 460 may involve detecting the context of the user's current online experience and taking some action based on this context. Thus, this context-sensitive feature can intelligently detect what the user wants to do based on which web page his was viewing at the time he pressed the button. One example of this type of action is the e-wallet 464 which simplifies the user experience at various merchants' websites M_1, M_2, ... , M_N.

In another embodiment, the authentication action 463 follows immediately from the launching action 462. Thus, although FIG. 46 shows two arrows directly flowing out of electronic card 460 into launch 462 and authentication 463, this alternative embodiment would show only one arrow directly flowing out of the electronic card 460. This one arrow would point to launch 462, which would point to the authentication action 463.

IPR2025-01150
Apple EX1071 Page 673

Importantly, these applications require no infrastructure changes. Existing sound systems in personal computers work with the electronic card.

5.1 BROADCAST MEDIA

One embodiment of the present invention is the user of the electronic card to download (and later redeem) coupons via broadcast media (e.g., television, radio). For the moment, the manner in which the coupons, targeted sales offers, special discounts, sales information, and the like are delivered to the broadcast media devices such as televisions and radios will not be discussed. Hereinafter, the term "coupon" or "coupon data" will be used to refer to these various sales offers. Thus, the electronic card 10 can receive coupons from a radio/stereo system 11 via sound waves 19w; a television 12 via sound waves 19x; a personal computer 14 via sound waves 19y; and a conventional non-web store 13 via sound waves 19z. To receive these sound waves, the electronic card 10 contains a transducer for converting the received sound waves into electrical signals for digital signal processing. The electronic card 10 is placed near the speakers of these broadcast media devices, computer speakers (such as speakers 14a and 14b), and speakers at checkout counters in conventional stores. Although the speakers generate the actual sound waves, the source of the sound waves (and the data therein) is located at key locations in the television/radio infrastructure (e.g., headend of a cable service), web infrastructure (e.g., web site), and the conventional store office (e.g., network server in the back room of a department store).

Once the coupon data has been received and stored in the electronic card 10, it can be redeemed in any number of ways. In one embodiment, the user of the electronic card 10 can use a web browser (e.g., Microsoft Internet Explorer or Netscape Navigator) in his personal computer 14 to access the Internet 16 via his Internet Service Provider (ISP) 15. Once on the Internet, the user can access any web merchant's web site 17 or web portal 18. Having located and accessed the web merchant 17 or web portal 18 that is sponsoring the coupon that he just downloaded, the user would then go to the web page that contains the coupon redemption information. Such a web page can be the home web site of the web merchant, or it could be merely a button on the web page that says simply, "Click here to use your electronic card coupon." When the user clicks on the button, the server associated with the web page would send an audio file (e.g., .wav file) to the web browser. The web browser would interact with the sound card in the computer 14 to play the audio file. The electronic card would receive the sound waves generated from the speakers 14a, 14b of the computer 14, process them along with the already stored coupon data, compare them to make sure that the proper coupon data is stored in the electronic card 10, and if the coupon data is proper, the electronic card 10 would generate a password on its LCD. The user enters the password manually on the keyboard and submits it to the web site. Then, depending on the type of coupon that the user previously downloaded into his electronic card, the web site could apply the coupon to the user's purchase or award a merchandise for free. This is just one of the many ways in which the user could use or otherwise redeem his coupon in his electronic card 10. This and other ways of redemption are detailed below.

An alternative option is that the customer will not need to remember the merchant's web address. The web address will be stored as part of the coupon data. The user would simply access a central homepage, press

IPR2025-01150
Apple EX1071 Page 674

the button on his card, and the card will transmit the data (two-way card) and the browser will direct him automatically to the merchant's web page. In fact, the web address may even direct the user to the exact product with the discount already in place. To save space and communication time, instead of full webpage addresses, the coupon will contain a coupon ID which will be interpreted at the central homepage. A second option will be to use a tray application that always listens and does the job of the central homepage (selection of coupon and redirection). In addition, using the same pattern recognition method described below, the coupon could be a recorded part of the commercial which will then be associated and detected in the central web page.

If the user stored multiple coupons, the browser will ask him which one to use and he will make his choice either via clicking or via the keyboard/mouse. These and other embodiments will be described further below.

5.1.1 BROADCAST MEDIA INFRASTRUCTURE

One embodiment of the present invention allows coupons to be downloaded from the television/radio infrastructure to a user's electronic card 10 (see FIG. 1). The manner in which the coupon can be redeemed varies from application to application. First and foremost, a brief discussion of the television and radio infrastructure will be provided.

Cable television systems are well known. As shown in FIG. 23, these systems are usually comprised of a headend 170a with one or more trunk lines 172a-172c extending therefrom, where each trunk line has a plurality of feeder lines 173a-173c extending therefrom into subscriber areas. Each subscriber 174a-17 is attached to a feeder line via a line tap onto the feeder or service line.

If the distances between the headend and subscriber areas are substantial, intervening distribution hubs 171a-171c may be located along the trunk lines to replenish the strength and quality of the signal transmitted to the subscribers. Distribution hubs simply act as small headends and exist to ensure the quality of delivered signal in large CATV networks. Each distribution hub may, in turn, be coupled to a plurality of service sites by feeder lines. Each service site may have one or more service lines extending therefrom to couple a plurality of subscribers to the service site.

In this cable network, a transmission signal is provided by the headend 170a over the trunk lines 172a-172c to the distribution hubs 171a-171c or service hubs. This amplified signal is then provided to the feeder lines 173a-173c extending from the distribution hub or service hub to provide the signal to the service sites. Taps located at each subscriber site bring the transmission signal into a subscriber's site.

The transmission signal from the headend 170a may include entertainment signals and data signals. The entertainment signals may be received as broadcast signals received via satellite 179 from an originating location. This originating location may be another headend 170b. This originating headend 170b receives its signals from channel or program sources 175a-175c. These channel or program sources 175a-175c may be HBO (i.e., Time Warner), TBS, ESPN, ABC, NBC, CBS, PBS, or even the Food Network. It is also possible for the channel or program sources 175a-175c to have a direct link to headend 170a (instead of headend 170b) if these channel or program sources are located reasonably close so that a satellite link is not necessary.

IPR2025-01150
Apple EX1071 Page 675

At the headend 170a, the policies and business strategies dictate which of the many programs the headend 170a receives from the headend 170b will be rebroadcast to the subscribers and on which channels. Each subscriber area may receive a different set of channels and programs as determined by the headend 170a. Of course, the subscriber also controls which of the available channels he receives based on his subscribed service.

Each broadcast signal is placed on its own channel within the spectrum of the trunk, feeder and service lines used in the CATV system. The spectrum of the lines coupling the CATV system together is the range of frequencies supported by the communication conduits used for the lines. In a typical CATV system, this spectrum is divided into a transmission portion and a return portion. The return portion of the spectrum may be used to support data transmissions, telemetry, and/or control information from subscriber sites back to the headend. The data transmissions from subscribers typically include status information about the subscriber's equipment which may be used by components at the headend to ascertain the status of the cable system or subscriber equipment.

Referring now to FIG. 24, the conventional broadcast television and radio infrastructure is somewhat analogous. A user 185, among many users, has a TV antenna on the roof of his house. With the antenna and the TV inside his house, the user can receive broadcast TV signals from a number of TV station transmission towers 183a-183c, if these transmission towers are reasonably close and are transmitting at a suitable power. These transmission towers 183a-183c are associated with local TV stations 181a-181c.

Typically, each TV station is affiliated with one of the major networks – NBC, CBS, ABC, PBS, Fox, or WB. By being affiliated with one of the networks, the local TV stations can broadcast network programming during prime time (usually 8 PM to 11:00 PM), late night (11:30 PM to 1:30 AM), daytime (e.g., soap operas), and certain other designated time periods (e.g., weekend sporting events). In addition, these local TV stations can broadcast locally produced programming such as local news, local sporting events (e.g., high school or local college), and local events (e.g., downtown Christmas parade). Finally, these local TV stations can broadcast syndicated programming at various desired time slots. These syndicated programs can be reruns of popular TV shows (e.g., MASH, Cheers, Star Trek), currently produced game shows (e.g., Jeopardy, Wheel of Fortune), or the lengthy infomercials, among others.

Usually, the TV stations 181a-181c receive non-locally produced programming from a network or programming source, such as source 184. If the distance is great, a link with a satellite 186 is needed. Typically, each local TV station would have its own satellite dish and receiver to receive these non-locally produced programming from the source 184. In other cases, a distribution center 180 is provided with a satellite dish and receiver which then delivers the programming to the appropriate local TV station 181a-181c via lines 182a-182c. Typically, the distribution center 180 is associated with a particular network (e.g., NBC) to serve several nearby local TV stations who are also affiliated with the same network but which serve different local regions (with some overlap).

The infrastructure for radio stations is similarly structured as shown in FIG. 24. Thus, a radio station 181a has local programming as well as network programming and syndicated programming (e.g., Howard Stern

IPR2025-01150
Apple EX1071 Page 676

Show). The non-locally produced programming are received from the network or program source via satellite. The locally-produced programs originate from the radio station itself normally. The user 185 has a radio/stereo system with speakers and an antenna.

5.1.2 BROADCAST MEDIA COUPON TRANSMISSION

A coupon is a sales item that a merchant distributes to the mass public or a limited set of the mass public (i.e., targeted consumers) to promote his store (web or otherwise), product line, service line, or other business. The hope is that after redemption of the coupon, the consumer will like the product or his "visit" to the store just enough so that the consumer will buy that coupon or visit that store again. With this initial step, the merchant hopes to breed brand or store loyalty with this consumer. Usually, coupons are found in print media (e.g., newspapers, magazines) or on ad banners in certain web pages. But, as mentioned above, coupon distribution via the print media or the Internet is inefficient and ineffective.

Use of a special card that simply records time slices of sound for playback to a centralized pattern recognition server that correlates each slice to a coupon is discussed more fully below. But in circumstances where a more brief and reliable way of communicating coupons is desired, or in information environments that are too data rich for convenient implementation of a pattern recognition server, another method of communicating coupons to a card from an ordinary television, radio or sound device will now be discussed.

In accordance with one embodiment of the present invention, coupon data can be either in the audible frequency range or ultrasonic range. These data are mixed with normal programming so that when the user is watching TV or listening to the radio, he can collect coupons in a relatively simple manner. The television or the radio set itself is a passive device; that is, it receives electromagnetic signals, demodulates them, and presents the information in the signals to the user via the TV screen and speakers. Thus, the TV set or radio set itself does not generate any coupons; rather, it merely presents what it receives from the program/channel source.

Accordingly, the coupon data are mixed at a point somewhere along (and including) the communication path between the network/channel/program source and the user. Taking the exemplary cable infrastructure illustrated in FIG. 23, the coupon data can be generated with the program at the program source, such as program source 175a. In one example, the studio that makes a particular movie or TV show can "place" a coupon into the plot of the show. Much like product placement, the producers of the TV show could, for example, create the data stream (see FIG. 5(B)) by electronically synthesizing it. In this example, this synthesized data stream is audible. During the making of that TV show, an actor could announce on-air, "Please take out your XYZ card to receive a free gift or coupon. In just a few seconds, the coupon will be delivered to you." A second method will be to show a special visual mark at the corner of the screen at the beginning of the commercial and remove it when it is over. At this point, the audible data stream is played. This is recorded as part of the show. Of course, the context of the TV show is such that this announcement will not seem out of place or inappropriate. The TV show could be a home shopping network or a standard sitcom. When this TV show, which was recorded sometime in the past, is finally broadcast on TV, and the user watches it, he will be able to download the coupon at the proper time. So, when the scene where that actor makes that

IPR2025-01150
Apple EX1071 Page 677

coupon announcement is shown, the user merely points his electronic card to the TV speakers and receive the audible data stream for storage in his card. The user now has the coupon or gift in his electronic card. Of course, only those users with the electronic card can interact with the TV in this manner to receive this coupon. In this case, the coupon is provided within the show itself and therefore, no mixing of the data stream with the audio tracks is necessary.

In an alternative embodiment, this embedded audio data could be played repeatedly throughout the broadcast of this show so that the user need not time his recording precisely. Thus, whenever this show is on, the user could record a portion of the broadcast and since the embedded audio data is looped over and over again, the user is assured of capturing this data in his electronic card.

For the most part, however, the merchant of the coupon do not want to be indelibly linked to a TV show, radio show, or movie forever. In this case, the data stream containing the coupon data is mixed with the audio tracks at another point in the broadcast link. If the merchant has some agreement with a channel or network source, such as HBO or CBS, he can ensure that his coupon his placed with certain shows for a certain time period. If the merchant's agreement runs for one year, he may specify that every episode of CBS's "60 Minutes" for the coming year should air the merchant's coupon at some specified time. Although "60 Minutes" is produced like always, the CBS channel source that is responsible for distributing the show to its affiliates mixes the merchant's coupon data stream with the audio tracks of "60 Minutes". The CBS channel source also provides some visual indication of when the data stream will be played to alert the viewer to get his card out for the download. This show is then provided by CBS to the headend 170b (FIG. 23) which then delivers "60 Minutes" along with other programming to the appropriate headend 170a for regional distribution. When "60 Minutes" is finally broadcast on cable TV, the user merely takes out his card at the appropriate time (which is specified) and downloads the coupon.

Similarly, a merchant may buy certain 30 second or 1 minute commercial slots to be played during commercial breaks of a TV show. The merchant may record the data stream in his commercial so that when the commercial is finally played, the coupon data can be played and the user can download the coupon.

Similarly, the mixing of the coupon with the programming (or commercial) may occur at the headend 170b or 170a. Normally, the headend associated with the cable service has commercial slots of its own to sell. Some of the merchants buy these commercial slots and much like the above TV commercial, the merchant records the coupon data stream with the commercial so that when the commercial finally airs, the coupon data stream is emitted and the prepared user can download the coupon. The headend could also mix coupon data streams on its own with the audio portion of the programs that are aired. A headend that is responsible for a region can strike deals with local merchants who want to air their coupon data stream. In this manner, local merchants can distribute the coupon data to the subscribers in the region of interest at a price much lower than the national merchant who wants to advertise nationally. This is similar to paying for local advertisement time on local TV channels.

The same principles apply to the conventional TV/radio broadcast infrastructure. The coupon data stream can be recorded or mixed at the production studio (e.g., for shows and commercials), the network source

IPR2025-01150
Apple EX1071 Page 678

(e.g., CBS), and the local station (e.g., station KXYZ). Each entity in this broadcast link can strike its own deals with merchants who want to provide coupon data to users.

When the data stream is emitted by the speaker of the TV or radio, the user normally points his electronic card in the direction of the sound and presses the RX button to receive and download the data. The card then turns off after the data has been received. If more coupons are available, the user can activate his card and receive more coupons. The number of coupons stored in the card is limited by the storage space.

Referring to FIG. 5(B), the data stream includes a data portion. This data portion can be any length and can contain any information. In the coupon case, the data portion may include a merchant ID and a coupon number. The coupon redemption scheme relies on these two pieces of information to authorize the redemption.

In another embodiment of the present invention, the coupon data are transmitted to those subscribers with set top boxes. Set top boxes are normally used for interactive TV as well as certain premium cable services (e.g., AT&T Cable Service's Expanded Service with Digital Cable). For these cable services, these set top boxes also provide some electronic TV program guide functionality so that the user can simply select his channel using his on-screen program guide rather than entering the channel number directly. Of course, the user can still enter the channel number directly if so desired.

For this embodiment, the coupon data are transmitted during off-peak hours (e.g., early in the morning) once a day, or during the vertical blanking intervals (VBI). As the coupon data is transmitted, the set top box receives and records them for later playback as necessary. Thus, instead of the coupons being associated with a program, the coupons are now associated with a channel or the electronic TV program guide. The user can turn to a dedicated Ad channel where he can scan the listed coupons and select the ones he wishes to download. When he has selected a coupon for download, he presses a button on his set top box remote control (or his electronic card). The set top box then plays the audio file that contains the coupon data. The user would of course have his electronic card ready and pointed toward the speaker. The coupon data is now stored in his electronic card.

5.1.3 BROADCAST MEDIA COUPON REDEMPTION

Assuming that at least one coupon is stored in the user's electronic card, the user has several options to redeem his coupon:

(1) Password-based Internet Manual Redemption -- access the coupon sponsor's website and redeem manually via a password

(2) Internet Automatic Redemption -- access the coupon sponsor's website and redeem automatically

(3) Store Redemption -- physically visit a store and manually redeem at the checkout line/kiosk

These redemption schemes will now be discussed. In the preferred embodiment, the automatic form of redemption if favored over the manual redemption, although both are feasible.

5.1.3.1 Password-based Internet Manual Redemption

Password-based Internet Manual Redemption implies that the user must enter some key sequence with his computer keyboard to redeem his coupon. In one embodiment, the user's electronic card includes an LCD display. In this embodiment, the user accesses the website associated with the stored coupon. Eventually, he

IPR2025-01150
Apple EX1071 Page 679

navigates to the page where the coupon redemption function is provided. He may even see a button on the web page that says "Click here to redeem with your electronic card." When the user presses the button on the web page, the web page asks the user to press the RX switch on his electronic card. The web page plays an audio file which includes what is hereinafter referred to as "redemption data" and the electronic card receives this audio signal and processes it.

Based on a known algorithm that checks whether the coupon is valid or not (based on the merchant ID and coupon number), the electronic card displays a password. Simultaneously, the web page asks if the user received the signal properly. If not, the user can press that button on the web page again to initiate the playing of the audio file. If the user's electronic card received the audio signal properly and provided a password, the web page provides a section that allows the user to manually enter the password. The user then enters the password. The web site checks to make sure that this is a valid password and if so, authorizes the redemption. If the password is not valid, the website will deny the redemption request. The user then proceeds in the conventional manner to either continue shopping or go to the checkout line to claim his gift or otherwise apply his coupon to his purchase.

In this embodiment, the password is unique to this particular redemption because the counter value and the individual ID (refer to the discussion above with respect to FIGS. 5(A) and 5(B)) in the card have been incorporated in the password generation. Thus, merely giving a friend this same password will not enable this friend to "redeem" a coupon because that password is unique to the electronic card holder and that particular transaction. Another electronic card user who downloads a coupon will have a different password.

In another embodiment, the special client software 114 (FIG. 11) plays a more important role. When the user navigates to the web page where the coupon redemption function is provided, he may see a button on the web page that says "Click here to redeem with your electronic card." When the user presses the button on the web page, the web page asks the user to press the TX switch on his electronic card. When the user presses the button on the web page, the web site delivers the redemption data which is provided to the special client software. The user also activates the TX switch on his electronic card to transmit the coupon data to the PC. The PC processes the coupon data with the redemption data and generates a password. The password is displayed by the PC and the user can enter it manually with his keyboard into the web page. The web site checks the password and either authorizes or denies the redemption request.

In the above two examples, the user's electronic card may hold several coupons. The processor checks each coupon separately with the redemption data to generate the password. For those coupons that are not associated with a particular merchant's redemption data, they are ignored.

Note that these password or two-factor security schemes are, as a practical matter, less convenient to the user. So, these two-factor security schemes will be employed if security is paramount. If, however, convenience is paramount, such as for online shopping, these two-factor security schemes will not be employed. The user only needs the electronic card itself to conduct his online shopping.

5.1.3.2 Internet Automatic Redemption

IPR2025-01150
Apple EX1071 Page 680

Internet Automatic Redemption implies that the user need not enter any key strokes with his computer keyboard to redeem his coupon. Furthermore, the user's electronic card need not have an LCD display. In this embodiment, the user accesses the website associated with the stored coupon. Eventually, he navigates to the page where the coupon redemption function is provided. He may even see a form on a web page that requests, "Please enter the coupon redemption number." The user then presses the TX switch on his electronic card which transmits his counter value, individual ID, and the coupon data. If more than one coupons are stored in the electronic card, all coupons are transmitted to the PC.

The special client software 114 (see FIG. 11) receives the data and displays a dialog box with some choices and asks the user which coupon he would like to redeem. The user selects the choice that corresponds to the coupon he wishes to redeem. The special client software then fills out the web page form with the coupon redemption number (which may incorporate the individual ID, counter value, and coupon data) and sends the form back to the web site. The web site checks the coupon data as well as the user's individual data and counter value to ensure that this user is a valid card holder and eligible to receive this coupon. The counter value is used to ensure that this same downloaded coupon cannot be used again by some computer hacker who stole the coupon redemption data online. As described above, with each press of the electronic card, the counter value increments.

In another embodiment, when the user navigates to the web page where the coupon redemption function is provided, he may see a button on the web page that says "Click here to redeem with your electronic card." When the user presses the button on the web page, the web page asks the user to press the TX switch on his electronic card. When the user presses the button on the web page, the web site delivers the redemption data which is provided to the special client software. The user also activates the TX switch on his electronic card to transmit the coupon data to the PC. The PC processes the coupon data with the redemption data and generates a password. The password is not displayed and the software can provide this password to the web site automatically without the user ever knowing the password. The web site checks the password and either authorizes or denies the redemption request.

Again, the password is unique to this particular redemption because the counter value and the individual ID (refer to the discussion above with respect to FIGS. 5(A) and 5(B)) in the card have been incorporated in the password generation. Another electronic card user who downloads a coupon will have a different password.

5.1.3.3 Store Redemption

In this embodiment, the user takes his electronic card to a conventional non-web store. Of course, the store sponsored the coupon he downloaded or otherwise sells a product/service of the company that sponsored the coupon. He takes his electronic card to a kiosk, which is equipped with a PC. The user activates the kiosk to prepare it to receive the coupon data. He then activates the TX switch on the electronic card to transmit the coupon data, along with his individual ID and counter value. The kiosk receives the information and checks to make sure the coupon is valid. If the store is a national or otherwise chain-type store, this check may occur at a designated network server that links other related stores. If the store is purely a local store, the check may be

IPR2025-01150
Apple EX1071 Page 681

done locally at the kiosk or a network server that serves that particular store. If the check indicates that the coupon is valid, the kiosk may generate an actual paper coupon for the user to use at the checkout line.

Note that in another embodiment, the system uses pattern recognition as described more fully below. In this pattern recognition embodiment, the kiosk may "listen" for the recorded time slice of audio stored in the electronic card and perform pattern matching.

In another embodiment, the user may simply go to the checkout line at the store (with or without any merchandise, depending on the coupon). At the checkout line, the store has a computer that also functions as an electronic cash register. Equipped with a standard sound device, the cashier asks the user to press his TX switch on his electronic card. He does so and the coupon data along with his individual ID and counter value are transmitted to the store computer. This transmitted data is now checked. Again, like the kiosk case above, if the store is a national or otherwise chain-type store, this check may occur at a designated network server that links other related stores. If the store is purely a local store, the check may be done locally at the network server that serves that particular store. If the check indicates that the coupon is valid, the computer allows the user to redeem that coupon. If some merchandise is involved, the value of the coupon is applied to the purchase of that merchandise. If a free promotional item is offered, the item is given to the user without charge. Thus, based on the nature of the coupon, the action taken after the check will vary.

Another redemption scheme involves the use of the magnetic strip on the electronic card. A code would be written onto the magnetic strip portion of the electronic card as the user downloads coupons electronically off the web or some media device. The logic circuitry necessary to write this code onto the magnetic strip area exists in the form of magnetic strip writers. The various components to realize the magnetic strip writer are manufactured in miniature form to comply with the electronic card's form factor requirements. Appropriate software in the electronic card would detect that a coupon was downloaded and stored in the electronic card. This software would then instruct the magnetic strip writer circuitry to write the redemption code onto the magnetic strip area of the electronic card.

5.1.4 INTERACTIVE TV AUCTION

In this embodiment, the television set is an interactive TV set, typically with a set top box. When a live auction is broadcast on one of the channels, the user is allowed to bid on an item by pressing the TX switch of his electronic card. For example, assume that one of the channels is an auction channel, perhaps even called "The Auction Channel." The Auction Channel broadcasts traditional auctions with perhaps live participants. However, in addition to live participants, TV viewers equipped with the electronic card of the present invention are also allowed to bid on the item. Whenever the user presses the TX switch, the electronic card sends out his individual ID, counter value, group ID, among other data. The two-way set top box receives the user's data stream and passes this data stream along to the various distribution hubs and headends that make up this return path. Ultimately, the user's data stream makes its way to the server of the Auction Channel for the particular auction he is viewing.

When the Auction Channel's server receives the user's data stream, performs an authentication check (i.e., the user is a valid user) and the request is a valid request by checking the counter value, among other data.

IPR2025-01150
Apple EX1071 Page 682

When all the checks have cleared, the user's data stream is interpreted as a valid bid by the Auction Channel's server and also by the human auctioneer. This process can continue until the item has been awarded to the winning bidder.

Alternatively, the user's data stream may go to a dedicated authentication server that is independent of the Auction Channel's server. Once authenticated by this authentication server, the user can then use his conventional set top box remote control to bid on items for that particular auction.

5.1.5 CONTENT RECORDING FOR SEARCH/REDIRECTION

In another embodiment of the present invention, the electronic card can be used for recording an audio clip of the raw content broadcast over TV, radio, or heard by the cardholder. Once the audio clip has been recorded, a variety of redemption schemes allow the user of the electronic card to benefit from the recording. For the purposes of this patent specification, the term "redemption" is used to denote any type of action that the user takes to obtain something for recording that audio clip with his electronic card. Basically, the redemption schemes include: (1) finding information that is related to or associated with the audio clip more quickly and easily than conventional Internet searching techniques; and (2) receiving coupons, incentive points, or other sales offers as a reward for watching that TV program/advertisement or listening to a particular radio broadcast/advertisement. These redemption schemes can be implemented on-line over the Internet or at a conventional store. Details of these redemption schemes are provided below.

5.1.5.1 Electronic card Hardware

Referring to FIG. 1 again, the electronic card 10 is now basically a portable digital recorder of sound. Audio, for example, from TV and/or radio can be recorded as an audio clip. Typically, only 5 to 10 seconds of the audio clip need to be recorded for the redemption scheme to succeed. Thus, if a user missed the beginning of a broadcast, he need not worry since recording any portion of the entire audio soundtrack is sufficient for successful redemption. As for the quality of the recording, high fidelity level is not necessary and thus low component/fabrication costs and small form factor sizes can be achieved.

FIG. 20 shows one embodiment of the electronic card that provides the analog recording function. This FIG. shows a two-way card, in which the receiver portion 209a functions as a sound recorder and the transmitter portion 209b functions as a playback device. Power to the entire card is provided by a power supply 207, which in one embodiment is a Varta LPF-25 battery. The power supply 207 provides power to the microprocessor 205, the switch block 206, and the RAM 208 for battery back-up.

The digital core of the card is a microprocessor unit 205, which is coupled to a battery backed-up RAM 208. The RAM 208 needs to be battery backed-up to keep the recorded sounds in memory for as long as the user desires. In one embodiment, the microprocessor 205 manages the memory in the RAM 208 in a first-in first-out (FIFO) scheme. In this manner, the oldest recorded and stored audio clip is played first (during playback). If not enough memory space is available, the microprocessor 205 erases the oldest recorded audio clip first. Thus, as more and more audio clips are recorded and stored, more and more of the oldest stored audio clips will be replaced by the newer audio clips if memory space becomes an issue.

IPR2025-01150
Apple EX1071 Page 683

For the analog front end portion, a transducer 200 and a switch block 206 are provided. The transducer 200 can be either a single transmitter/receiver transducer or two separate transducers (i.e., one transducer functions as a microphone and the other transducer functions as a speaker). The switch block 206 provides power to the entire card. In one embodiment, the card contains two switches – a record switch and a transmit switch. These two switches are provided in the switch block 206. As described above, the switch block has silicon switches so that when the user releases the switch too soon, the rest of the circuitry in the card still has enough power to perform their respective functions. The recording feature will now be discussed. When the record switch is pressed in the switch block 206, power from the power supply 207 is provided to the transducer 200 as well as the rest of the circuitry in the card. Sound that is picked up by the transducer microphone is delivered to the receiver portion 209a of the card where it is amplified (amplifier 201), filtered (BPF 202), and gain controlled (AGC 203) prior to being digitized (A/D 204). The digitized sound is provided to microprocessor 205 which stores the digitized recording in RAM 208. Because each recorded audio clip takes up only 5-10 seconds, the RAM 208 must be large enough to support all the recordings that need to be stored. Typically, 5 seconds of sound take up approximately 500 KB of memory.

The playback feature will now be discussed. Having stored the sound in RAM 208, the recorded sound can be played by the user at any time. When the user presses the playback switch in the switch block 206, the recorded sound stored in RAM will be played through the transducer speaker of the card. Each press of the playback switch plays a single recorded audio clip in the order in which they were stored. Thus, the first press of the playback switch activates the playback of the oldest audio clip file. The second press of the playback switch activates the playback of the second oldest audio clip file. This process is circular so that after the newest audio clip file is played, the next audio clip file to be played corresponds to the oldest audio clip file. Of course, one ordinarily skilled in the art can devise other similar schemes to playback recorded audio. Multiple buttons can be implemented as well as a single button with multiple functions (or modes). Perhaps a delete button can be implemented so that the user can selectively delete the desired audio clip.

The circuitry in the transmitter portion 209b of the card is similar to that of FIGS. 2, 7, 8, 9, and 10. However, in this embodiment, the switch press activates a transmit routine that incorporates the audio clip file stored in RAM 208. A pointer is implemented that keeps track of which audio clip to play. After each press of the playback switch, the audio file being pointed to is played, and the pointer then moves to the next oldest audio file in RAM 208. In addition, the DES3 encryption scheme which includes the use of the group ID, individual ID, and counter values can also be used for authentication purposes. Thus, when the playback switch is pressed, an encrypted version of the audio clip file along with other authentication data is transmitted to the computer's microphone. The server receiving this data can authenticate the user and provide the pattern recognition search service for website redirection or coupon/incentive point collection, as described below.

5.1.5.2 Server Architecture

A server computer station 210 associated with the broadcast media interactive system in accordance with one embodiment of the present invention will now be discussed with respect to FIG. 21. At the core of the server 210 is a web server 215b which interfaces with a database server 212, a messaging server 215a, an

IPR2025-01150
Apple EX1071 Page 684

authentication server 213, and the Internet 16. The web server 215b is further coupled to communications lines 219f (e.g., via a modem or network router connected to server 210) and the Internet 16.

In one embodiment, the web server 215b performs many tasks related to the management of the accounts, merchandises, coupons, incentive points, and soundtracks, music sales, sales of other services or merchandise associated with the recorded sound clips, or other information services relevant to the card issuer. From executing code for any number of different applications, managing resources, handling web requests, managing files and records, creating files and records, deleting files and records, delegating tasks, and handling exceptions, the web server 215b provides the main processing for the server 210. As noted above, this functionality, in other embodiments, could be distributed across multiple hardware servers.

The web server 215b also works with a messaging server 215a via line 219d (e.g., the system bus or a network connection to another hardware server) and a database server 212 via line 219b. The messaging server 215a works with the web server 215b via line 219d and is also connected to the Internet via communication lines 219e. The messaging server 215a provides various messaging functionality in various communications media such as telephone, email, instant messaging, active desktop application, and web browser notices. For example, email notices such as product news, discount updates, and customer service access are provided via communications line 219e. News of upcoming sales offers that may interest the potential customer are delivered frequently. Also, any questions that a user may have may be directed to customer service through the messaging server 215a, which will direct the email to the appropriate personnel within the customer service department. As noted above, various forms of instant messaging as are well known in the art could replace some or all of the functionality of messaging server 215a.

Note that communications lines 219e and 219f are standard interfaces to the Internet (e.g., an Ethernet or other network interface to a router and CSU/DSU, modem, etc.) or across machines which are typically Ethernet-connected at the "back end" of the network.

In another embodiment, the web server 215b and messaging server 215a are integrated in an Internet server 215. The interface to the Internet 16 is provided by primary communications line 219f (line 219e is not implemented). Thus, all web traffic passes through this Internet server 215 via communications line 219f. The messaging server 215a communicates with the web server 215b and the back end of the system (e.g., database server 212).

The database server 212 performs many tasks related to the creation, deletion, and management of various files and records managed by the server 210. The database server 212 supports the web server 215b in accomplishing its tasks of running the redemption portion of the broadcast media interactive system. The database server includes a management tools and web page information unit 212a and a pattern recognition search engine unit 212b. The management tools and web page information unit 212a provides exactly that – tools for the web page administrator to update, modify, and troubleshoot his web site. The web page information is also provided herein so that the web server 215b accesses the web page information from this unit 212a. Thus, when a user logs into the web page associated with server 210, the look and feel of this web page is stored in the unit 212a. However, the web server does not access the unit 212a for each access of this

IPR2025-01150
Apple EX1071 Page 685

web page; rather, the web server 215b accesses the web information in the unit 212a only periodically to update its contents. The pattern recognition search engine 212b will be discussed in greater detail below. Generally, however, the pattern recognition search engine 212b performs pattern recognition matching functionality between a user-submitted audio clip and the soundtrack files in the soundtrack database 211d.

The database server 212 serves a database of content to be operated or accessed in conjunction with card operation. For example, that database server 212 can serve an incentive points database 211a, a coupon database 211b, a merchandise database 211c, a soundtrack database 211d, and an account database 211e. These databases 211a-211e are coupled to a communications line 219a and to the database server 212.

These databases on communications line 219a comprise the "back end" of the system. Note that the common bus-like illustration of the communications line 140 is merely conceptual. The databases may not actually be on a common bus. These databases may be widely dispersed geographically or integrated into one database. Also, some of the databases may be on a common bus while others may be located remotely and accessed via the Internet.

The incentive points database 211a contains various incentive points banner ads and programs. Additionally, the prerequisites for earning these incentive points are also stored herein. Similarly, the coupon database 211b contains various coupon information that is either disseminated via the messaging server 215a or awarded to certain users when certain requirements are satisfied. Also, the merchandise database 211c contains various merchandise information that can be purchased by users or awarded based on satisfying certain requirements. These databases 211a-211c can also contain links to specific web pages associated with the incentive point, coupon, or merchandise so that the user can be properly redirected to that website. In another embodiment, these databases do not contain ads, programs, coupons or information; rather, these databases contain only links where the user can be properly redirected for more detailed information. The website associated with the link has the programs and coupons that are awarded to users. If necessary, these websites communicate with the account database 211e to keep credits, debits, and points information.

The soundtrack database 211d contains soundtrack files for those TV programs, TV ads, radio programs, and radio ads of companies that are participating in this broadcast interactive system. This soundtrack database could also just be a collection of music from a given genre that is available for sale. That is useful for implementations in which cardholders know that they can operate their card to identify that sort of music. For example, a "top 40" card or a "country & western" card might be considered. The various incentive points, coupons, and merchandise are awarded in conjunction with some matching function performed by the pattern recognition search engine 212b against the files in the soundtrack database 211d. Alternatively, the matching function results in the user being redirected to the website that is associated with the matching soundtrack file.

For example, assume that a requirement for winning a certain number of incentive points or a particular coupon or a particular merchandise is providing proof that the user watched a particular ad that appeared in conjunction with a certain TV show (e.g., ABC Corporation's ad in an "X-Files" episode). One form of proof that the server 210 will accept is the audio clip recorded with the electronic card 10 (FIG. 1). The

IPR2025-01150
Apple EX1071 Page 686

user records an audio clip from that advertisement (perhaps the jingle portion of the ad). The user then accesses the website associated with this server 210 with his browser and plays back the recording. The pattern recognition search engine 212b compares the user's audio clip to those stored in the soundtrack database. If a match is found between the user's submitted audio file and a soundtrack file in the soundtrack database 211d as determined by the pattern recognition search engine 212b, then the incentive points, coupons, and/or merchandise are awarded to the user who submitted that audio file.

Analogously, the successful match may result in the user being redirected to a particular web page where he can get more information on the product/service that was advertised in that TV ad. For example, if a user recorded an audio clip from a commercial featuring XYZ Corporation's coffeemaker, the pattern recognition search engine would then match the user-submitted audio clip with the appropriate soundtrack file associated with XYZ's coffeemaker. The match results in the user being redirected to the website associated with the XYZ coffeemaker.

In another example, the user may record a sound clip from some music that he heard over the radio. Although the user is unsure of the music's identity, he knows that he "likes" it. He accesses some central music website where he plays his sound clip. The pattern recognition software identifies the music and provides for the user the various CDs and other music forms (e.g., MP3) that are available for purchase. Thus, without knowing the title or artist of the music that he just heard on the radio, the user is able to identify and purchase that piece of music by merely recording a sound clip from that music and playing it back to a central website. This is especially useful because in most cases, the radio station rarely identifies the title (or even the artist) of a piece of music prior to actually playing that piece of music over the air. Usually, this identification occurs after the music is played. Sometimes, the radio disc jockey identifies this music along with several other songs that have also aired, which complicates the identification process for the user. Not only does the user have to match the identification with the actual song he heard, but he may have to wait for quite some time before the radio disc jockey makes the on-air identification. With this embodiment of the present invention, the user merely records the a clip of the song and play it back to a central music website. The music website will identify the music immediately and also suggest CDs that contain that song to purchase.

The memory 214 provides support for the database server 212 and the authentication server 213 so that these servers can serve all the user requests coming in. For example, hundreds if not thousands of users may be accessing this server 210 to submit audio clips. These audio clips are temporarily stored in the memory 214 until they are served by the database server 212, the authentication server 213, or both. The pattern recognition search process also requires some memory space to perform the match functions.

The account database 211e contains information about each user's account. Normally, only a user with an account (i.e., member) get the benefit of this broadcast media interactive system with points, coupons, and merchandise. The account information includes account balance (points or otherwise), expiration date for each point or group of points, redemption information, credit card information, billing information, billing address, and whether the account is authorized for using points for credit. Although this embodiment illustrated in FIG.

IPR2025-01150
Apple EX1071 Page 687

2 shows the account database 211e integrated with the rest of the server 210, another embodiment may have the account database located in a third party's server and maintained by the third party.

These databases 211a-211e contain appropriate linking fields so that an entry in one database can be associated with a related entry in another database. For example, when a user earns incentive points from the incentive points database 211a, that user's account in the account database 211e is appropriately updated.

In another embodiment, the incentive points database 211a, the coupon database 211b, and the merchandise database 211c are integrated into one database. The soundtrack database 211d and the account database 211e, however, are kept separate. In still another embodiment, these databases are distributed across one or more machines. These machines are coupled via communications line 219a to the database server 212. These databases comprise the "back end" of the system which the Internet server 215 access.

The authentication server 213 provides security functionality so that only those users with a proper account can access the features provided by the server 210. In particular, the data stream of the electronic card, which includes the group ID, individual ID, counter value, and raw data, can be encrypted. These fields can be checked against the account database to ensure that the proper user (individual ID, counter value) associated with a proper participating merchant (group ID) is accessing the system. Of course, the audio clip (i.e., raw data) is used only when the user has been authenticated. The authentication server also ensures that only those users with the properly sponsored electronic card (which performs the encryption and frequency translation (e.g., to ultrasound)) can access the server. Thus, anyone with a standard tape recorder cannot merely record an audio clip of a TV commercial, access the website associated with server 210, playback the audio clip, and obtain the desired service (e.g., redirection) or item (incentive points, coupons, merchandise).

In another embodiment, the authentication server is not implemented so that, for example, any user with a tape recorder could record the relevant audio clip, access the web site associated with server 210, playback the recording, and obtain the desired service or item, so long as the user is a member (i.e., has an account in the account database 211e) or opens a new account. This aspect, however, might be less than desirable because of the lack of convenience that the electronic card would otherwise provide. Still, the basic audio recording and playback functionality required by the system could be so provided.

The pattern recognition search engine (212b in FIG. 21) will now be discussed. In particular, the pattern recognition search functionality in the pattern recognition search engine will be described. Referring now to FIG. 22, the 5-10 second audio clip that was submitted by the user is represented by reference numeral 220. This audio clip is sampled at sampling block 221. In one embodiment, the sampling rate is 2,000 samples per second. The sampled audio clip is presented to a normalization block 222. The normalized audio clip is then presented to filtering block 223 to remove undesired frequency components.

A time slice block 224 receives the filtered audio clip. This time slice block divides the audio clip into time slices, where each time slice is approximately 20-50 msec in duration. Each audio file in the soundtrack database 211d (in FIG. 21) has also been divided into time slices. The search for a match between the user-submitted audio clip and one or more audio files in the soundtrack database 211d (in FIG. 21) involves comparing time slices of the user-submitted audio clip and time slices of the audio files in the soundtrack

IPR2025-01150
Apple EX1071 Page 688

database. The length of each time slice in the pattern recognition search engine 211d (in FIG. 21) should be short enough to make the match process time-invariant. In other words, the incoming audio clip submitted by the user is a 5-10 second clip from any portion of the soundtrack that aired on TV or radio. One user may start recording as soon as the soundtrack began, while another user starts recording 4.2 seconds into the soundtrack. No two users may record the same section of the broadcast soundtrack. To compensate for this time variance, the match process must make the time slices short enough so as the make the search engine time invariant. On the other hand, each time slice must not be so short that the match process would be too computationally intensive requiring a very fast processor. Analogously, if the time slice is too long, the pattern recognition search engine may not find any match whatsoever.

For each time slice, a feature calculation block 225 performs feature calculations. The feature calculation block 225 attempts to extract some usable feature for each time slice. Typically, the feature calculation block 225 performs some time domain to frequency domain transformation process. In one embodiment, the feature calculation block 225 performs a Fourier Transform on the data in each time slice. In another embodiment, the feature calculation block 225 performs linear predictive coding (LPC) on the data in each time slice. In still another embodiment, the feature calculation block 225 performs a power spectral density on the data in each time slice. However, the present invention is not limited to such time-to-frequency domain transformations. Other transformations as known to those ordinarily skilled in the art of pattern recognition search technology can be applied.

Based on the feature calculation for each time slice, a comparator block 226 attempts to find a match between each time slice from the audio clip submitted by the user and the time slices in the soundtrack database 211d (in FIG. 21). In one embodiment, a time slice associated with the user's audio clip is compared with each time slice in the soundtrack database. The calculated features in each time slice are compared to each other. The audio file in the soundtrack database that provides the closest match for this initial time slice results in the search engine producing a hypothesis where that audio file in the soundtrack database is considered a match. This hypothesis will be tested in block 227 as more time slices associated with the user's audio clip are compared to the soundtrack database. The check hypothesis block 227 creates a table or a list of soundtrack files that have successfully matched the time slices in comparator block 226. When the number of matches for a particular soundtrack file exceeds some "high confidence" threshold, then the particular soundtrack file is considered a match with high confidence. Alternatively, if a particular soundtrack file exceeds some "medium confidence" threshold (which is much less than the "high confidence" threshold) of matches and no more time slices are available for further comparisons, then that particular soundtrack file is considered a match with medium confidence. Similarly, if a particular soundtrack file exceeds some "low confidence" threshold (which is much less than the "medium confidence" threshold) of matches and no more time slices are available for further comparisons, then that particular soundtrack file is considered a match with low confidence.

Also, if a particular soundtrack file does not exceed the "low confidence" threshold and no more time slices are available for further comparisons, then the pattern recognition search engine will determine that no

IPR2025-01150
Apple EX1071 Page 689

match exists. Alternatively, the pattern recognition search engine may determine that a match with negligible confidence exists for this latter case.

5.1.5.3 System Operation

In this section, the recording of content will be described first, followed by the various redemption schemes. In general, a user need to merely press the record button on his electronic card when a TV commercial, TV program, infomercial, radio commercial, or radio program is being aired. However, to get any benefit out of this broadcast media interactive system, the broadcast content must have a corresponding soundtrack file in the soundtrack database 211d (in FIG. 21). Normally, the soundtrack can include the entire audio from the content, whether it's an hour-long drama, a two-hour long TV movie, a half-hour sitcom, or a thirty-second commercial.

The operation of the server in FIG. 21 can be done centrally or in distributive fashion. In the central operation scheme, only one website or entity would own and operate the server of FIG. 21. Accordingly, all users must come to this entity's website to request pattern recognition search services to obtain the coupons, incentive points, sales information or to be otherwise redirected to the proper website where the user can receive coupons, points, and sales information. Usually, the owner of the server of FIG. 21 negotiated some type of arrangement with a merchant (XYZ Corporation for ads, commercials, infomercials), TV network (e.g., ABC, CBS, NBC, Fox), cable service provider (e.g., AT&T Cable Services), satellite service (e.g., Direct TV), local TV station, local radio station, and the like. This arrangement includes placing the soundtrack of the program or the commercial in the soundtrack database for pattern recognition searching purposes. Without such an arrangement, the user can record any content he pleases but he will not be able to redeem it for any value in return.

In the distributed scheme, any web merchant, network, cable provider, local station (TV, radio, or otherwise), and the like can own and maintain its own server of FIG. 21. In this case, users would have to go to each web entity's website for service. If a user just recorded an audio clip of a commercial on CBS, he may have to go to the website of either CBS or the company associated with that commercial. In this distributed scheme, multi-entity arrangements may not be necessary.

For example, assume that CBS wants to increase viewership of certain TV programs. To utilize the various embodiments of the present invention, the electronic cards must be distributed to users so that they will use them when watching TV programs. CBS and/or other entities may provide for card distribution in any number of methods.

One method includes distributing these cards in the same package as another product. For example, in a joint venture with TV Guide Magazine, CBS and TV Guide distribute these electronic cards as a securely placed insert in the upcoming issues of TV Guide (with or without any additional price increase in the TV Guide). As another example, CBS and a certain XYZ Corporation agree to distribute these electronic cards in XYZ's compact discs (CD) in a joint venture to co-market CBS and XYZ Corporation's CD division. When a user purchases an XYZ CD, the CD package includes a free electronic card.

IPR2025-01150
Apple EX1071 Page 690

In another distribution scheme, CBS may limit distribution of these cards to some entity with a large membership base. For example, in a joint venture with AOL, CBS and AOL agree to distribute these electronic cards to AOL members only. AOL members would receive these cards in the mail. Similarly, VISA card holders may receive these electronic cards in the mail as a result of some arrangement between CBS and VISA.

In another distribution scheme, the major credit card organizations (i.e., VISA, Mastercard, American Express) arrange for its member issuing banks to distribute these cards to all new and existing card holders. In this arrangement, CBS has no involvement in the distribution, but rather benefits from having some other organization handle the distribution of the cards.

Whatever the card distribution scheme, assume for the purpose of discussion that these electronic cards are now in the hands of users. CBS would of course market the use of these electronic cards via print (e.g., newspapers, magazines) and electronic media (e.g., TV commercials, radio broadcasts, Internet newsgroups, CBS's website). CBS would also have some arrangement with the server of FIG. 21 to carry soundtracks of its programs and commercials in the soundtrack database 211d (in FIG. 21). Now, to increase viewership, CBS would market certain programs heavily. It mentions that by recording an audio clip of a CBS program (or relevant portion of a CBS program, such as the opening credits) or a commercial that appeared within a program's time slot, the user could redeem the recording to earn coupons to various merchandise, earn incentive points such as mileage with a popular airline, win free merchandise, or otherwise obtain some benefit. In this case, the broadcast media interactive system benefits both the sponsoring entity (e.g., CBS, TV Guide, XYZ Corporation) by increasing viewership or product purchase, as well as benefiting the user.

Redemption schemes will now be discussed. Basically, the redemption schemes include: (1) finding information that is related to or associated with the audio clip more quickly and easily than conventional Internet searching techniques; and (2) receiving coupons, incentive points, or other sales offers as a reward for watching that TV program/advertisement or listening to a particular radio broadcast/advertisement. These redemption schemes can be implemented on-line over the Internet or at a conventional store.

In the first type of redemption scheme, the user would take his electronic card, which contains the audio clip of a TV program or commercial, to his computer and access the Internet. The user initially recorded this audio clip because he was interested in a particular TV program (if his audio clip was some portion of the TV program), or some product or company (if his audio clip was of some portion of a TV commercial or radio commercial). The user wants more information about that program, an actor/actress of that program, the network itself (e.g., CBS) carrying that program, the product that was showcased in that commercial, or the company that makes/distributes that product in that commercial. However, the use of a conventional search engine might be too complicated, inefficient, or both when he tries to find the relevant information on the web. The electronic card facilitates his searching efforts.

When he accesses the website associated with the server of FIG. 21, the website then instructs the user to play the recording to his PC microphone. He plays the recording. When a match occurs between the user's audio clip and a file in the soundtrack database 211d (in FIG. 21), the server then redirects him to the relevant web page. Assume that the user was interested in a particular product in a TV commercial, the server redirects

IPR2025-01150
Apple EX1071 Page 691

him to the website of the company that makes or sells that particular product. In may cases, the user is directed to the particular web page that has the detailed information about that product to simplify the process for the user. The user need not be directed to a company website where he then has to wade through the tens or hundreds of pages of products that the company makes or sells. Rather, he is directed to the very page that has all the information that the user desires on that particular product. From here, the user can access information about the company that makes or sells that product, if desired.

Assume that the user is interested in finding more information about a particular actor who appeared in a television program. While watching that program, the user would record an audio clip of a portion of that program. He would then playback this recording in the manner described above as instructed by the website. The website associated with the server of FIG. 21 would then perform a pattern recognition search of the submitted audio clip. If a match occurs, the website would then redirect him to a web page that corresponds to the TV show he was watching. From this website, the user can then find links to the actors in this program, including the actor he is interested in, and access the linked web pages to obtain more information about that actor. If desired, the user can also obtain more information about the network that broadcast that TV show, the studio that made that TV program, or a whole host of other information related to that TV program.

Similarly, assume that the user recorded an audio clip of a TV commercial. In that commercial, the merchant advertised certain coupons or mileage points by going to his website and registering. The user takes the recorded audio clip, plays it to the server via his microphone across the Internet, and waits for pattern match. The server then informs the user that a match occurred (or no match), and redirects him to the merchant's webpage. Here, the user can register to earn his coupons or mileage points. In this case, the user's account balance is modified to reflect the earning of the mileage points. This account can be at either the website that the user was redirected to or the website of FIG. 21, where the account database 211e is maintained. This example is also related to the second redemption scheme. However, in this example, both the redirection and the earning of coupons or points occur together.

As another example of this second redemption scheme, the user takes his recorded audio clip in his electronic card to the website associated with the server of FIG. 21. When he plays back the recorded audio clip, the server performs the pattern match search and generates some match result. If a successful match results, the user with the proper account in the account database 211e earns the advertised incentive points, mileage points, or coupons. These earnings are reflected in the account database 211e associated with that user. The user can then redeem these coupons at any participating merchant and follow rules associated with their redemption, such as using the coupons prior to the expiration date.

As mentioned briefly above, the user can also take his electronic card to a conventional non-web store for redemption. Of course, the store sponsored the coupon that he saw (and recorded) on TV or radio or otherwise sells a product/service of another company that sponsored the coupon. Sometime after recording the audio clip with his electronic card, the user takes his electronic card to a kiosk, which is equipped with a computing station or terminal. The user activates the kiosk to prepare it to receive the coupon data. He then activates the playback switch on the electronic card to play the recorded audio clip. The kiosk receives the

IPR2025-01150
Apple EX1071 Page 692

information and delivers the audio clip to a server or computing system that contains the pattern recognition search engine and the soundtrack database. If the store is a national or otherwise chain-type store, this search function may occur at a designated network server that links other related stores. If the store is purely a local store, the search may be done locally at the kiosk or a network server that serves that particular store. If the search indicates that the coupon is valid (i.e., audio clip matches a soundtrack file), the kiosk may generate an actual paper coupon for the user to use at the checkout line.

In a variation of this embodiment, the user may also simply go to the checkout line at an actual conventional store (with or without any merchandise, depending on the coupon). At the checkout line, the store has a computer that also functions as an electronic cash register. Equipped with a standard sound device, the cashier asks the user to press his playback switch on his electronic card. He does so and the audio clip is transmitted to the store computer. This transmitted audio clip is now checked with the soundtrack files in the soundtrack database. Again, like the kiosk case above, if the store is a national or otherwise chain-type store, this check may occur at a designated network server that links other related stores. If the store is purely a local store, the check may be done locally at the a network server that serves that particular store. If the check indicates that the coupon is valid, the computer allows the user to redeem that coupon. If some merchandise is involved, the value of the coupon is applied to the purchase of that merchandise. If a free promotional item is offered, the item is given to the user without charge. Thus, based on the nature of the coupon, the action taken after the check will vary.

Similarly, the user may go to a kiosk or customer service station. When he plays the recorded audio clip, the kiosk or customer service station informs him the location of the merchandise associated with the recorded audio clip. The user can then find his item in that store with relative ease.

5.1.6 BOOKMARKS FOR BROADCAST MEDIA

In a variation of the content recording embodiment, the audio clip can be used to keep a "virtual bookmark" in the electronic card with respect to the broadcast content. Later, when he access the Internet, he can playback his recording at a central website. Once the pattern recognition functionality in that website finds a match, it directs him to the website associated with that recorded content.

Typically, when a user is watching television or listening to the radio, he may be interested in particular content that just aired. However, he has no easy momentary access to the Internet to look up that content. In some instances, even if he has easy momentary access to the Internet, he does not want to look for more information relevant to that content because he wants to continue watching/listening to the broadcast that is airing. In these cases, the electronic card can be used to record an audio clip of the broadcast. By doing so, he has stored a virtual bookmark to a web address.

Later, at his convenience, he can access the web and go to a central website. This central website has a pattern recognition functionality. When the user plays back the recorded audio clip, the pattern recognition software attempts to find a match. When it finds a match, this match is associated with a table that contains web addresses. At this point, this central website can redirect him automatically to this web address or simply display the web address for the user. This web address has more detailed information on the product/service

IPR2025-01150
Apple EX1071 Page 693

that was the subject of the broadcast he just recorded. If the broadcast was a commercial, the recording would allow the user to later be redirected to the webpage of the merchant associated with that commercial or even directly to the webpage of the product/service being advertised. If the broadcast was a TV program, the recording would allow the use to later be redirected to the webpage of the network or production company that produced that program, or even to a fan webpage of that particular TV program.

Multiple recordings can be stored in the electronic card so that in effect, the user is storing multiple "virtual bookmarks." They are analogous to bookmarks because web bookmarks on browsers allow the user to conveniently and quickly access a particular desired webpage without any searching. Similarly, the "virtual bookmarks" in the electronic cards allow the user to conveniently and quickly access a particular webpage without any searching effort by the user.

In another embodiment, the "virtual bookmark" can be used to make a realtime purchase on a home shopping network channel. When the user sees an item on the home shopping network channel that he wants to purchase, he records an audio clip while that item is on display on TV. The user would take this audio clip to his computer, access the home shopping network website, and playback the recording. When the pattern recognition software in the server detects a match, the user is given the option to purchase that item. Alternatively, the user could go to a central website where the pattern recognition feature redirects him to the home shopping network website based on the successful pattern match. Thereafter, the user navigates to the webpage containing the item or the redirection automatically takes the user to the webpage of that item.

5.2 SMART E-WALLET SYSTEM

In accordance with one embodiment of the present invention, a smart e-wallet application is provided which allows the user to use the electronic card in conjunction with a web browser to make on-line shopping faster and more convenient. Essentially, the smart e-wallet system according to one embodiment of the present invention allows the user to automatically launch a browser, send the user ID and password to the e-wallet server, and emulate the "fill" and "submit" buttons when the user is in a website's checkout line with the simple press of the switch in the electronic card. More details are provided below.

5.2.1 INSTALLATION

The smart e-wallet system comprises the e-wallet client software, the electronic card, software associated with the electronic card (DSP, sound card drivers, etc.) and an e-wallet server. The installation of the e-wallet client software and the electronic card software can be accomplished using standard methods. In one embodiment, the user would already have an electronic card that is sponsored by a merchant, portal, or some other entity that has an interest in distributing the electronic cards. The software installation process includes downloading the electronic card software from the website associated with the electronic card company and also downloading the e-wallet client software from the website associated with the e-wallet company. These two separate processes will now be described.

Referring to FIG. 29, a log server 296 and a registration server 295 are provided. In one embodiment, the log server 296 is operated by and associated with the electronic card company and the registration server 295 is operated by and associated with the e-wallet company. Alternatively, the log server 296 is operated by

IPR2025-01150
Apple EX1071 Page 694

and associated with an e-wallet company and the registration server 295 is operated by and associated with a typical web merchant. In other embodiments, both the log server 296 and the registration server 295 are operated and associated with a single company, whether electronic card, e-wallet, or web merchant/portal.

Typically, the servers are NT-based systems that use the IIS platform to handle Internet requests and feature a SQL server by Microsoft to manage and store the collected data. The log server 296 primarily handles user registration of the electronic card, installation of the software associated with the electronic card, and collects MIS data for later use and analysis.

As part of the registration and software installation process, the log server stores and updates a list of users and their corresponding electronic card IDs by name. Note that while the server knows each electronic card ID, it does not know or have access to the electronic card's secret key (i.e., MyEWallet password) which is generated by the hash function, as described further below in the security section of the patent specification. The log server also prepares the installation software and personal data file for each user. Finally, the log server stores and retrieves each user's usage characteristics.

To start the installation process, the user accesses a website that is associated with an e-wallet company, such as the website supported by registration server 295 in FIG. 29. The user may also be asked to provide other personal details including:

(1) full name (first, middle, last)
(2) email address
(3) electronic card number (or user ID)
(4) optional e-wallet profile name
(5) address 1
(6) address 2 (optional)
(7) city
(8) state/province
(9) zip/postal code
(10) home telephone number
(11) work telephone number
(12) interests/hobbies
(13) shopping preference
(14) household size
(15) household income
(16) Question for password
(17) Secret answer for password question

These are just representative information that the registration process requires. Some information may not be requested at all. In another embodiment, the user need not manually enter these information; rather, the information is stored in the electronic card itself and the mere activation of the card will provide this information to the server.

IPR2025-01150
Apple EX1071 Page 695

Since this registration server 295 is associated with the e-wallet company only, the registration server 295 takes the user to the log server 296, or the server operated by the company associated with the electronic card. After all, the e-wallet company provides e-wallet service and software to many different types of people, regardless of whether or not they have the electronic card of the present invention. The company associated with the log server 296 provides the service/software for the electronic card. Alternatively, the user may have gone directly to the website associated with the electronic card company first. However, as described above, if the user happens to go to the website associated with the e-wallet service first, that website will redirect the user to the website associated with the electronic card company.

The log server 296 delivers a registration web page that requires the user to enter the electronic card number. A dialog box can pop up to inform the user of the terms and conditions of the e-wallet/electronic card program. When the user agrees, the log server 296 delivers the software download page to the user. The user then downloads the software associated with the electronic card which can include the data file for personal information. An application file also includes a one-time code which is similar to the electronic card's transmission of the Series in the data stream. This one-time code is unique to each user and is used later in the smart e-wallet application for security purposes, as described further below. The user then subsequently installs the software using standard techniques, such as using an installation wizard program. The install wizard also tells the user how to install the microphone and test the microphone, sound card, and the electronic card. At this point, only the software associated with the electronic card is installed. This software is similar to software 114 of FIG. 11.

Finally, the installed software sends the user to the website associated with the e-wallet system. Here, the user name and password are entered by the installed software and the e-wallet client software is downloaded. The e-wallet client software can then be installed using its own techniques. The user is then notified that the installation of the smart e-wallet application has been successfully completed. The entire installation process takes only a few minutes (with a 33.6K baud modem).

Of course, the separate e-wallet company-sponsored registration server and the electronic card company-sponsored log server need not be two separate servers. Either, or both, companies can agree to operate a single server that provides registration for e-wallet and registration for the electronic card.

Alternatively, the user may purchase a disk or CD-based software package, which he then installs in the conventional manner. Also, the software could be bundled together with other pieces of unrelated software when the user purchases a computer from a store or directly from a manufacturer. Once installed, the user can proceed to the website associated with the e-wallet and/or electronic card and register.

The smart e-wallet system allows for multiple installations in multiple personal computers. Thus, a user could use the smart e-wallet system from the home and the office with a single electronic card. The installation procedure is as described above. However, a security mechanism is provided to ensure that the subsequent installations are legitimate. In the process of installing the software for the first time, the log server/registration server will provide the user three unique information options (i.e., question and answer). The user must provide a response to one of these options. In subsequent installations, the registration server/log

IPR2025-01150
Apple EX1071 Page 696

server will prompt the user with the same question. If the user provides a correct response, the server will allow the new installation to proceed.

5.2.2 OPERATION

An e-wallet is a convenient application that allows the user to shop and purchase items on the web with relative ease. Because the user had registered with the proper personal information such as name, address, phone number, credit card number, expiration date, and the like, the user's shopping experience is a painless and positive one. Indeed, this information may have already been entered by the card's provider. When the user is about to purchase some item at a website, he goes to the checkout line. Instead of filling out a form like he would normally do, he invokes the e-wallet application which contains all of his personal information. The e-wallet application would either fill out the form automatically for the user or deliver equivalent information to the website so that the sales transaction can be finalized.

Referring now to FIG. 29, the smart e-wallet application (which includes the e-wallet client software and the electronic card software) is a single tray application which is represented as an icon in the System Tray by the Windows OS if the application is active. Typically, the smart e-wallet application opens automatically on start-up. Of course, the user can turn off (i.e., close) the e-wallet application at any time after it has been opened by, for example, right clicking the tray icon and selecting "Exit." The icon will then promptly disappear from the system tray. Conversely, the user can manually open the e-wallet application from the Program Menu, or if a short cut has been provided on the desktop.

If the user has successfully registered with the e-wallet system (e.g., registration server 295 in FIG. 29), the user can use the electronic card 10 to gain instant access to a designated e-wallet "home" website and perform easy and secure purchases from that site. For the purpose of this patent specification, this designated "home" site is called MyEWallet.

First and foremost, the computer station 14 is powered up and running. Secondly, the sound system is also running properly and active. When the user clicks on the electronic card, the electronic card transmits a data stream which should be detected by the client software. The electronic card software portion of the smart e-wallet application checks for a valid transmission (i.e., user password). It the transmission is invalid, the user receives a security warning. If the transmission is valid, the smart e-wallet application performs any number of functions that is context-sensitive. For the most part, the smart e-wallet application checks the launch status (i.e., open or closed) of the web browser and the URL of the web page accessed. FIG. 30 shows a flowchart of this context-sensitive process.

The process starts at step 300. Step 301 checks to determine if the web browser is closed or opened. FIG. 29 shows a portion 290 of the computer screen that displays the web browser. If the web browser 291 (in FIG. 29) is closed, the smart e-wallet application launches the PC's default browser at step 302, accesses the MyEWallet website at step 303, and logs the user into the website (steps 306, 307). If the user is properly registered, the web page opened will be the user's personalized web page. The e-wallet interface 292 (in FIG. 29) will appear with the user ID and password automatically filled in by the smart e-wallet application as shown in step 306. Thereafter, the user ID and password are delivered to the MyEWallet website at step 307. If

IPR2025-01150
Apple EX1071 Page 697

proper, the user has now been logged into the MyEWallet website. The user can browser and shop as he pleases as indicated at step 308. At this point, the user's e-wallet which contains his personal information can be used to fill out a form or otherwise deliver these information to the website to finalize any sales transaction. Note that the smart e-wallet application fills in the user ID and password and submits them automatically to the MyEWallet server to log in. Thus, the mere press of the switch in the electronic card automates an otherwise manual process.

Returning to step 301, if the web browser is open, the smart e-wallet application checks the URL of the current web page at step 304. If the current URL is not MyEWallet, the smart e-wallet application opens another window at step 305, accesses the MyEWallet web page at step 303, and logs in the user as described above. As in the first case above, the smart e-wallet application fills in (step 306) and submits (step 307) the user ID and password automatically. At this point, the user proceeds with his web browsing and shopping in this second window. The previously opened first window is not associated with the smart e-wallet system so any tasks performed in this first window will not benefit from any automated tasks already performed by the smart e-wallet system. In another embodiment, the smart e-wallet system will access the MyEWallet web page and log in the user in the first window, without opening up another window. Thus, in this alternative embodiment, step 305 is eliminated.

Returning to step 304, if the browser is already opened to the MyEWallet URL but the user did not log in yet, the smart e-wallet application proceeds to fill in the user ID and password in the e-wallet interface 292 (in FIG. 29) at step 306, followed by submission of the user ID and password to the MyEWallet server at step 307. If proper, the user is logged into the MyEWallet system and can now take advantage of the e-wallet system.

Once the user is logged into the MyEWallet server, the next click of the electronic card performs other tasks. If the application is in the "fill" stage, the smart e-wallet application will fill out the form on the current web page, just as if the user had clicked on the "fill" button with the mouse. If the form is completely filled out, the web page would now be in the submit stage. The next press of the electronic card emulates the press of the "submit" button.

The user can, of course, fill out the form himself. If any portion of the form is filled out, the smart e-wallet application detects that the web page is in the "submit" stage. If the browser is already opened to the MyEWallet URL and the application is in the "submit" stage, the smart e-wallet application will submit the completed form on the current .html page to the appropriate server, just as if the user had clicked on the "submit" button with the mouse.

During these user transactions with web merchants and portals, the smart e-wallet application sends usage information to the log server 296. Specifically, whenever the electronic card is activated, the log server 296 gathers the following information:

(1) electronic card serial number (or individual ID)

(2) group ID (i.e., sponsoring web merchant or portal)

(3) server date and time

IPR2025-01150
Apple EX1071 Page 698

(4) PC date and time

(5) Counter value (or card click number)

(6) Action performed by card (e.g., open browser, login to wallet, press "fill" button)

(7) URL of the website visited by the user

These data can be used later to monitor user on-line behavior so that targeted marketing and advertising schemes can be employed. Additionally, if the user has some technical or other problems with the system, the appropriate customer service representative can assist the user more effectively with these stored historical data.

5.2.3 SECURITY

Generally, the e-wallet application in the client computer station performs two checks – (1) card signal is valid based on signal structure, and (2) card transaction is valid based on the counter value. These checks must be performed in realtime whenever a sound is detected by the sound system of the PC. In one embodiment, the client computer station checks both card signal transmission validity and card transaction validity. In another embodiment, the client computer station performs card signal transmission validity and a remote server performs card transaction validity.

The sound system, and in particular the microphone, is active in the computer station. Accordingly, any signal or noise can be picked up by the microphone. Noise or other random sounds should not trigger the operation of the e-wallet client application. To trigger the operation of this e-wallet system, a proper signal from the electronic card has to be detected.

As described above in the data format section of this patent specification, the electronic card transmits f0, f1, sync byte, known byte, the data, and the CRC, along with start and stop bits at every byte interval. The data portion consists of the individual ID and the Series (which is generated by applying DES3 encryption on the key, group ID, and counter value). The transmitted signal that is generated by the card has a unique structure, which the client software in the PC can use to detect a valid signal.

The e-wallet client software also has a table that was generated from a DES3 operation on the card signal so that the client can perform a pseudo decryption function. This table has the following fields – card signal, counter value, and user password. Also, the e-wallet application keeps track of the last counter value that was transmitted by the electronic card (and detected by the e-wallet application) as an additional check, as explained further below. In one embodiment, the table includes 3,000 possible card signals that could be detected by the e-wallet client software. Based on the various possible card signals, the table provides corresponding counter values and user passwords.

When a signal (or noise) is detected, the e-wallet application first determines if the signal is a valid electronic card transmission. If it is not a valid signal, the signal is ignored and no further processing is necessary. If, however, the signal is valid, the e-wallet application determines whether the card transaction is valid. The e-wallet application determines card transaction validity based on the counter value in the table based derived from the card signal structure. If the derived counter value in the table is greater than the counter value that was previously stored by the e-wallet system, then the card transaction is considered valid. Why?

IPR2025-01150
Apple EX1071 Page 699

The electronic card increments the counter value in the card each time the card switch is pressed. Thus, if the current counter value of my card is 24, this implies that I had pressed the card 23 previous times. This counter value of 23 is currently stored in the PC. When the user presses the electronic card, the counter value of 24 is transmitted to the PC and the card increments its internal counter value to 25. This 24th press of the electronic card is a valid transaction because the transmitted counter value 24 is greater than the stored counter value of 23.

If, however, an interceptor recorded the electronic card transmission while the user pressed the electronic card when the 24 counter value was transmitted, he may attempt to use this recording to break into the user's account. At this point, the PC's counter value is now 24 because the user had just transmitted the counter value of 24. If the interceptor attempts to log into the user's MyEWallet account by playing back the sound recording to the microphone, the sound recording would transmit a signal that included the counter value of 24. The PC's counter value is 24. Since the interceptor's signal's counter value of 24 is not greater than the PC's counter value of 24, the card transaction is considered invalid.

Once the card transaction is considered valid, the smart e-wallet application performs a two-factor on-the-fly authentication operation to generate a MyEWallet password. As mentioned above, the electronic card transmits a data stream which, for the most part, is constant except for the counter value. Accordingly, each transmission of the data stream in the electronic card contains a one-time code and the individual ID (or card serial number). Also, a one-time code is also generated by the server that provided the software download during the smart e-wallet application and provided to the client computer station. This one-time code is stored in the hard disk during the software installation and is different for each user. Upon determination of a valid transmission and a valid transaction, the smart e-wallet application takes the detected one-time code from the electronic card and the hard disk-stored one-time code and hashes them together to generate a MyEWallet password. In another embodiment, a simple XOR operation could be performed on the card's one-time code and the hard disk-stored one-time code to generate the MyEWallet password.

Multiple benefits are provided by this on-the-fly authentication scheme:

(1) Only the electronic card in accordance with the present invention can be used to log into the MyEWallet server and access the user's account. No other card can achieve successful authentication.

(2) Since the hashing function generates the MyEWallet password from both the electronic card's transmission and the one-time codes on the hard disk, the password does not "exist" in either location; that is, the MyEWallet password is neither in the electronic card nor the client computer station's hard disk. A hacker/virus will not be able to retrieve the electronic card's secret ID (or password) from examining the user's computer hard disk since the secret ID (and password) are not stored there. The secret ID and password are not stored in the application's .exe file. Similarly, even if someone stole the card, the MyEWallet password cannot be determined since the MyEWallet password is generated anew from the information from the electronic card and information from the computer station.

IPR2025-01150
Apple EX1071 Page 700

(3) Because of the use of the always incrementing counter value, the mere recording by an interceptor of one or more of the electronic card's transmission and the subsequent playback of that recording will not enable the interceptor to gain access to the smart e-wallet system. As described above, the smart e-wallet system only accepts card transactions with a counter value that is higher than the counter value stored in the smart e-wallet system.

(4) Because the one-time code transmitted from the electronic card is unique for every transaction, the user need not remember the password since the smart e-wallet system generates the password for each transaction.

In another embodiment of the present invention, the counter value is tracked by the log server. By doing so, a particular security problem associated with PC-based tracking of the counter value is eliminated. To elaborate on the problem, assume that the smart e-wallet application is installed and running in two PCs – one at home and the other at the office. One day, the home PC's counter value is 15 and the office PC's counter value is 14. The user uses the office PC to purchase various items on the web. As a result, the counter value in the office PC is now at 18. During the transaction where the counter value 17 was transmitted to the office PC, an eavesdropper recorded this card transmission. He could then take the recording to the user's home and if he somehow accessed the user's home PC, he could log into the smart e-wallet system and access the user's account. Why? The recorded transmission includes the counter value of 17. The home PC checks for a valid transaction by comparing the received counter value with the last counter value in the computer, which is 15 in this example. Since the received counter value (i.e., 17) is greater than the last counter value (i.e., 15) in the computer, the smart e-wallet system considers the transaction to be valid.

In contrast, a server-based solution to the tracking of counter value would eliminate this problem altogether. Because the server tracks the counter value, any recording of transmissions and subsequent playback would not enable the interceptor to access the MyEWallet account. The counter value in the recording would not be greater than the counter value in the server, regardless of which computer (office or home) is used. Similarly, this problem would not be an issue at all even if the PC kept track of the counter value if the user used only one computer for all transactions.

As mentioned before, the primary purpose of the authentication server is to authenticate users. To this end, the authentication server maintains a database of the following that information associated with each user: DES3 keys; counter values; electronic card individual ID (or card serial number); electronic card group ID; and other secure personal information such as user name, password, credit card number, credit card expiration date, and the like. When a user wants to log into the smart e-wallet system, the user presses the switch on the electronic card. This transmitted data is included in the request that is delivered to the server over the Internet. When this request is received, the server checks the individual ID (serial number) of the card transmission. Remember, the individual ID is not encrypted. The server then decrypts the data using DES3, checks to make sure that the individual ID is associated with the group ID, and then checks the counter value. Refer to FIG. 32 and the corresponding discussion below.

5.3 WEB TRANSACTIONS AND AUTHENTICATION

IPR2025-01150
Apple EX1071 Page 701

The use of the electronic card in accordance with one embodiment of the present invention provides many benefits for on-line web transactions. One problem with the current method of conducting sales transactions over the web is that merchants and banks are concerned about card presence issues. In other words, because the merchants and banks cannot get your signature on the sales transaction slip like conventional store purchases, the risk of repudiation of that sales transaction falls on the merchant. How do the merchants know that you are who you say you are and are using your card as opposed to someone else's card? If a sales transaction is repudiated, the merchant does not get paid; the credit card issuing bank loses some customer satisfaction; the acquirer bank loses some transaction cost for processing this repudiated transaction as well as experiencing some annoyance; and the relationship between the acquirer bank and the merchant can potentially deteriorate.

Generally speaking, the credit card fraud rules dictate that when a transaction is "card present," the risk of fraud falls on the issuer. In a conventional store purchase, the merchant processes the customer's credit card by checking with the issuer before completing the sales transaction. When the credit card is cleared, the merchant finalizes the sales transaction. This is done in realtime. On the other hand, when the transaction is "card not present," the risk of fraud falls on the merchant. Usually, these transactions are the telephone or Internet orders where the reliability of the credit card actually being present is low.

By using the electronic card of the present invention, the card presence issues are significantly reduced. With the appropriate client side and server side software, the only transactions accepted by the participating merchants, acquirer banks, and issuer banks are those involving the electronic card. The issuer bank (or even the credit card organizations) can require the merchant to only accept the electronic card of the present invention or else the risk of fraud falls on the merchant. Customers will no longer be able to merely type in the credit card number because these participating institutions will want some greater assurance that the credit card is present during the sales transaction.

For example, assume that a company JKL, Inc. is a web portal. JKL has been able to successfully sign on numerous merchants onto its website. In addition JKL has provided the electronic card of the present invention to all of its members. They instruct the member to use the electronic card for all sales transactions conducted on their portal or with merchants associated with the portal. With such an arrangement, the acquirer bank for merchant XYZ Company agreed to pay the merchant XYZ Company the full amount of all sales transactions conducted with the electronic card. This acquirer bank believes that the use of the electronic card minimizes card presence issues and the transaction is trustworthy. Similarly, the user of the electronic card is secure in knowing that his credit card number is not being broadcast throughout the web where it could be potentially intercepted and used elsewhere. He knows that purchases made with merchants associated with the JKL web portal are bona fide legitimate purchases that he made himself (or an authorized agent).

Similarly, a web merchant such as XYZ Company has a website. It provides the electronic card to all of its members. The company requires use of the electronic card to conduct sales of its items. It sets up this policy to protect its members from unscrupulous credit card thieves and to ensure that its acquirer bank will guarantee payment for all sales transactions. The risk of repudiation is low for the merchant.

IPR2025-01150
Apple EX1071 Page 702

The following sections provide details into the credit card infrastructure that the electronic card of the present invention supports, some on-line authentication applications, some off-line authentication applications, and other web-related applications.

5.3.1 CREDIT CARD INFRASTRUCTURE

Referring now to FIG. 31, a simplified diagram shows the relationship among the various players for credit card transactions. The customer 314 normally obtains a credit card from his issuer bank 313 (e.g., CitiBank). He may have obtained the credit card by filling out an application or the issuer bank pre-approved the credit card and sent it to the customer. Regardless, the customer 314 has an account with the issuer bank 313. For all his transactions with the credit card, the customer 314 receives periodic statements of his activities from the issuer bank 313.

The customer 314 purchases merchandise or some service from a merchant 311 whether web-based or conventional store-based. If cash is used, no credit card-related issues are raised. However, if the customer uses a credit card, the various parties shown in FIG. 31 are involved at some point or another. With the credit card, the customer 314 can purchase goods and services from the merchant 311. Sometimes, this sales transaction can be legitimate or illegitimate (e.g., stolen credit card). But for the most part, this sales transaction is usually finalized.

In order to be paid for a given sales transaction involving a credit card, the merchant 311 sets up an account with an acquirer bank 312. The merchant can select any number of acquirer banks to conduct its business. The acquirer bank 312 will honor the credit card-based sales transaction and pay the merchant 311 so long as the merchant 311 complies with the rules governing their business relationship. For example, the acquirer bank 312 may require that a signature of the customer 314 be provided on the sales slip. For web transactions, the acquirer bank 312 may require certain security signing authorities be used to decrease the risk of repudiation. The particular deal between the merchant 311 and the acquirer bank 312 can vary but usually involves a small flat fee per credit card sales transaction or a small percentage (with a cap on the actual dollar amount) per transaction. In any case, the acquirer bank 312 also makes some money out of the sales transaction between the customer 314 and the merchant 313.

Of course, the acquirer bank 312 ultimately gets paid by the customer's issuer bank 31, who in turn require corresponding payment from the customer, usually by check or money order. The issuer bank 313 also makes some money from the interest from customers 314 who do not pay the full amount of the credit card balance by the due date.

Governing the behavior of the issuer bank 313 and the acquirer bank is the government (not shown) and the appropriate credit card organizations 310, such as VISA and MasterCard. Of course, the government regulates the banking industry heavily to protect consumers and the banks themselves. The credit card organizations 310 control everything from the credit card itself (e.g., physical specifications, electrical specifications, logo placement, photo placement, embossing) to credit card readers and the communications protocol for on-line verification. Accordingly, the credit card organizations 310 place additional restrictions on the issuer bank 313 and the acquirer bank 312.

IPR2025-01150
Apple EX1071 Page 703

At times, a particular sales transaction can be disputed by the customer 314 because: (1) the sales transaction is legitimate but the customer cannot remember the transaction; (2) the sales transaction is not legitimate and of course, the customer cannot remember the transaction; (3) the sales transaction is legitimate, the customer remembers the transaction, and the customer still wants to dispute the transaction out of criminal intent; or (4) the sales transaction is legitimate, the customer remembers the transaction, and the customer disputes the transaction price. To resolve the dispute, the customer 314 can call the issuer bank 313. For low priced items, the issuer bank 313 typically credits the customer's account regardless of whether the dispute or the sales transaction is legitimate or not. In other instances, however, the issuer bank may resort to actual proof that the customer's signature is provided on the sales receipt. For web purchases, no signature is available to serve as such a proof. Any number of people with the credit card number could have initiated and completed that sales transaction over the web.

The electronic card of the present invention alleviates these card presence issues. Various card distribution models are possible within the framework of this credit card infrastructure. The electronic card can be distributed or otherwise sponsored by any of the following players: (1) merchant, (2) issuer bank, and (3) credit card organization.

First, a merchant, whether web merchant, web portal, or some other company with a web presence, can distribute the cards to its members and potential members. If this company does not get involved in the distribution of the electronic cards, it can sponsor the electronic cards instead. Thus, members can use the electronic card to purchase goods and services over the web at any website associated with this electronic card. Of course, if multiple merchants are sponsoring this electronic card, the member customer can use the electronic card at any website associated with these sponsoring merchants to make a purchase.

Similarly, an Internet Service Provider (ISP) can sponsor or distribute these electronic cards to its subscribers. In one embodiment, the ISP indicates to its subscribers the participating merchants that accept the electronic card as a means of payment. Initially, this list of participating merchants may be fairly limited but as more and more subscribers use the electronic card, more and more merchants will accept the electronic card as the payment means instead of (or in addition to) the conventional credit card.

In another embodiment, the ISP could set up the authentication server with the smart e-wallet system. The subscriber initially logs into the authentication server at the ISP and once authenticated, the subscriber can browse the web as usual and shop on-line. When the subscriber encounters a purchase form as a result of selecting a merchandise and going to the checkout line, the subscriber can use the form fill function of the smart e-wallet to complete the sales transaction. Refer to the smart e-wallet system description above.

Second, the electronic card could be distributed by the issuer banks 313 themselves. So, as customers 314 apply for credit cards, they receive these electronic cards instead. However, these electronic cards could be used like the conventional credit cards because the electronic cards comply with standard credit card form factor requirements. To the average customer, these electronic cards are no different from the standard conventional credit cards with the magnetic strip, logo and embossed name, credit card number, and expiration date.

IPR2025-01150
Apple EX1071 Page 704

Third, and related to the second point above, the electronic card could be sponsored by or otherwise supported by the credit card organizations (e.g., VISA, MasterCard, American Express). Thus, all issuer banks must provide electronic cards that comply with the requirements specified in this patent specification when distributing new or replacement credit cards to their respective member account holder customers.

In another embodiment, the issuer bank can bundle an online service membership with the credit card account. So, when a customer applies for a credit card, the issuer bank sends the customer the electronic card (which can also function as a conventional credit card with the magnetic swipe) and an automatic online service membership. The first use of the electronic card (when the user has accessed the online service company's website) could affiliate the user with the account. With this bundling, the online service provider could keep track of various user-related usage data. The online service provider could then send membership (and cardholder) usage data to the card issuer bank.

The principle advantages of this bundling scheme to banks is that they increase the frequency and depth of interaction with their cardholders. The effect is to heighten the cardholders' awareness of the issuers brand and services. This could lead to interesting opportunities, such as maintaining more detailed databases on use habits to help make more tailored offers of additional services to the cardholder. The increased presence of the card in users' everyday experiences could also lead to increased transaction volumes.

Moreover, the fact that users activate their cards more regularly than they would use a simple payment card leads directly to applications not otherwise possible. Issuers of cards under the present invention, by virtue of network servers used to authenticate the cards, can be made aware of when cards are being activated. Since the cards are being used in the context of Internet sessions, issuers may assume that cardholders will be present near their computers for some limited period following card activation. During that period of time, issuers can use the opportunity of a cardholder's presence to exchange useful messages with the cardholder. Exemplary messages include notifying cardholders of upcoming bill due dates, notifying cardholders of past due dates, and notifying cardholders of special promotional offers or discounts. Ideally, the cardholder would also provide a mechanism for the user to respond immediately. Because the issuer knows that the user has a card presence, the issuer can even use that opportunity to conduct higher risk transactions than they normally would in a card-not-present atmosphere. Because of the presence of the card, the issuer might, for example, allow balance transfers, withdrawals or bill payments to be paid online.

Another embodiment for increasing interaction between issuers and cardholders integrates the cards with "push" technology, such as is known in the art, for sending a priori messages to Internet users. At any point during an Internet session (whether or not a card has been activated but preferably after), alerts that call for card activation can be pushed out to the cardholder over the Internet. Exemplary alerts of this kind include notification of successful or unsuccessful bids for auctions or 'reverse auctions' (e.g. eBay, Priceline), as well as stock trading alerts. Through integration of "push" technology to the electronic card's client software, alerts can be conveniently delivered to the cardholder. As is known in the art, "push" technology can deliver such information as messages, content and patches to client software, without direct client request.

IPR2025-01150
Apple EX1071 Page 705

In one embodiment, a cardholder is pushed an alert, indicating that her bid to a reverse auction was not accepted. The user could then be prompted to activate their electronic card to authenticate their re-entry to the bidding system in one step. This scenario saves time in the re-bid process, and can reduce both customer drop-off rates in re-bidding, as well as re-bid repudiation. This scenario provides advantage over the current system of unauthenticated, email alerts. In another embodiment, the user is pushed an alert indicating their successful bid. The user could then be prompted to activate their electronic card in order to print a record of their successful bid.

In another embodiment, the integration of the card with push technology provides users with the opportunity to pay bills securely. The client software could be configured by the user or service provider to receive bill payment alerts from merchants, utilities or financial services. For example, bill payment and presentment services could push payment alerts to customers, to remind them to pay their telephone and electrical utilities bills. In a similar fashion, online financial service companies could remind users to make mortgage or margin payments, or to contact customer service regarding returned checks.

The user authentication functionality of the card enables secure payment of such bills in direct response to these prompts by operating a card.

5.3.2 ON-LINE AUTHENTICATION

In accordance with one embodiment of the present invention, the on-line authentication works in a manner similar to that of the smart e-wallet system described above. Generally, the electronic card interactive system can involve some checks locally at the client PC or remotely at the authenticating server.

For the local check, when the user presses the switch in his electronic card, the PC processes the signal and checks for electronic card transmission validity. If the structure of the signal detected by the PC's microphone and sound system is similar to that of the electronic card's signal, then the signal is presumed to be valid. Thereafter, the PC checks for electronic card transaction validity. Here, the PC merely checks whether the counter value in the signal transmitted by the electronic card is greater than the counter value last stored by the PC. If the transmitted counter value is indeed greater than the counter value stored in the PC, then the card transaction is presumed to be valid. In another embodiment, the counter check will occur at the authentication server, instead of at the local client PC. So far, the checks have only been made locally at the client PC. The remotely located authentication server will also perform checks of its own.

To perform the remote check, an authentication server includes a database, decryption facilities, and authentication logic. Refer to FIG. 32. The authentication process begins at step 320. The database includes the user names, DES3 keys, and other secure information (e.g., password, credit card number, expiration date, group ID, counter value, individual ID). Once the electronic card transmission passes the local client checks, the data from the electronic card transmission is delivered to the authentication server as an authentication request at step 321.

The data stream in the electronic card's transmission, which is included in the authentication request, includes an encrypted portion and an unencrypted portion. The encrypted portion includes the DES3 key, group ID, and counter value. The unencrypted portion includes the individual ID. The authentication server takes the

IPR2025-01150
Apple EX1071 Page 706

unencrypted individual ID and checks if a corresponding user is associated with that individual ID at step 322. If so, the authentication server decrypts the encrypted portion of the data stream at step 323. If not, the authentication server returns a security error message or a message otherwise indicating that access is denied at step 327 before ending at step 328.

At step 324, the authentication server checks if the group ID in the decrypted portion of the authentication request corresponds to the individual ID just verified. If that check is passed, the authentication server checks if the counter value in the authentication request is greater than the stored counter value at step 325. If not, access is denied at step 327. If the counter value in the authentication request is greater, then the authentication has been successful. The new counter value is then stored in the database associated with this user. This counter value check at the authentication server is in contrast to another embodiment where the counter value check occurs at the local client PC, as described above. Once the user has been authenticated, the authentication server returns a confirmation that indicates that authentication has been successful at step 326. This authentication process ends at step 328.

Once authenticated, the user is free to shop, purchase, and otherwise browse on the web. For e-wallet applications, the smart e-wallet application facilitates the form filling function in finalizing sales transactions. Smart e-wallet applications are provided above in the smart e-wallet system section. For other applications, the authentication process merely allows a user to access and other wise complete the sales transaction after pressing the TX switch on the electronic card. For example, once a user has shopped and selected an item to purchase from a website, the website delivers a purchase form to fill out. The user does so. However, instead of the credit card number, the user is asked to take out his electronic card and press the button. The user does so. When both the user's PC and the remote authentication server has authenticated the card transmission, the website will either return a web page that states "Thank you for your order. Your order number is 1234ABC" where the return confirmation message from the authentication server also finalized the sales (by emulating the "submit" button on the web page). Alternatively, a message is displayed indicating that the authentication process has been successful. The user then proceeds to submit the form manually and complete the sales transaction in the conventional manner.

This authentication model can be implemented in several different ways. The authentication server can be located or otherwise maintained and operated by several entities: (1) third party (e.g., private security based company, bank, or credit card organization), (2) merchant or web portal, or (3) ISP. These implementation strategies will now be discussed.

For the merchants, a convenient implementation strategy would involve some third party such as the hypothetical company RST Corporation which dedicates one or more authentication servers for various merchants. The third party could also be a bank (normally the issuer bank) or the credit card organization. Thus, the disruption to the merchants' web system would be minimized. Customers merely access RST's website to shop. When these customers have selected some merchandise to purchase, they merely take them to the checkout line on the website. Although the sales procedure varies from merchant to merchant, invariably

IPR2025-01150
Apple EX1071 Page 707

the customers get to a web page where they have to provide some personal details such as name, shipping address, and credit card number.

At this point, the customer is asked to take out his electronic card and press the button. When he does so, his PC handles the local authentication as described above. When he passes the local authentication checks, an authentication request is delivered to the IP address associated with the third party's authentication server location. Here, the third party's authentication server handles the authentication of this user. If authentication fails; access is denied and the merchant's server is notified in real-time of this condition. The merchant would then refuse this particular user's purchase request because, for various reasons, this user's account is delinquent, the account does not exist, the transaction is not valid because the counter value is not valid (perhaps the user was using a recording of another person's card transmission), the group ID is not valid, or the serial number (individual ID) is not valid. Alternatively, the merchant would assist the user in setting up an account.

If, however, the authentication server returns a confirmation to the merchant's server in real-time, the merchant's server would then allow the user to manually continue with the purchase process since the merchant deems this user to be present and in good standing. Alternatively, the confirmation from the authentication server to the merchant's server may also trigger the automatic completion of the sales transaction. The authentication request associated with the user pressing the switch on his electronic card essentially emulates the "submit" button that would normally be present in these sales forms.

This implementation strategy represents an advantage over the current on-line transactions because the merchants would receive transaction confirmation from a trusted source. This trusted source is the third party which not only confirms card presence during the sales transaction, but also checks various aspects of the account – from account delinquency to non-existence of the account. The frequent contact between the third party and the merchant and the added fraud-protection over conventional "card-not-present" transactions strengthen the relationship between the third party and the web merchant. If the third party is the issuer bank, the relationship between the web merchant and the bank would improve. For example, a credit card issuer of electronic cards under the present invention could offer to assume the risk of those "card-not-present" transactions only to merchants participating in the issuer's e-wallet, or e-commerce portal service. The effect would be raising the interaction with cardholders and transaction volume, without taking on real fraud risk, since the present invention provides adequate assurance that a transaction is, in actual fact, card-present.

For the second implementation strategy, the merchant and/or web portals themselves operate the authentication server independent of any third party. In this case, the database it maintains only keeps track of its own members. However, this implementation strategy may be less attractive to merchants who are more concerned with improving and maintaining their own content, instead of maintaining and operating an authentication server. However, it is a viable strategy for those merchants with the resources to support this separate server.

For the third implementation strategy, an ISP maintains and operates the authentication server. If only a few ISPs participate in this venture, only those subscribers in a region serviced by that ISP can benefit from the electronic card interactive system. To gain universal acceptance, many ISPs located throughout the world

IPR2025-01150
Apple EX1071 Page 708

must participate in this venture because web merchants are located across the web. However, it is possible to have the ISP authenticate the user when the user launches the browser. Upon accessing the ISP, the user will be asked to press the electronic card switch for authentication. Alternatively, the user will be asked to press the electronic card switch to launch the browser followed by other functionality in a manner similar to the smart e-wallet system described above. Thereafter, the smart e-wallet application will fill out any form for the user when he is about to purchase an item from a web merchant.

Ideally, the payment card associations (Visa, Mastercard, American Express, Discover, etc.) would agree that transactions effected by cards under the present invention were actually considered "card present," and honored to the same extent as any other card-present transactions. But also note that under any of these schemes for online authentication, those payment card associations need not make any change to their own transaction processing systems in order for merchants under the current invention to enjoy the benefit of card-present transactions. In the prior art, the payment card associations' systems are equipped to identify in real time whether a transaction is card-present (in store) or card-not-present (via phone or Internet.) Under the current invention, a merchant could be provided with evidence for its records that a transaction was effected not by manual entry of a card number, but by an actual transmission from a physical card. If a cardholder does not report a card lost or stolen, and then later attempts to repudiate the transaction, the merchant would have in his records good evidence that the transaction was genuine.

5.3.3 OFF-LINE AUTHENTICATION

In accordance with another embodiment of the present invention, off-line authentication works in a manner similar to that of the smart e-wallet system and the on-line authentication described above. The difference with the off-line authentication is that confirmation is not provided to the merchant in real-time.

In one embodiment, the confirmation would be sent to the merchants via email or through some other non-real-time means. In this way, the merchant and the customer could deal with each other in the conventional manner without waiting for the third party authentication server to complete the authentication check. But, before the merchant ships the merchandise or provides the service to the customer, the merchant would check to make sure the confirmation has been received. If the confirmation has been received, that sales transaction has been approved by the authenticating third party. If the confirmation has not been received, the merchant would hold shipment of the merchandise or otherwise refuse to provide the requested service. The third party could also keep the confirmation (or lack of confirmation) report for each sales transaction for future reference without affecting shipment or providing the service.

Like the real-time confirmation example described above, this embodiment represents an advantage over the current on-line transactions because the merchants would receive transaction confirmation from a trusted source, albeit in non-real-time fashion. This trusted source is the third party which not only confirms card presence during the sales transaction, but also checks various aspects of the account – from account delinquency to non-existence of the account. The frequent contact between the third party and the merchant and the added fraud-protection over conventional "card-not-present" transactions strengthen the relationship

IPR2025-01150
Apple EX1071 Page 709

between the third party and the web merchant. If the third party is the issuer bank, the relationship between the web merchant and the bank would improve. No major changes are required for the merchant's web site and the web server for the non-real-time authentication.

In another embodiment, the authentication server can assist those merchants who, for various reasons, do not want to make any changes to his system. The merchant may not even want to do the simple act of turning on the authentication flag in his server. Perhaps the merchant does not even want to perform any authentication. How do you provide authentication services to these merchants?

In this embodiment, the authentication server would place the confirmation number in a form field that is normally not used in most, if not all, of the purchase forms that websites require customers to fill out to place an order. In this embodiment, the ADDRESS LINE #2 would be used. This field is hardly, if ever, used by customers. In other webpages, a NOTES field is provided. The sequence of operations are as follows:

When the customer has selected an item to purchase on the web, he goes to the checkout line and encounters a form. He must fill out this form to place the order with the web merchant. In most of these forms is a field that is typically called "ADDRESS LINE #2." With the smart e-wallet application or other special client software that is designed for use with the electronic card, the customer takes out his electronic card and presses the button. The electronic card then transmits its data to the PC via the PC microphone. The client software delivers this data to a third party authentication server which performs the authentication in a manner described above. The authentication server then sends a transaction confirmation number back to the customer's PC client software, which fills in the ADDRESS LINE #2 field with this transaction confirmation number in the merchant's purchase order form page.

In one embodiment, the transaction confirmation number is merely a randomly generated number. In another embodiment, the transaction confirmation number is actually a digital signature of the order number and a public key. A digital signature is used to authenticate the identity of the sender (i.e., the third party authentication server) or the signer of the document. The use of the digital signature ensures that the signed document cannot be easily repudiated, cannot be imitated by someone else, and can be easily time-stamped.

A special merchant software can process all the purchase forms and associate customers with successful or unsuccessful authentication results. Thus, after completing the sales transaction, the third party authentication server places the transaction confirmation number on the purchase order form via the special client software located in the customer's PC. When the customer finalizes the sales, the purchase order form is submitted to the merchant. At the end of the day, the merchant has electronic versions of all the purchase order forms that have been filled out by customers as they purchased the merchant's products or services.

The special merchant software would process all the purchase order forms and decipher the transaction confirmation number provided on the ADDRESS LINE #2 field off-line. The special merchant software would then generate a report that indicates the success or failure of the authentication for each customer. The nature of the transaction confirmation number would provide this indication. The merchant can use this report to hold the shipment of the item purchased. Of course, the merchant would check with the customer to inquire why the

IPR2025-01150
Apple EX1071 Page 710

authentication failed and may even assist the customer in repairing the situation if the situation is reparable (e.g., insufficient credit limit, expired electronic card).

This embodiment of using the ADDRESS LINE #2 field represents an advantage over current on-line transactions because it provides merchants a transaction confirmation number from a trusted source. This transaction confirmation number indicates that the customer had the electronic card associated with a particular customer's credit card account present when he made the web purchase. Merchants can use this transaction confirmation number to validate the customer in real-time, if necessary, or any time thereafter. This information provides the proof necessary to counter later repudiations. This method prevents such fraud techniques as credit card number generators or stolen credit card numbers since the actual credit card number is not delivered over the Internet. Also, no changes are required in the merchant's web page or server.

In accordance with another embodiment of the present invention, some additional information is provided in the credit-card field in conjunction with the standard credit card number for authentication purposes. For example, a one-way card with an e-wallet software is provided. Whenever the user makes a purchase, he presses the button on the electronic card. With the button press, the card calculates the next number in a series, and sends it to the PC. The PC turns on the e-wallet engine and fills the address and credit card fields. However, instead of filling the regular credit card number, it fills a special code.

An exemplary code is designed as follows: 4 constant digits to designate the card number as a special kind, 6 digits for the card ID, and 6 digits of the card-sponsoring company's ID, and 6 digits from the pseudo-random series generated by the card (based on the counter value).

The merchant receives the card number and sends it through some channel to the acquirer bank as is typically done today. When the acquirer bank sees the special 4 first digits, he queries the server to checks whether the last 6 digits are valid according to the counter value. If two identical codes are received (same counter value), then a theft or some fraud has occurred, or if the code received is too old, then there was an attempt for theft. The server is located at the issuer bank and instead of listening for one credit number per user as is normally done, it listens for a unique credit card number per transaction.

5.3.4 PASSWORD GENERATOR

For this application, the electronic card and the PC client software are used to generate an ever-changing password to the user to access a web page. The electronic card contains a display for presenting the password to the user. The user then manually enters the newly generated password with the keyboard to enter the web page.

In this embodiment, the password generator includes the electronic card with a display, the special client software, the web browser, and the server that performs the authentication. Typically, the user browses the web and attempts to access a web page that he may or may not have an account with. If he has an account with this web page, he also has the electronic card provided to him by this merchant or some other sponsoring company that work. For various reasons, the access is limited to those users with open accounts and the electronic card. When the user requests access to this web page, the web page informs him that access is limited to members in good standing.

IPR2025-01150
Apple EX1071 Page 711

The web page asks the user to start the authentication process and when done, to enter the newly generated password before submitting the authentication form back to the website. The user enters his name (or ID) and perhaps a password. The server associated with this web page then sends an encrypted number to the user's PC via the web browser. This number is also accessible by the special client software. In another embodiment, the number is not encrypted. The special client software in the PC sends this number to the user via the PC speakers. This number can be based on the counter value or a randomly generated number. The counter value can be accessible by the server because the account database includes the counter value for this particular user.

The electronic card detects the encrypted number, decrypts it with its private key, and generates a password. This password is then presented on the electronic card's display. Concurrently, the web site server has also generated a password since the password-generating functionality is analogous in both the electronic card and the server. At this point, the user enters the password with the computer keyboard into the authentication form on the web page and submits it. When the server receives this password, it compares this received password to the password it generated internally. If a match exists, the user is allowed to access the web page. If a match does not exist, the user is denied access to the web page.

This approach provides several advantages over the conventional password-related approaches. Because the password is different for each transaction, the system is more secure. The user need not remember the password and even if one password was stolen somehow, that thief could not use it for another transaction. Also, the password does not exist in the electronic card, the PC, and the authenticating server for a long period of time. The password exists in the electronic card and the server for a short period of time. In the electronic card, the password is saved in RAM so when the electronic card powers down, the password is forever gone. In the server, the password exists for a short time (e.g., 5 minutes) that is just long enough for the user to log in successfully. Thereafter, the server discards the password immediately. In this configuration, the PC need not have a microphone since the user is not using the electronic card to directly transmit any data to the PC (or server). On a related note, the special client software does not need any special digital signal processing section to process any received signals since the electronic card will not be transmitting any signals to the PC.

5.3.5 CHALLENGE-RESPONSE

In another embodiment of the present invention, the merchant and user can employ challenge-response techniques to verify to each other's trustworthiness. Usually, one of the parties verifies that the other is indeed the party it claims to be for a given transaction. In some cases, however, both parties may want to verify each other for a given transaction.

In either case, digital certificates can be used. As known to those skilled in the art, a digital certificate is similar to an electronic "credit card" that establishes the certificate user's credentials when doing business or other transactions on the web. It is normally issued by a certification authority. The digital certificate contains the user's name, serial number, expiration dates, a copy of the certificate holder's public key, and the digital signature of the certificate-issuing authority so that the recipient of the digital certificate can verify that the certificate is indeed authentic and real. Some digital certificates conform to the X.509 standard.

IPR2025-01150
Apple EX1071 Page 712

FIG. 33 shows the sequence of steps of actions taken by the electronic card and the merchant in the case where the customer wants to verify the merchant. Initially, the merchant sends a digital certificate over the web to the customer. The digital certificate contains the date of expiration, name of merchant, signature of the certification authority (e.g., Verisign), and the merchant's public key. The customer's PC receives the digital certificate and in turn, transmits the digital certificate to the customer's electronic card. The electronic card contains standard logic and programming to perform a check to make sure the digital certificate is valid. In one embodiment, the electronic card checks to make sure that the digital certificate is signed by the certification authority and contains no errors. By verifying that the digital certificate is properly signed by the certification authority, the customer is making sure that no one is faking the information in the certificate.

At this point, the customer has the public key of the merchant. The customer can verify the merchant by sending a challenge and then testing the response to the challenge. The electronic card generates a random number. The customer transmits the random number to the PC. The PC then sends the random number to the merchant. The merchant signs the random number with the merchant's private key and sends the signed random number back to the customer's PC. The PC receives the signed random number and sends it to the electronic card. The electronic card checks the signed random number with the merchant's public key, which it obtained earlier. If the proper random number is recovered, then the merchant is presumed to indeed be the merchant it claims to be. The customer can now trust the merchant. Alternatively, instead of the customer sending a random number, the customer can send a digital certificate, which contains the ID and a public key. This certificate is sent by way of the certification authority.

Note that in this example, the party on the other side of the transaction knows the public key that matches the private key. The certification authority ensures that this public key belongs the merchant when the digital certificate has been delivered to the customer. To indicate a successful verification, the electronic card contains logic to sound an audible alert such as a ringing bell. If the verification is not successful, the electronic card can sound a different audible alert such as a buzzer.

In an alternative embodiment, the electronic card is not involved in this process. Rather, the PC performs all the steps that the electronic card is programmed to perform as shown in FIG. 33.

FIG. 34 shows the sequence of steps of actions taken by the electronic card and the merchant in the case where the merchant wants to verify the customer. For this case where the merchant needs to check the customer's identity to determine whether it can trust the merchant, a similar procedure is provided in the opposite direction. The customer's electronic card sends the card ID number (i.e., individual ID or serial number), the customer's public key, and a digital certificate. The PC receives this transmission and sends the card ID, the customer's public key, and the digital certificate to the merchant.

When the merchant receives the card ID, the customer's public key, and the digital certificate, it checks to make sure that it is a good signature from the certification authority. This provides the merchant with the assurance that no one is faking the card ID and public key.

The merchant then sends a random number to the PC, which retransmits it to the electronic card. The electronic card signs the random number with its private key and sends the signed random number back to the

IPR2025-01150
Apple EX1071 Page 713

PC. The PC then sends the signed random number back to the merchant. The merchant receives the signed random number and checks it with the customer's public key. If the check is proper, the merchant can be assured that it is dealing with the electronic card that it purports to be. The merchant can trust the electronic card.

FIG. 35 shows the sequence of steps of actions taken by the electronic card and the merchant in the case where they want to verify each other. In this embodiment, both the customer and the merchant check each other substantially concurrently. The electronic card sends a first set of data including the digital certificate, the card ID, the customer's public key, and a challenge (e.g., random number) to the PC. The PC retransmits the first set of data over the web to the merchant.

The merchant receives this first set of data and signs the challenge with the merchant's private key. The merchant then sends a second set of data which includes its own challenge, the response to the customer's challenge, and the digital certificate which contains the merchant's public key (among other data as described above). The customer's PC receives this second set of data and retransmits it to the electronic card.

The electronic card checks the digital certificate to make sure it was signed by the proper certification authority and the response to the customer's challenge (i.e., the random number originally sent by the customer and subsequently signed by the merchant with the merchant's private key). The customer checks the response with the public key that was just sent by the merchant as part of the digital certificate. If the response is proper, then the customer can trust the merchant. The electronic card then signs the merchant's challenge with the customer's private key and sends the response back to the merchant. In an alternative embodiment, the electronic card is not involved in this step of the process. In other words, the PC checks the merchant's digital certificate and the response to the customer's challenge with the merchant's public key.

The merchant then receives the customer's response to its challenge. The merchant checks the response with the customer's public key that was delivered initially. If the check is proper, the merchant can trust the customer.

In another embodiment, the electronic card can send back the response via conventional telephone systems. Thus, the merchant sends a challenge via the Internet to the customer's PC. The electronic card receives the challenge via the PC. The electronic card calculates the digital signature to sign the challenge and sends the response back via the conventional land-line telephone or cellular telephone system. In this embodiment, the acoustic signal is in the audible range. The merchant receives the response and checks it to make sure it is valid.

In another application, the use of the electronic card in chat rooms or message boards can prove invaluable in proving the authenticity of the user. Thus, the user would use the electronic card to log into the message board or chat room. The server would, of course, verify the identity of the user based on the electronic card and employing the techniques described above.

5.3.6 CRYPTO SERVICE PROVIDER (CSP)

As mentioned numerous times in this patent specification, the electronic card in accordance with one embodiment of the present invention should be compliant with the existing infrastructure. For Windows-based

IPR2025-01150
Apple EX1071 Page 714

systems, all web browsers and servers support client authentication by using Public Key Infrastructure (PKI), as known to those skilled in the art. Other exemplary merchant servers that support CSP include Apache, IIS, and Netscape Server. To use this authentication method, merchants need only turn on the "user authentication" flag within their server software, which requires selecting a button in a set-up menu.

Essentially, PKI allows users to send documents with digital certificates to prove that the user is indeed the user. The client authentication involves the use of cryptographic API (or crypto API), which provides an API between the various applications that are running in the user's client computer system (such as Microsoft Internet Explorer, Outlook Express, Word, etc.) and the cryptographic service provider (CSP) module.

As known to those ordinarily skilled in the art, CSP is a block of code distributed in Dynamic Link Library form that allows programs that are aware of it to connect and use its resources. Generally, CSP resources are essentially the hashing and encryption algorithms that it contains. Physically, each Crypto Service Provider (CSP) is a dynamic-link-library (DLL) with an associated cryptographic signature authorizing it for use by the Crypto API. One of the jobs of the CSP is to protect private key information from being exposed. Each CSP provides a different implementation of the Crypto API. Some provide stronger cryptographic algorithms than others. In addition to Microsoft, a number of third party developers have also released their own versions of Crypto Service Providers, each with its own unique set of ciphers, data formats and protocols. Indeed, two different providers may in fact include the same cipher algorithm but it would be incompatible due to different padding schemes, different key lengths, and different default modes.

Practically speaking, the CSP interacts with the user (and the user's applications in his client computer station) to allow the user to perform various security related tasks such as choose disk, give fingerprint (or voice print or biometric data), and the like. Because all web browsers and servers support it, the merchants who want a web presence are also required to support it. Thus, the CSP does not represent any change to the existing infrastructure.

In general, the CSP essentially enables the servers to ask the users to send digital certificates. The CSP in the client sends an unsigned digital certificate. The server which supports CSP receives the digital certificate and sends a random number back to the client to have it digitally signed. The client receives this random number and signs it with its private key and sends the signed random number back to the server. The server receives this signed random number and checks it with the client's public key for final authentication.

One drawback to this conventional approach is that the private key is held in the customer's client computer station. Thus, some hacker could theoretically break into that client computer station and steal private key. In accordance with another embodiment of the present invention, the private key is held in a third party CSP server. Referring now to FIG. 36, the electronic card sends its data (i.e., individual ID, group ID, etc.) to the PC. Similarly, the web merchant sends a random number (i.e., challenge) to the PC across the web.

The PC, through the CSP module, sends a digital certificate (which includes the customer's public key) and the electronic card data to a third party CSP server. This third party CSP server functions as a digital certificate signing facility and holder of private keys of all its members. This CSP server signs the digital certificate, signs the random number with the customer's private key, and then sends them back to the PC. The

IPR2025-01150
Apple EX1071 Page 715

CSP server also checks the data sent from the electronic card for "card presence" issues, which includes checking counter values and other parameters as described above in the On-Line Authentication section of the patent specification. The PC then delivers the signed digital certificate and random number to the web merchant who checks the signature with the customer's public key.

In an alternative embodiment, the digital certificate with the customer's public key could be sent directly to the merchant first. Thereafter, the electronic card sends the data and the merchant sends the challenge to the PC.

This scheme provides strong customer authentication without installing new server software. Cardholder privacy is also preserved because transaction information is not sent in real time to an Internet authentication server. With minor configuration changes to the existing software, merchants can confirm that a given electronic card was present in a particular transaction.

5.4 PLUG-IN APPLICATIONS

In accordance with another embodiment of the present invention, the special client software 114 (in FIG. 11) and works with one or more plug-ins in an integrated fashion. In one embodiment, the plug-ins are all subservient to the master special client software 114 (in FIG. 11). Thus, in addition to communicating with the electronic card, the special client software also manages the plug-ins. In another embodiment, the plug-ins are dominant over the special client software and can potentially perform more advanced and powerful functionality.

As known to those ordinarily skilled in the art, plug-ins or plug-in applications are supplementary programs to the user's web browser which assist the web browser to provide dynamic content that the web browser alone could not provide, such as playing sound or video. These so-called helper applications run as a separate application and require that a second window be opened. Plug-ins are easily installed and used with the web browser. A plug-in application is recognized automatically by the browser and its function is integrated into the main HTML file that is being presented. Exemplary popular plug-ins are Adobe's Acrobat, a document presentation and navigation program that lets user's view documents just as they look in the print medium; RealNetworks' RealVideo or RealAudio streaming media players, and Macromedia's Shockwave for Director, an interactive animation and sound player. Hundreds of plug-ins are available for download/install on the web or install via CD-ROM.

5.4.1 PLUG-IN SUBSERVIENT

In this embodiment, the special client software 114 (in FIG. 11) functions as the master or manager of the various plug-ins that are associated with the electronic card. These plug-ins are bidirectionally coupled to the special client software via the API layer. The special client software generally functions as described above – DSP for communicating with the electronic card, initialization, interaction with the web browser, interaction with the PC's sound system, etc. Additionally, the special client software basically provides the front end interface to the user and manages/launches the plug-ins when needed.

The plug-ins are generally sponsored by and/or written by various service providers, web merchants, or any company for that matter. By definition, these plug-ins are other software applications in the PC that are

IPR2025-01150
Apple EX1071 Page 716

called into service whenever the web browser, or in this case, the special client software needs them. Because these plug-ins are merely subservient support applications, their functions are controlled or otherwise limited by the special client software.

As the manager of the plug-ins, the main special client software keeps track of the group ID. As described above, the group ID is essentially the identifying number or code that represents the sponsoring entity, whether it is an individual, a company, or some other organization. For example, XYZ Corporation may sponsor a set of the electronic cards in accordance with the present invention to promote their website and product lines. They distributed the electronic cards to members and potential members so that they could use them to purchase products, request sales information, earn incentive points, obtain coupons and other discounts, and otherwise receive updated news about the company. Thus, XYZ Corporation is assigned a unique group ID that are provided in their electronic cards. Electronic cards sponsored by other companies will have their own respective companies' group ID. Theoretically, a user could have many different electronic cards just like some users have many different credit cards.

So, when the electronic card associated with a particular web merchant transmits some data to the PC, the special client software performs the DSP functionality to recover the data and checks the group ID. Based on the group ID, the special client software looks for the appropriate plug-in and enables its functionality. If the plug-in is outdated, the special client software will access a newer version of the plug-in over the web, download it, and install it. This may be done with or without the assistance of the user.

The special client software is equipped with additional functionality, because it is more than just a switch that routes the electronic card data to the proper plug-in based on the group ID. Assume that the special client software is sponsored by a particular bank, let's say the user's Visa issuing bank. This special client software associated can update and keep user passwords and IDs, check the user's credit card if it is delinquent, keep track of the number of times the user accesses the web, assist the user in navigating to the bank's home web page, assist the user in updating plug-ins, provide special offers to member users, scan other financial or other software in the PC and offer updates, retrieve email for the user, and numerous other functions related to the user's web experience with his bank. If a plug-in is necessary to view/hear content in a certain way, then the subservient plug-ins will be appropriately launched and enabled.

The kinds of functionality that can be supported by the plug-ins are limitless. Returning to the above example where the special client software is sponsored by the user's bank, the special client software may deliver the user to the bank's home page where, based on the content and various functionality programmed in that home page, the various plug-ins provide support, such as interactive buttons, sound effects, playing video, playing animation, and the like that are embedded on that web page. For example, a plug-in that provides the user with an interactive calculator to automatically calculate various aspects of his account may be provided. Furthermore, the user may be able to play a real-time video from the security camera at this bank with another plug-in. Another plug-in allows the user to send an email or message to various bank personnel to address questions concerning his account. If the user wanted to view one of his checks that did not clear, a document viewer plug-in is provided to assist the user in viewing that check.

IPR2025-01150
Apple EX1071 Page 717

Continuing with this example, another plug-in provides a message to the user via email whenever his account balance has reached certain thresholds (i.e., low threshold that incurs a charge) so that the user can take appropriate action. If the balance is too low, the user can quickly make a deposit or some other adjustments to his account so that he will not incur that penalty charge. Similarly, the user can have a plug-in that sends the user an email whenever anyone withdraws or deposits a certain threshold amount of money. These email or messaging plug-ins operate by automatically contacting the bank's web server, accessing the user's account, checking the account activity since that last time the plug-in logged in, and notifying the user of the activity (if any). The plug-in could send an email to the user's email address, or alternatively, display a message on the user's PC desktop in a manner similar to an active desktop.

In another embodiment, the plug-in associated with XYZ Corporation allows users to log into XYZ's website. In other words, the user takes out his XYZ Corporation electronic card and presses the TX switch. The electronic card transmits the data which includes the group ID and the microphone in the PC receives it. The data eventually makes its way to the sound card and then the special client software.

Based on the group ID, the special client software looks for the XYZ plug-in in the PC. If the plug-in is not available in the PC, the special client software accesses XYZ's website to download and install the latest plug-in. In the alternative, the special client software asks the user to download and install the XYZ plug-in. If the plug-in is detected, the special client software launches the plug-in, which then launches the web browser (if it has not been launched already). If the web browser has been launched, the plug-in navigates to XYZ's home web page. In another embodiment, if the web browser is already launched, the plug-in opens another window to navigate to XYZ's home web page.

At this point, the user is free to navigate anywhere on XYZ's website, or anywhere else for that matter. Note that the plug-in enabled the user to automatically log into the electronic card sponsor's (i.e., XYZ Corporation) website by the mere press of the switch on the electronic card. The master special client software steered the data to the plug-in associated with the group ID.

Another exemplary plug-in allows the user to log into a special members-only web page of the sponsoring web merchant/portal to obtain coupons, discounts, special offers, and other promotional items. Thus, if RST Corporation sponsored a particular electronic card and distributed the electronic cards to its members, the user of that electronic card could also log into a particular web page with the press of a button in the electronic card. On this web page are various promotional offers, discounts, and the like, which are available only to members of RST Corporation's website. The plug-in not only allowed member users to log into this special site but provided functionality that are optimized to view/hear certain information on this web page. Various interactive functionality on this web page are also made possible with the plug-in.

Another exemplary plug-in interacts with an electronic card that functions as a "voucher" or credit-limited card. The electronic card is then generic to multiple or many different web merchants. As users try to purchase merchandise with web merchant(s) that support this "voucher" electronic card, the plug-in checks the purchase to make sure that the user does not exceed his credit limit. Appropriate logic is provided in the plug-in to interact with the web browser to obtain the purchase price of an item so that the proper credit limit check can

IPR2025-01150
Apple EX1071 Page 718

be performed by the plug-in. If multiple web merchants support this electronic card, this generic plug-in can have different credit limits for each web merchant. If a credit limit is exceeded for a particular purchase, the user is notified with some dialog box and the purchase is otherwise cancelled. Thus, as the user navigates the web and attempts to make purchases, the plug-in checks each purchase to make sure the user is not exceeding the credit limit in his "voucher" electronic card.

If the electronic card is a multi-vendor card, the special client software determines which web page the user navigates to first in this subservient plug-in embodiment. If, however, the plug-in is dominant as described below, the plug-in itself determines which web page to navigate to first. This may create some conflict between or among competing dominant plug-ins.

5.4.2 PLUG-IN DOMINANT

In this embodiment, the plug-in is dominant over the special client software. In fact, the special client software merely provides the DSP functionality and checks the group ID to deliver the electronic card-transmitted data to the appropriate plug-in corresponding to the group ID. Beyond this, the special client software relies on the plug-ins for additional support.

In one embodiment, the dominant plug-in can be an application that is placed in the tray with an icon and is running concurrently. The dominant plug-in serves as the front end interface to the user. With this front end, the merchant associated with this plug-in can place advertisement, promotions, special offers, and other items that promote this web merchant's business. By being dominant over the special client software, the web merchant sponsoring the plug-in can write more code for the plug-in to provide more functionality. Indeed, the plug-in could be designed to operate with not only the electronic card described herein but other technologies as well, such as bar code readers.

Generally, the user takes out his XYZ Company's electronic card and presses the button. This data transmission results in the special client software detecting the group ID and enabling the XYZ plug-in to be launched. The XYZ plug-in now takes over, instead of the subservient plug-in embodiments where the plug-ins serve a more supporting supplementary role to the special client software.

Once again, the plug-in can provide various functionality such as messaging service associated with XYZ's website, delinquency information of the user's credit card, and provide ads and other sales information. Essentially, the exemplary functionality described above for the subservient plug-in are applicable for the dominant plug-in except that the front end is designed around the dominant plug-in. The special client software merely assists the dominant plug-in perform its tasks, i.e., by routing the electronic card transmitted data to the proper plug-in based on the group ID.

For both the plug-in dominant and plug-in subservient embodiments, the invention increases and enhances customer loyalty through electronic medium. By merely pressing the electronic card button, the web browser would open to a particular web page, whether it is the home web page of the company sponsoring the electronic card or the special client software. By going to this web page over and over again with the simple act of pressing the button on the electronic card, the user becomes more and more exposed to that web page's messages/ads/promotions. To increase the user's loyalty to this web page, the merchant sponsoring the

IPR2025-01150
Apple EX1071 Page 719

electronic card can offer incentive points to users for every visit to their web page using the electronic card. The plug-in can appropriately inform the web page whether the user accessed the web page through normal web browsing means or through the electronic card. Thus, even if the use had bookmarked various websites in the web browser, the loyalty program sponsored by this web merchant to promote the use of their electronic card will increase customer loyalty.

Additionally, the plug-in can navigate the user to the user's personalized web page on the web merchant's website or a particular community/interest group message board whenever the user uses the electronic card. In this way, targeted advertising, sales offers, discounts, and other coupons can be tailored to the user's specific interests/needs based on his past purchase decisions or the past purchase decisions of those group of people who are like the user (based on some statistical profiling scheme). Specific functionality needed by website can be provided by the plug-ins (e.g., playing sports game instant replay video/animation file for other community members to see).

5.5 POINTS/CASH PURCHASING MECHANISM

One embodiment of the present invention provides for a remote purchasing mechanism that involves the interaction of a consumer, a card issuer, and a web-based merchant. At the consumer end, an electronic card (or electronic card) and a client computer system are used. In the client computer system, a special client remote access software in accordance with one embodiment of the present invention is installed and running. In addition, a standard microphone, speaker(s), and a web browser are utilized. At the card issuer end, a card issuer server is provided to handle the consumer's account and authentication needs. At the merchant end, a merchant server or a server hosting the merchant's website is provided.

As a starting point for discussing one embodiment of the present invention, refer to FIG. 45. A consumer, who also has a membership with a card issuer 452 (to be explained further below), is equipped with a client computer system 451. The client computer system 451 has, among other things, a web browser which the consumer uses the surf the web and make purchases at various web-based stores. The web surfacing occurs on channel 457 with respect to this particular merchant server 453, which provides the product that the consumer wishes to purchase. When the consumer encounters a product that he wishes to purchase, he ultimately goes to the electronic checkout line of that particular web-based store. Normally, the web-based store, via merchant server 453, requires him to complete a form which asks for his name, shipping address, billing address, credit card number, expiration date of his credit card, and other personal information. Instead of manually filling out the form as usual, the consumer can use the secure purchasing mechanism in accordance with one embodiment of the present invention.

At the outset, the consumer is equipped with an electronic card 450 (or electronic card 450). The client computer system is a standard personal computer with a monitor operating on a Windows-based or Apple-based operating system. The electronic card 450 interacts with the client computer system 451 via medium 454. This interaction occurs to transfer the consumer's digital identification (ID) from the electronic card 450 to the client computer system to effectuate some transaction that is of interest to the consumer. The digital ID may be encrypted first in the electronic card and then transmitted to the client computer system 451.

IPR2025-01150
Apple EX1071 Page 720

After receiving the encrypted digital ID from the electronic card 450, the client computer system 451 opens another channel 455 to the card issuer server 452 which resides on the Internet and delivers the encrypted digital ID. The client computer system 451 may also send the URL of the merchant server in the same request or in a subsequent request. It accomplishes this using standard Internet accessing schemes by sending a request to the Internet with the uniform resource locator (URL) associated with the card issuer server 452. The card issuer server 452 is typically maintained and operated by a company that provides membership to Internet users and keeps member accounts of various selected currency. Thus, one card issuer may elect to provide frequent flyer miles to its members and allow its members to conduct sales transactions using the frequent flyer miles. Another card issuer may elect to provide incentive points to its members. Still another card issuer may elect to provide jelly beans as a form of currency to its members. Moreover, a card issuer may issue all these forms of currency. Whatever the currency, the card issuer company establishes and maintains an account database of its members. This account database includes name, shipping address, billing address, credit card number, expiration date, and digital ID. Of course, other information on the account holder may also be provided as necessary. The digital ID in the account is associated with the digital ID of the member/consumer that is programmed into the electronic card 450.

In addition to allowing the consumer to select the currency of his choice (that is also accepted by the card issuer), the card issuer also allows the consumer to allocate the amounts in that currency (and other currency) in any way that he desires for the purchase at hand. For example, assume that a book on a book merchant website costs $25. The consumer wants to buy that book but he wants to pay half in cash and the other half in accumulated incentive points at the current exchange rate. The card issuer server sends the credit card information to the merchant and subtracts (or credits) the appropriate number of incentive points from (or to) his account based on that day's exchange rate.

Having received the encrypted digital ID from the client computer system 451, the card issuer server 452 decrypts the digital ID, authenticates it, and references the account database to ensure that the digital ID corresponds to a valid member. In accordance with one embodiment, the card issuer server then opens up another channel 456 in the Internet and sends the credit card information of the member to the merchant server 453. The merchant server 453 processes the credit card information to finalize the sale and sends back a confirmation web page (which indicates that the sale is complete and typically provides a sales confirmation number) to the card issuer server 452. The card issuer server 452 then forwards the confirmation web page back to the client computer system 451. Alternatively, the merchant server 453 sends the confirmation page directly back to the consumer at the client computer system 451 via channel 457 without going through the card issuer server 452.

In another embodiment, the card issuer server 452 sends a confirmation back to client computer system 451 via channel 455 indicating that the digital ID is valid. The confirmation data may also include instructions and member profile data to the client computer system 451 to fill out the merchant's purchasing form. In another embodiment, the member profile data is stored in the electronic card itself so that no additional member profile data need to be sent back to the client computer system from the card issuer server. Having been

IPR2025-01150
Apple EX1071 Page 721

instructed to complete the form, the client computer system 451 completes the merchant's form in the web browser in automated fashion. The consumer then sends the completed form directly to the merchant server via channel 457. The sale is finalized in the conventional manner. In this case, the card issuer server 452 merely authenticates the consumer and delivers the confirmation back to the client computer system 451.

When the confirmation and instructions data are sent back to the client computer system, the special client remote access software in the client computer system opens up a second window (in addition to the window associated with the web browser). This second window provides the indication to the user of the confirmation. This second window also provides the user with the opportunity to select the desired currency for the sales transaction and specify the allocation (e.g., 40% cash and 60% incentive points for that particular purchase). When the user specifies the currency and the allocation, the information is sent back to the card issuer server, which processes the information by affecting the appropriate accounts. In one embodiment, the card issuer server then sends the credit card information to the merchant server. In another embodiment, the card issuer server sends the credit card information concurrently with the confirmation and instruction data, and the user and card issuer server negotiate for the currency and allocation later.

Note that with this secure purchasing mechanism, the card issuer can increase membership by appealing to the many Internet users who want to use alternate forms of currency to buy goods and services over the web. Additionally, because no special software is needed at the merchant server end, members can use their desired form of currency with any web merchant, unlike the past where consumers were limited to buying/redeeming points at the select few sponsoring merchants. With increased membership and usage, the purchasing mechanism of the present invention will improve and promote name branding of the card issuer's card or card issuer's service.

For the user, a purchase can be made with any web merchant with any desired form of currency (so long as the card issuer supports it). Additionally, because the data transfer from his electronic card to the PC to the merchant (via the card issuer) and back to the user is encrypted throughout the process, additional security is provided.

The special client remote access software performs multiple tasks that are important to the various embodiments of the present invention. During the initial stages of the user's on-line purchase, the special client remote access software processes the sound waves corresponding to the digital ID that have been emitted by the electronic card 10. After having been received by the microphone and processed by the sound card, the sound waves are processed further. The special client remote access software checks the encrypted digital ID sound waves to make sure that the data is complete and corresponds to the appropriate user's electronic card 450. After the check is completed, the special client remote access software opens another Internet channel to send a request to the card issuer server 452. The special client remote access software also sends the digital ID to the card issuer server 452.

During the next stage of the sales transaction, the card issuer server 452 sends back either: (1) a confirmation that the digital ID has been authenticated or no confirmation, or (2) a forwarded web page from the merchant server that indicates that the sale has been finalized with the proper confirmation number. In the

IPR2025-01150
Apple EX1071 Page 722

first case, the confirmation (or no confirmation) from the card issuer server includes instructions and data for the special client remote access software to complete the form that the merchant server requires for consummating the purchase. The special client remote access software then completes the form displayed in the web browser window without any intervention by the user. After automatically filling out the form, the special client remote access software is not involved any further in the transaction. The user interacts with the merchant server directly with his web browser to finalize the transaction.

In the second case, the card issuer sends the credit card and other relevant information to the merchant server. Thereafter, the merchant server finalizes the sales transaction with the information provided by the card issuer server and sends back the web page that contains the confirmation number of the order (and also some indication that the sale has been consummated such as "Thank you for your order. Your confirmation number is xyzabc123.").

In another embodiment, the electronic card is not needed. In other words, the user merely enters some digital ID with his keyboard. This digital ID is then encrypted and sent to the card issuer server, which processes this information as described above.

In summary, the various components of the system interact with each other to facilitate the purchasing process. The electronic card interacts with the special client remote access software via the client computer system's microphone to transfer a digital ID. The special client remote access software is capable of interacting with the speaker/microphone drivers in the client computer system for transferring the digital ID of the consumer, the web browser for transferring form data, and the card issuer server for authentication and other purchasing tasks. The card issuer server interacts with the special client remote access software for authentication and effectuating other purchasing tasks and the merchant server for delivering payment information. The merchant server interacts with the client web browser for standard web access and the card issuer server for transferring payment information.

The benefits to the card issuer are primarily two-fold. First, because non-conventional currency are permitted to be used by its members, membership in the card issuer company will grow and be very active in sales transactions. Second, the widespread use of the electronic card as a member of the card issuer company will promote name branding of the card itself.

The benefits to the consumer are also primarily two-fold. First, because data is encrypted throughout the entire link of the sales chain (from electronic card to PC to merchant and back), the purchasing mechanism is more secure than today's conventional method. Second, the user can use any desired form of currency (and in any amounts depending on how he allocates the cost) to make a purchase on the web with any web merchant, not just the few sponsoring merchants as he was accustomed to in the past.

5.6 BAR CODE READER

In another embodiment of the present invention, a portable bar code reader is used to scan bar codes to provide an effective link to the bar code's corresponding website for faster service. A couple of examples will be provided to clarify this embodiment.

Assume that a user purchased a merchandise from the store. This merchandise offers a $5 rebate if the

IPR2025-01150
Apple EX1071 Page 723

proof of purchase is returned to the manufacturer. In this embodiment, the user utilizes a portable bar code reader to scan the bar code of this merchandise instead to store the bar code in the reader.

The bar code reader can then be taken to the user's PC. After launching the web browser, the user takes out the bar code reader and presses the TX switch. The bar code reader then emits the sound which contains the data corresponding to the bar code. The structure and format of this sound signal is analogous to the sound signal described above in this patent specification. Part of the data in the bar code is the URL of manufacturer's website. The URL may correspond to the customer support web page, the technical support web page, or any other web page associated with the manufacturer of the merchandise.

When the special client software detects and properly decodes this signal, it provides the URL information along with any other data in the bar code (e.g., product serial number, model number) to the web browser which promptly navigates the user to the web page specified by the URL. Once at this web page, the user can then apply for the rebate by providing the name and shipping address. The manufacturer can then send a check in the amount of $5 for the rebate. Alternatively, the user can set up an account on this website so that his account can be credited.

As another example, the URL in the bar code can direct the user to a particular web site to get more information about that product, the manufacturer's other product lines, and other related sales information. The user may also earn coupons and other discounts for simply navigating to these web pages. The bar code represents a convenient way for the user to access the relevant web sites.

5.7 CARD-TO-CARD INFORMATION EXCHANGE

In another embodiment of the present invention, the electronic card is two-way card where the receiver is operational and waiting for signals when the power is on. In this embodiment, the electronic card contains user profile information. This user profile information includes name, company, title, email address, telephone number, and special interests (e.g., computer hardware, video graphics, software game developer). The electronic cards essentially communicate with each other to: (1) exchange information for storage, and (2) match two users (i.e., customer and vendor, or vendor and vendor) with similar interests.

In the first scenario, the action taken by the electronic cards is analogous to the exchange of business cards. To avoid collisions, though, the transmissions should occur at different time periods. As one user nears another user, the first user can press the TX switch to send the information to the second user. Then, the second user would press the TX switch to send his information to the first user. An audible alert (i.e., beep) would indicate when the transmission is complete (or the data storage is complete). This embodiment implies a manual operation.

Another embodiment is pseudo-automatic. When the first user nears a second user, the two users would each press the TX switch to transmit their respective contact information to the other. Instead of transmitting immediately, the two electronic cards would each determine some random time period. At the expiration of that time period, the electronic card would then transmit the information. Although both users may have pressed the TX switch substantially at the same time, the generation and use of the random time period ensures that, more often than not, the two electronic cards would each transmit information at different

IPR2025-01150
Apple EX1071 Page 724

time periods. Also, circuitry in the electronic card can be provided such that when one of the electronic card detects a valid electronic card signal from the other electronic card, and this electronic card's randomly generated transmission time period has not expired yet, this electronic card will not transmit the signal as long as it is receiving a valid electronic card signal. Even if the randomly generated transmission time period has expired, this electronic card will not transmit until all of the other electronic card's signal has been received and processed. Then, this electronic card will transmit its own information.

In both cases, an acknowledgment signal may also be implemented. In the first case, the electronic card will retransmit until the other electronic card sent an acknowledgment. Then, the second electronic card would transmit (and retransmit) until the acknowledgment signal was received by the first electronic card. In the second case, each electronic card generates a random time period. At the expiration of that time period, the electronic card will transmit the data to the other electronic card. Thus, using the randomly generated time periods for the transmissions, each card will continue to retransmit after each the expiration of each newly generated random time period until an acknowledgment from the other card is received and processed.

In the second scenario, the electronic card can be used as a means to match entities together – whether buyer-seller, vendor-developer, or employer-potential employee at a job fair. Thus, in one example, a potential buyer goes to a convention. At each booth, the vendor has a reader that can receive and process signals that are transmitted by the electronic card. When the user of the electronic card nears the booth, he presses the TX switch on the electronic card and the reader at the booth receives and processes the signal. If the company at this booth sells a product or is otherwise in a field that is related to the electronic card user's field or special interest, then the reader would indicate a match. The reader would send a match acknowledgment signal or a no-match acknowledgment signal to the electronic card. The electronic card would provide an audible alert that corresponds to the match or no-match acknowledgment signal, e.g., beep for match and buzz for no-match.

In all the scenarios above, the user can take his electronic card to his PC and later download the data therein. Either pressing another button or the same button in download mode (e.g., press twice in rapid succession) will cause the electronic card to transmit the data to the PC. The special client software could then process the data and store them in some usable format. Thereafter, the user could transfer the stored data in whatever application (e.g., Palm Pilot organizer) he desires.

5.8 WEBPAGE-DEPENDENT ACTIVATION

With thousands and thousands of webpages on the web, not every website will support the communications protocol of the present invention; that is, not all webpages are designed to listen for the electronic card transmission to perform some function or play an audio file that contains some data in a format that the electronic card of the present invention can understand. However, some websites support the communications protocol.

The user, however, is unaware of which website supports the communications protocol of the present invention as he navigates from one website to another. Two solutions to this problem are offered – (1) webpage provides indication, and (2) client station provides indication.

In the first solution, the website itself will indicate that it supports the communications protocol and

IPR2025-01150
Apple EX1071 Page 725

thus, the user will be able to take advantage of the electronic card's many benefits. A simple brand logo of either the card's sponsor or the card's manufacturer can be this indication. In other cases, a more lengthy explanation will be provided on the website – something of the form "This website supports the XYZ acoustic card. Please do not press the button on your XYZ acoustic card unless prompted to do so. We will provide some feedback to indicate that your transaction with the XYZ acoustic card has been successful." This instruction may be coupled with eye-pleasing graphics and other animation to make it clear to the user that the timing of the button press is important. Thus, as the user surfs the web, he will be alerted to those websites that support the communications protocol of the present invention.

In the second client station-based solution, the client station via the special client software will provide the indication to the user. In this embodiment, the special client software is installed in the client computer station. It is resident locally and is part of the System Tray set of applications. Normally, it is "asleep" in that it provides no apparent functionality to the user. However, it is operational and communicates with the web browser or whatever application is used to access the web. The special client software is installed in the client and "wakes up" whenever it detects a webpage that supports the communications protocol of the electronic card. This is accomplished by providing a code in the accessed webpage.

As discussed above, some websites support the communications protocol and others do not. This websites that support the communications protocol can embed a special code that is also known to the manufacturer of the electronic card. When the user accesses a website that has this embedded code, the special client software "wakes up" and alerts the user that this website supports the communications protocol of his electronic card. This alert can be a flashing icon on the Icon Tool Bar of the user's Windows desktop, a flashing or pulsating icon of the electronic card on the upper right corner of the screen, or some other visual or auditory cue. This tells the user that he can use his electronic card to conduct whatever transaction he has in mind on that site.

This special code can be provided as part of the header text. The code can also be used in conjunction with some logo or graphic on the webpage that indicates the exact type of electronic card supported. For example, the user has two electronic cards – XYZ Corporation's shopping card and a EZTrade Company's online trading card. At a particular website, the website indicates via some graphic that only the XYZ electronic card is supported.

In addition, different codes can be used in different webpages (or even in the same webpage) depending on the particular function that it supports. Perhaps a one particular webpage will fill out a form for the user when the user presses the button on the electronic card, while another webpage will authenticate the user to access his account. These context- and function-sensitive codes can be detected by the special client software so that the user's press of that single button on his electronic card will accomplish different things.

In a preferred embodiment, a single card can be used to interact with a large number of different web services. This makes a single card more useful to a cardholder. It also gives rise to an opportunity for card issuers to share in the revenues obtained by the service provider that makes the card-present authentication available. For example, assume that an online stock trading service finds this card-present authentication under

IPR2025-01150
Apple EX1071 Page 726

the present invention attractive enough that they will pay two cents to the authentication service provider every time a card is used to log in. As a way to encourage card use or adoption, the service provider could pass one of those two cents through to the issuer of the card used to effect that authentication. Ultimately, such revenue sharing could contribute to a "network effect" growing the demand for electronic cards, since all issuers and participating web services would be financially encouraged to keep their cards and services open to authenticating universally, and not just to their own services. Users under such a regime would benefit from the ability to use any card under the present invention to authenticate to any card-ready online (or telephone-based) service.

5.9 ELECTRONIC LOYALTY

Despite the advantage of money as a universally accepted means of payment, some consumers may not be willing to buy certain goods with money. Just as gamblers part with their money more freely when converted into "chips," consumers may be more willing to part with an alternative form of currency. "Points" are an example of a popular alternative currency used by many incentive award programs, as described below.

What are incentive award programs and how did they come about? Merchants have long realized that due to marketing costs, the first sale made to a customer is far more expensive (and thus less profitable) than ensuing sales. In order to maximize profits, most merchants work to build long-time relationships with customers, yielding ongoing sales with higher and higher profits. While many merchants would be willing to offer lower prices to entice particular customers to stick with them and not switch to competitors, this is often impractical and always expensive. Charging different customers different prices is difficult at many levels and even if it could be accomplished, giving the incremental profit back to the consumer defeats the merchant's goal in the first place. For this reason, incentive award programs were developed.

What is an incentive award program? Incentive award programs come in two varieties – loyalty incentives and attention marketing. Loyalty incentive programs award "purchase points" to those consumers who take certain purchasing actions. A classic loyalty incentive program provides a benefit to consumers who stick with or are loyal to a merchant and not switch to competitors, while "punishing" those who switch from brand to brand. Typically, an incentive is an incremental benefit that is worthless until enough points have been earned to redeem for a discount or a gift. Attention marketing programs reward consumers with "attention points" for paying attention to a marketing message.

The loyalty incentive program will be discussed first. A highly successful form of loyalty incentive award program with which many people are familiar is the airline mileage program, although non-mileage-based programs also are widespread. Mileage programs currently are conducted by almost every commercial airline. Travelers can earn mileage or mileage points by purchasing an airline ticket and actually taking the trip. The exact number of miles earned by the traveler is usually calculated by some formula based on the distance of the trip. After accumulating a certain number of miles or mileage points, the traveler can redeem his miles for a free or discounted airline ticket or some other award (e.g., coffee maker, free upgrades) that he can select from a catalog. The price-shopping, airline-switching fickle traveler would arguably not benefit (or not benefit sooner) than the traveler who is loyal to one airline.

IPR2025-01150
Apple EX1071 Page 727

Similar incentive award programs also have begun to flourish in an online environment over the Internet. Buyers can earn points online, for example, by purchasing goods from an online merchant, clicking on advertisements, filling out registrations and surveys, and performing various other activities of interest to merchants, advertisers and other companies. Users accumulate "points" into an "account" from which they can redeem their points for certain goods or services.

Even those consumers who are not regular online users or even familiar with the Internet may well be familiar with a variation of the point system. Many merchants award discounted or free merchandise to loyal and frequent customers. For example, by ordering a regular meal at a restaurant on ten different occasions (recorded on a stamped card), the customer may get 50% off the eleventh meal (or even get the eleventh meal free). Similarly, another merchant might give a loyal customer a free drink with his meal after every seventh or tenth visit. Another merchant might give $10 off the next purchase for a first-time customer. These variations on the loyalty incentive point system are just that – variations. Even though an actual physical card may be stamped after each visit to a restaurant or a gift certificate is handed out, these stamps and gift certificates are analogous to points, albeit in non-electronic form.

The tremendous power of loyalty incentives is this: the more points that a consumer has earned, the more the consumer wants points. Each incremental point is more and more valuable to the consumer because high point levels are associated with more exclusive (and valuable) benefits. So, the merchant benefits from the increased returns. The best customers are the least likely to switch to a competitor.

Although most point systems are still merchant-specific, more and more merchants are forming relationships with one another so that points are more universally accepted across different merchants, and thus more desirable to consumers. For example, purchasing goods from one merchant can result in earning points with another merchant. A consumer's use of his credit card might earn the consumer miles with Jones Airlines. Similarly, points earned through one merchant may be redeemable with another designated merchant. Thus, the consumer is no longer restricted to one merchant's catalog at redemption time.

But this is deceptive. Typically, points earned at an online store are usually not redeemable at a conventional bricks-and-mortar store, and voce-versa. Thus, the thousands of points earned at XYZ.com is worthless at the local department store. If a universal points database existed that allowed consumers to accumulate points and store points, much like a bank, as well as redeem them almost anywhere, consumers might be more motivated to participate in incentive award programs with greater frequency.

Thus, incentive award systems have demonstrated the viability of altering consumers' behavior if consumers perceive the points to be of value. Yet, the fixed-merchant nature and the inability to earn/redeem points between online and offline stores in existing incentive award systems often have limited the perceived value of points.

In accordance with one embodiment of the present invention, the Uniform Points System uses payment units, which can be in the form of actual points (and credit points) or cash (and credit). Uniform Points can be either purchase points or attention points. These points are part of a rewards system that rewards users who use the electronic card of the present invention. Although Uniform Points can be viewed as a separate form of

IPR2025-01150
Apple EX1071 Page 728

currency to purchase products, Uniform Points are better viewed as a means of building a mutually beneficial relationship between merchants and buyers. Thus, as users earn more and more Uniform Points, the users are rewarded with gifts and redeemable merchandise, while merchants are rewarded with more sales-generating traffic on their websites.

Although any form of payment unit can be used in the Uniform Points System of the present invention (including a mixture of cash and points), the patent specification will describe the embodiments with respect to points. However, one skilled in the art will recognize that the implementation details will be similar if money or alternative forms of currency were used instead of points.

How do users earn points? Participating merchants award Uniform Points to consumers, and allow for their redemption, in numerous ways. More importantly, these participating merchants have made these Uniform Points so universal that Uniform Points earned through one merchant can be redeemed with another merchant, and vice versa. Additionally, Uniform Points can also be converted into miles for many frequent flyer programs, and vice versa.

These Uniform Points can be earned in any number of ways, such as by registration, by purchase of product/service, and by viewing advertisements. The consumer is not necessarily required to visit any one website to earn points; rather, Uniform Points can be earned through any website or conventional bricks-and-mortar store that awards Uniform Points (i.e., those merchants with some relationship to Yahoo). Uniform Points can also be earned in other ways. Consumers can earn points from select merchants by:

(1) switching long distance carriers,
(2) updating user registration information periodically (to track changing interests)
(3) trying out a new service with an already existing membership,
(4) signing up for a new credit card,
(5) entering a merchant-sponsored sweepstakes,
(6) signing up for a trial membership to any merchant-sponsored club,
(7) playing online games such as poker, blackjack, and slots,
(8) answering questions for an online poll,
(9) trying a new product with no obligations,
(10) requesting a free quote on a vehicle,
(11) visiting a website (although some registration may be involved),
(12) writing and submitting product reviews (e.g., books, music, video),
(13) downloading software from a website,
(14) signing up a friend to some club membership,
(15) serving an online community by answering user questions,
(16) Points could be awarded as a multiplier (i.e., "Click here to double your points"),
(17) Points could be awarded offline as well (e.g., for using a shopping card at a supermarket), and
(18) purchasing a threshold amount of goods from multiple merchants.

IPR2025-01150
Apple EX1071 Page 729

This list is merely representative of the ways in which points can be earned. This list is not meant to be a comprehensive list. As mentioned above, these Uniform Points are universally accepted among the participating merchants. Thus, points earned through one merchant can be redeemed through another merchant. So, when a consumer earns 50 points through a music merchant by purchasing some compact discs, that consumer can redeem those earned 50 points with a pet supply merchant to purchase dog food. Of course, the music merchant may have one set of rules on how to earn these points and the pet supply merchant may have a different set of rules on how and when to redeem points and what thresholds are required for redemption. So long as these rules are observed, the consumer can use points like cash and apply them across different merchants.

Referring now to FIG. 47, the Uniform Points System will now be described. The central database 475 keeps track of points, gift certificates, and cardholder information. Points are as described above. Gift certificates are items that have a specific cash value that can be used at the gift certificate-sponsoring merchant's store, whether online or offline. Thus, a $20 gift certificate from XYZ Corporation is typically redeemable only at the XYZ store. The central database 475 can be considered a points/use database which keeps track of any online and offline card use, whether the card is used as a loyalty card (for earning and redeeming incentive points), a gift certificate, or an ATM card. Each registered user is associated with his own account for each of these uses. Usually, the central database 475 is periodically synchronized with each participating merchant's own account database, such as that associated with merchant account server 472 and 474. In other embodiments, the central account database 475 keeps the only copy of the account information so that the merchant's server 472 or 474 would have to access the central database to access any particular user's account information.

If the electronic card is used as a wireless acoustic card as described in this patent specification, the press of the button on the electronic card 470A triggers the transmission of a data stream. This data stream can be as simple as the card-specific digital ID. The user's PC 471 detects this data transmission and relays this card-specific digital ID (among other data described above) to the specific merchant's account and authentication server 472. Of course, the user may have automatically launched into (via the activation of the electronic card) or manually navigated to this merchant's website. The merchant's website would support the communications protocol of the present invention.

After performing whatever authentication tasks are needed, the server 472 accesses the account therein of the authenticated user. Based on the action taken by the user, the user's account is adjusted. For example, the user may have 50,000 points in his account and by the mere press of the electronic card button, he spent 20,000 points on a brand new color TV set. With this action, the central database subtracts the 20,000 points from this user's account. In another example, the user has an electronic card that represents a $20 gift certificate. The user accesses the merchant's website and uses $17 of this $20-valued gift certificate to purchase a CD. The central database adjusts this user's gift certificate account to reflect this purchase so that only $3 is now remaining. As a gift certificate, the electronic card of the present invention replaces the current paper gift certificates that merchants hand out.

IPR2025-01150
Apple EX1071 Page 730

Alternatively, the user could actually walk into a conventional bricks-and-mortar store and use the electronic card 470B. Because the current electronic card 470B has the traditional magnetic stripe on them, this electronic card could be used with any conventional magnetic stripe card reader 473. The authentication is performed via the merchant's account server 474 and the user's account is accessed via the central account database 475. This central account database 475 is the same database used for the non-magnetic stripe embodiment described above.

Thus, the versatile electronic card 470A/470B with the acoustic electronics and the conventional magnetic stripe makes it more attractive and convenient for the user to shop online and offline. On top of that, the central account database 475 increases the user's offline purchasing power through online purchasing actions, and vice versa. A user can shop online and earn incentive points. Because of the universally used central account database 475, these incentive points that were earned online can now be redeemed offline at any participating bricks-and-mortar store. The central account database 475 keeps track of any earned/redeemed points.

5.10 ADDITIONAL SYNERGIES WITH VOICE

The present invention's preferred communication method (data modulated on sound) gives rise to a number of convenient synergies when implemented with known voice technologies such as voice recognition and voice verification, Voice over Internet Protocol (VoIP). Generally, one of the goals of the present invention is to provide convenient, portable, physical authentication means for the Internet, in a known form factor used in the offline world, that does not require any infrastructure change unlike the traditional smart cards. The recent proliferation of voice applications for the Internet, such as voice recognition, and voice navigation for Internet browsers assures that sound infrastructure (microphones and speakers) are rapidly penetrating into all Internet platforms. The microphones being installed for those other purposes, generally speaking, are well suited for the card communications techniques described herein.

Generally, the strength of a security system is measured, in part, by the number and diversity of the security "factors" being required. Three such genres of security factors are commonly known as "something you know" (e.g. a password); "something you have" (e.g. a card, such as the reader-free electronic card described herein); and "something you are" (e.g. biometric measures such as voice.) For example, a password by itself may not provide complete security, because a holder may inadvertently disclose it, or the password can be guessed. A reader-free electronic card in accordance with the present invention can be lost or stolen. But when, as in accordance with various aspects of the present invention, a password is used as one factor, and the authenticated presence of a reader-free electronic card is used as another, security is enhanced.

For some applications, however, including high security transactions like extremely large financial transactions, there is no security factor equal in value to assuring that the correct person is present. Voice authentication as a biometric security factor is known in the art of computer security. Typically, these schemes will require the authenticating user to read arbitrary text, and then compare these vocal patterns to the authentic user's own speech patterns to verify conformity. One limitation of biometric security schemes, and voice authentication is no exception, is the requirement of special equipment to receive the biometric data (e.g.

IPR2025-01150
Apple EX1071 Page 731

fingerprint or iris readers, or microphones and sound systems for voice authentication). There are abundant known techniques for deploying voice authentication on a single computer, or over a network by sending voice sounds to and receiving authentication codes from, a network server.

But the fact that any issuer of the acoustic reader-free electronic cards of the present invention can be sure that each and every base station includes a microphone solves this barrier to introducing voice authentication as a security factor. Thus, one embodiment of the present invention enables the proprietor of a security system to deploy a regime including the "something you have" factor in the form of a card or other physical token practicing the acoustic data transmission techniques discussed above, plus any combination of a password or other "something you know" factor, plus biometric verification by voice authentication.

Lack of perceived security and a lack of user trust remain the principal deterrents to people adopting habits of shopping and doing commerce online. Because the base station described above includes a microphone and sound system, increased personal relationship and trust can be established under the present invention by requiring presence of a reader-free electronic card, and adding the personal attention of speaking with live people using VoIP techniques.

Major banks are moving to increase adoption of their online account services. Online banking represents a significant cost savings over in person banking at branches, and even telephone banking. But customers may hesitate to conduct banking activities online because over the Internet, no particular customer service representative can interact with shoppers directly. But known VoIP systems enable voice-based conversations with the other persons visiting a particular website, or with customer service representatives manning that site.

Under the present invention, when combined with online banking or other secure online services, an acoustic electronic card can be activated to enable various functionality within the sound infrastructure. The customer learns to trust the Internet and his transactions therein because of the guaranteed "card presence" transactions that are accepted by online merchants/financial institutions. Furthermore, conversations can be recorded for resolving non-repudiation issues for online banking and other conversations with merchants. The user can also choose his desired customer service representative. In the non-financial Internet world, one embodiment of the present invention allows authentication and limited audience chat plus voice chat in a message board or chat room.

6.0 NON-ACOUSTIC EMBODIMENTS

Instead of acoustics, another embodiment of the present invention uses radio frequency (RF) and magnetic field transmission/reception techniques to couple the electronic card and the client computer station.

For RF, data from the PC to the electronic card is transmitted using VHF or UHF frequencies. These high frequencies can be achieved by software manipulation at the PC. The CPU of the PC uses its data-address bus as the transmission antennas and modulating signals on the bus. The electronic card receives and decodes these signals with standard RF decoding circuitry. Alternatively, the PC can employ On-Off RF modulation by halting and restarting the CPU. The electronic card receives and decodes these signals with standard RF decoding circuitry.

IPR2025-01150
Apple EX1071 Page 732

For magnetic field, the PC speakers transmit the data from the PC to the electronic card. However, instead of picking off the audio signal, the electronic card picks up the magnetic field created by the speakers and their wires which are present when the audio is played. The pick-up element in the electronic card is a loop antenna.

6.1 RADIO FREQUENCY (RF)

Instead of acoustic signals, the client computer station (e.g., personal computer) can generate RF signals to the electronic card. With appropriate RF decoding circuitry, the electronic card can receive and decode the RF signals to process the data therein. Again, no additional hardware would be necessary in the PC to generate the RF signals.

The unique RF transmission technique in the PC involves using the address-data bus as the transmission antenna and the CPU as the oscillator. The PC currently generates electromagnetic signals because the electronic circuitry in the PC applies voltage to the various buses causing current to run along the wires. The electromagnetic signal is RF in nature because the PC's microprocessor speed is typically in the RF range (tens to hundreds of MHz). The microprocessor's speed is typically 100-450 MHz, although more and more new PCs are being sold with microprocessors in the gigahertz range.

As known to those ordinarily skilled in the art, the main frequency component of an RF signal is at the base carrier frequency. For a microprocessor at 100 MHz, a lot of the signal's power is present at 100 MHz. Signal power is also present at other frequencies which are whole number multiples of the main base frequency. Thus, some signal power is present at 50 MHz (multiple of 2), 33.33 MHz (multiple of 3), 25 MHz (multiple of 4), 20 MHz (multiple of 5), and so on. However, the higher the multiple, the less likely that the RF signal will have a frequency component at that corresponding frequency. Thus, at a multiple of 100, the chance that some frequency component would exist at 1 MHz is low. In some embodiments, appropriate division is performed to obtain the FSK frequencies from the higher RF frequencies.

The first step is to select the frequency of the RF transmission. In the FSK scheme utilized in this invention, the two frequencies are approximately 1 kHz apart. So, for example, one frequency can be 10.7 MHz while the other frequency is 10.699 MHz. The period of these frequencies would also have to be determined. Thus, for the frequency 10.7 MHz, the period is 93.4579 ns.

The next step is to determine how much time an instruction takes. Based on this instruction time and the frequencies selected above, the number of instructions needed for the whole period for each frequency can be determined. If frequency 10.7 MHz is selected for one of the RF frequencies, the number of instructions to fill up the above-calculated 93.4579 ns period would also be needed.

The PC's CPU itself will modulate the address-data bus for the desired frequency. In the above example, since 10.7 MHz was selected as one of the frequencies for transmission, the CPU will apply a logic "1" to the bus for half the period and apply a logic "0" for the other half of the period. The length of these logic "1" and "0" values that are applied to the bus can be controlled by the number of instructions that are delivered to the microprocessor since the time duration of each instruction is known. Accordingly, an RF frequency component will exist at 10.7 MHz in the above example. For longer periods (for lower frequencies), more

IPR2025-01150
Apple EX1071 Page 733

instructions are delivered to the microprocessor. For shorter periods (for higher frequencies), less instructions are delivered to the microprocessor.

At the electronic card, appropriate RF decoding circuitry can be employed to receive and decode the RF signals. Referring to FIG. 37, a high level view of the RF decoding circuitry in the electronic card is provided. In this design, off-the-shelf RF IC's are used. The transducer 370 receives RF signals and converts them to workable voltage levels. The pre-amplifier and bandpass filter 371 amplify and clean up the signals for further processing. In particular, the pre-amplifier portion of the unit 371 is a high input impedance amplifier. The bandpass filter portion of the unit 371 filters the signal in order to attenuate speech (or noise) signals. The RF signal is presented to the FM intermediate frequency (IF) unit 372. A quadrature network unit 374 is provided for frequency decoding using quadrature demodulation. Finally, the microprocessor unit 373 in the electronic card accepts the digital demodulated FSK signal, or in the alternative, an analog voltage that is correlated to the input frequency.

FIG. 38 shows an alternative embodiment. The transducer 380 receives RF signals and converts them to workable voltage levels. The RF signal is presented to the FM intermediate frequency (IF) unit 381 for filtering. The bandpass filter 382 cleans up the signals for further processing. The filtered RF signal is presented to the FM intermediate frequency (IF) unit 383 for further filtering. A quadrature network unit 385 is provided for frequency decoding using quadrature demodulation. Finally, the microprocessor unit 384 in the electronic card accepts the digital demodulated FSK signal, or in the alternative, an analog voltage that is correlated to the input frequency.

In the electronic card to PC transmission, the microphone in the PC can be used as the receiving antenna. However, the frequencies selected for the RF signal should be in the frequency range supported by the sound card in the PC. If the RF signal is in the 10 mV range, the sound card in the PC can detect it and process it as audio signals even though the transmission was via RF.

This embodiment provides several advantages. By using RF signals, the DSP software is much simpler in the electronic card. RF signals are much stronger and easier to process than acoustic signals. Lots of standard RF components are available in the market at lower cost. The use of RF avoids most acoustic-related issues, such as echo cancellation, range, and interference. The use of RF signals also result in higher bit rates. Also, in the PC-to-electronic card transmission direction, the sound card drivers in the PC need not be checked. In fact, a sound system in the PC is not needed at all for this PC-to-electronic card transmission direction.

6.2 MAGNETIC FIELD

In another embodiment of the present invention, the interactive system uses magnetic fields. When audio is played by the speakers, the currents created by driving the speakers are not negligible and thus induce a significant magnetic field. This magnetic field is generated by the speakers and the wires. However, these magnetic fields drop off significantly by a power of 3 so distance from the source of the magnetic field is important.

To pick up the magnetic field, the electronic card must be reasonably close to the source of the magnetic field, i.e., speakers and wires. Referring now to FIG. 39, the electronic card employs a loop antenna

IPR2025-01150
Apple EX1071 Page 734

390 instead of an acoustic transducer to pick up the magnetic field. Because the received the magnetic field induces a current in the loop antenna, a current-to-voltage converter 391 is provided. The remainder of the components are similar to that for decoding acoustic signals. In particular, the gain and bandpass filter 392 filters the signal for further processing. An AGC block 394 is provided for SNR improvement. The final processed signal is provided to the microprocessor unit 393 for data processing.

With respect to power, a conventional small-sized battery such as Varta LPF-25 is used. In some other embodiments, electronic card power is obtained from the PC via the Hall effect. The electronic card merely has an antenna with which to pick up signals for processing.

The foregoing description of a preferred embodiment of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Obviously, many modifications and variations will be apparent to practitioners skilled in this art. One skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention.

What is claimed is:

IPR2025-01150
Apple EX1071 Page 735

CLAIMS

1. A one-way portable device, comprising:

a device body that has a thickness less than 0.8 mm and a switch;

memory logic for storing device information; and

transmission electronics coupled to the switch that emit a wireless signal based on the device information in accordance with a first data format when the switch is activated.

2. The device of claim 1, wherein the wireless signal is an acoustic signal.

3. The device of claim 2, wherein the acoustic signal is an ultrasound acoustic signal.

4. The device of claim 1, wherein the wireless signal is radio frequency (RF) signal.

5. The device of claim 1, wherein the wireless signal is a magnetic signal.

6. The device of claim 2, wherein the first data format further comprises:

a first frequency shift keying (FSK) portion to identify a first frequency in a FSK signaling scheme;

a second frequency shift keying (FSK) portion to identify a second frequency in the FSK signaling scheme;

a synchronization portion for facilitating the proper reception of the wireless signal;

a known portion that both the portable device and a targeted receiver of the wireless signal knows;

a data portion comprising various combinations of the first frequency and the second frequency to represent the device information; and

an error checking code portion to allow some targeted receiver to check for errors in the received data.

7. The device of claim 6, wherein the first data format further comprises;

start and stop bits inserted in selected locations between the first FSK portion and the error checking code portion.

8. A two-way portable device, comprising:

a device body that has a thickness less than 0.8 mm and a switch;

memory logic for storing device information;

reception electronics for receiving wireless signals; and

transmission electronics coupled to the switch that emit a wireless signal based on the device information in accordance with a first data format when the switch is activated.

9. The device of claim 8, wherein the wireless signal is an acoustic signal.

IPR2025-01150
Apple EX1071 Page 736

10. The device of claim 9, wherein the acoustic signal is an ultrasound acoustic signal.

11. The device of claim 8, wherein the wireless signal is radio frequency (RF) signal.

12. The device of claim 8, wherein the wireless signal is a magnetic signal.

13. The device of claim 8, wherein the first data format further comprises:

a first frequency shift keying (FSK) portion to identify a first frequency in a FSK signalling scheme;

a second frequency shift keying (FSK) portion to identify a second frequency in the FSK signalling scheme;

a synchronization portion for facilitating the proper reception of the wireless signal by some target receiver;

a known portion that both the portable device and some targeted receiver of the wireless signal know;

a data portion comprising various combinations of the first frequency and the second frequency to represent the device information; and

an error checking code portion to allow some targeted receiver to check for errors in the received data.

14. The device of claim 13, wherein the first data format further comprises;

start and stop bits inserted in selected locations between the first FSK portion and the error checking code portion.

15. A method of transmitting a data stream from a portable device, said data stream including device information in the portable device, comprising steps:

preparing a synchronization portion for facilitating the proper reception of the data stream by some target receiver;

preparing a known portion that both the portable device and some targeted receiver of the wireless signal know;

preparing a data portion to represent the device information; and

preparing an error checking code portion to allow some targeted receiver to check for errors in the received data.

16. The method of claim 15, wherein the preparing the data portion step includes:

reading a counter value from a counter;

assigning a group ID and an individual ID to the portable device;

assigning a secret key in accordance with asymmetric crypto systems; and

IPR2025-01150
Apple EX1071 Page 737

calculating a series by applying a first cryptographic algorithm to the secret key, the group ID, and the counter value.

17. The method of claim 16, wherein the first cryptographic algorithm is Data Encryption Standard (DES3).

18. The method of claim 16, wherein the preparing the data portion step further includes:
incrementing the counter value in the counter.

19. The method of claim 18, wherein the preparing the data portion step further includes:
combining the series and the individual ID.

20. The method of claim 19, further comprising step:
placing the synchronization portion, the known portion, the data portion, and the error checking code portion into a send buffer.

21. The method of claim 20, further comprising steps:
transmitting a first frequency shift keying (FSK) portion to identify a first frequency in a FSK signalling scheme; and
transmitting a second frequency shift keying (FSK) portion to identify a second frequency in the FSK signalling scheme.

22. The method of claim 21, further comprising steps:
transmitting a start bit;
transmitting a selected segment of the send buffer; and
transmitting a stop bit.

23. The method of claim 22, further comprising steps;
determining if any more segment is remaining in the send buffer;
if a segment remains, transmitting a start bit;
transmitting the selected segment of the send buffer; and
transmitting a stop bit.

24. The method of claim 16, wherein the individual ID includes a credit card number.

IPR2025-01150
Apple EX1071 Page 738

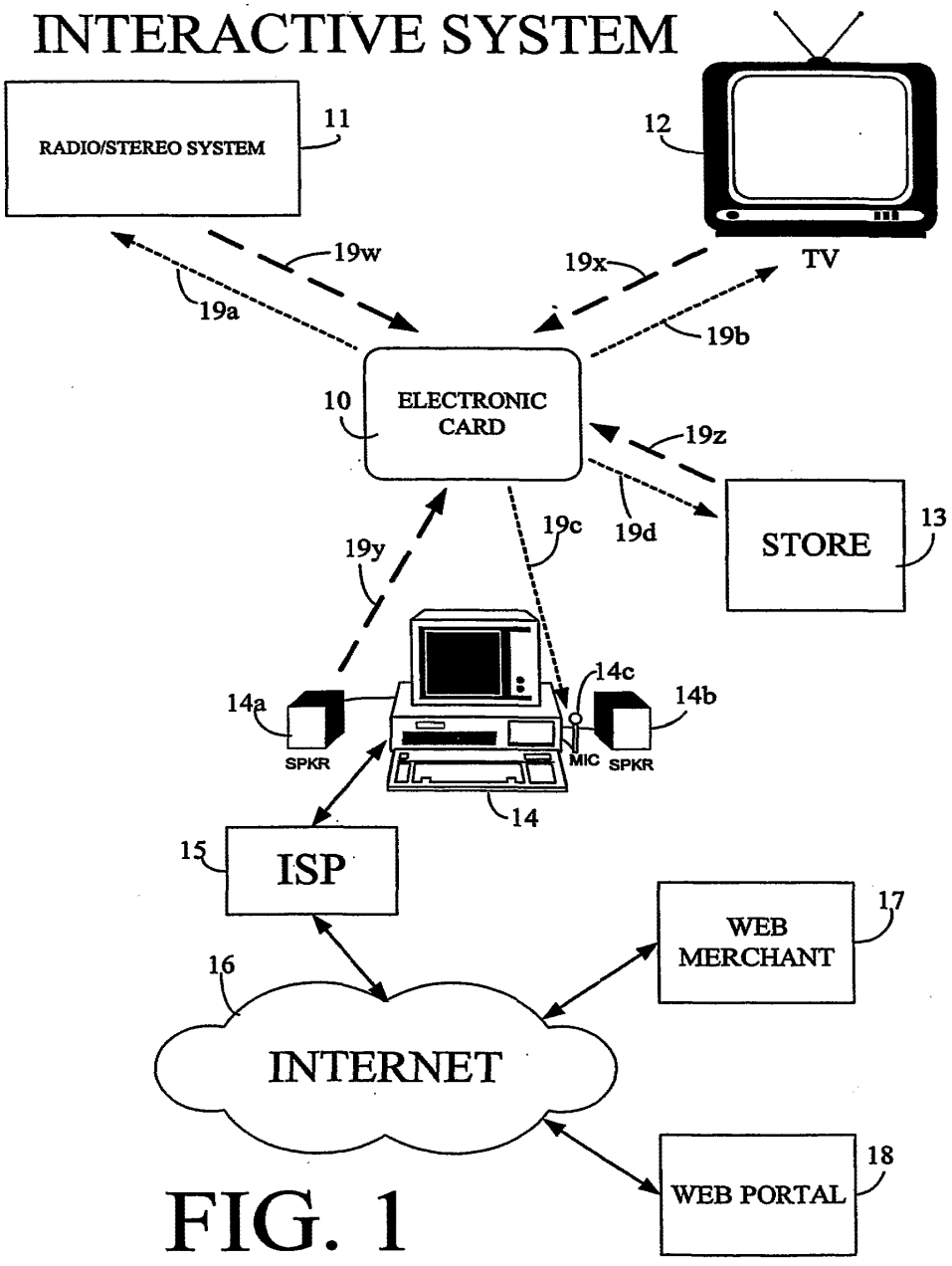

INTERACTIVE SYSTEM
RADIO/STEREO SYSTEM
11
12
TV
19w
19x
19a
19b
10
ELECTRONIC CARD
19z
19y
19c
19d
STORE
13
14a
14c
14b
SPKR
MIC
SPKR
14
15
ISP
16
WEB MERCHANT
17
INTERNET
WEB PORTAL
18

FIG. 1

ONE-WAY TX CARD

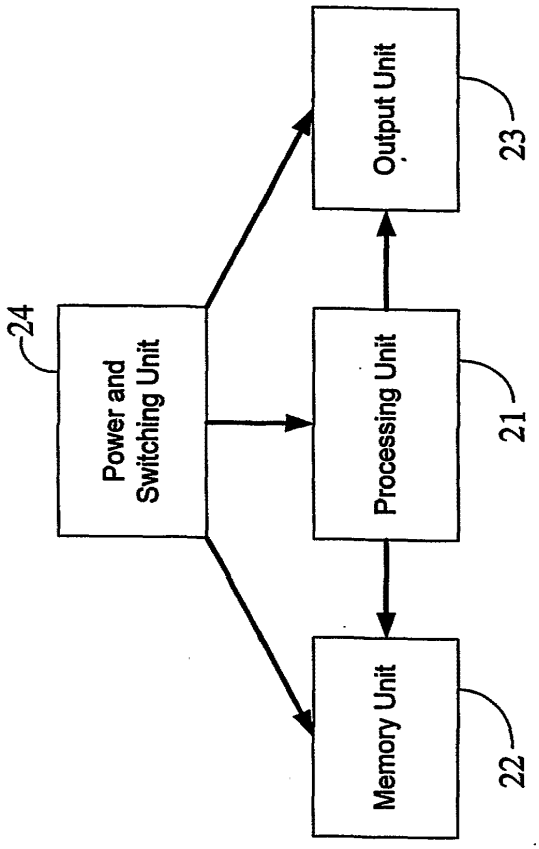


FIG. 2

TWO-WAY CARD

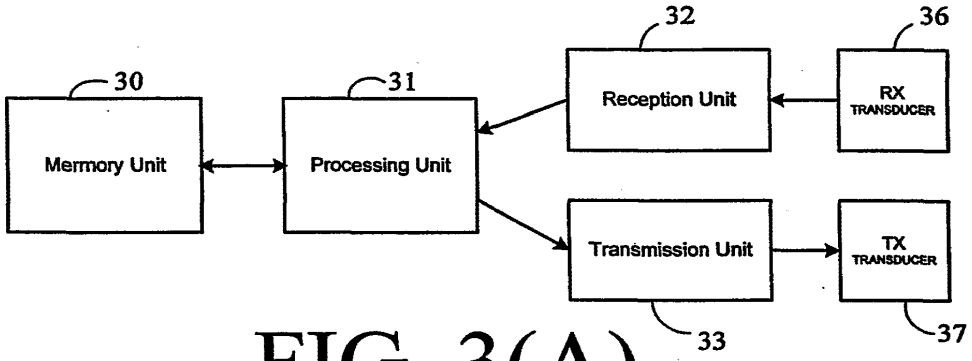


FIG. 3(A)

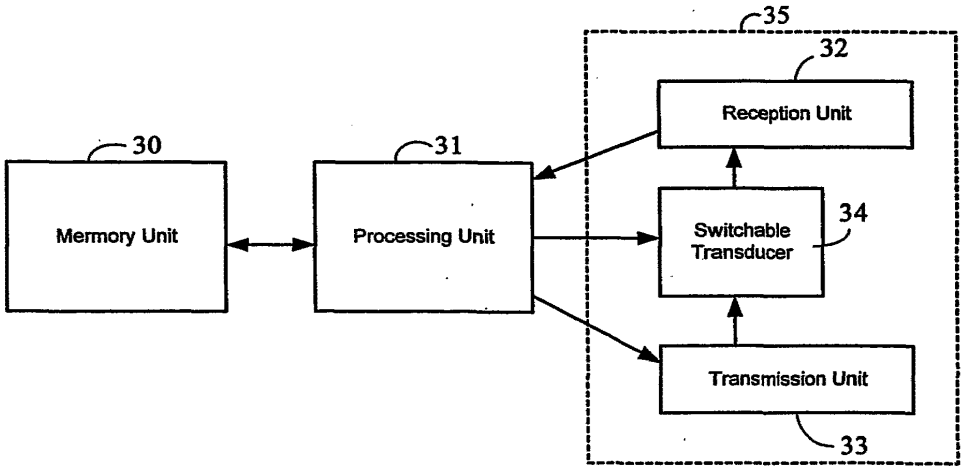


FIG. 3(B)

CARD RECEIVER

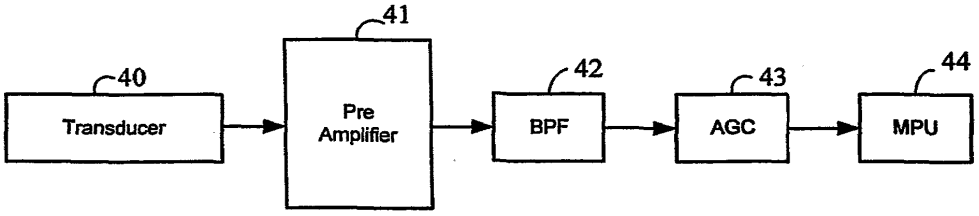


FIG. 4(A)

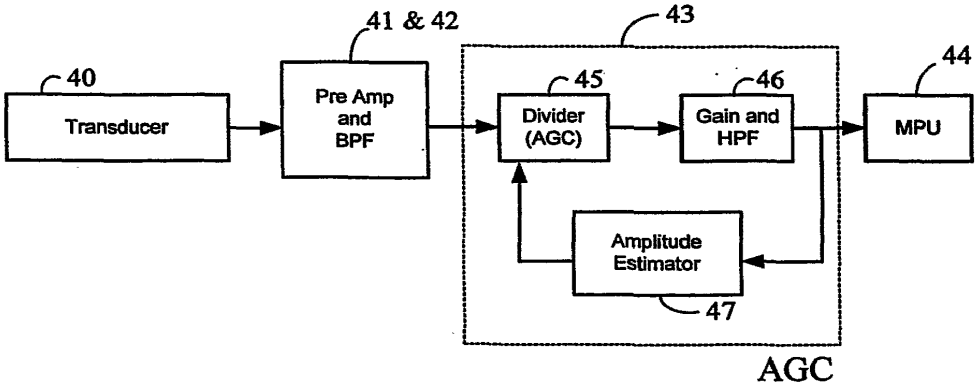


FIG. 4(B)

DATA FORMAT

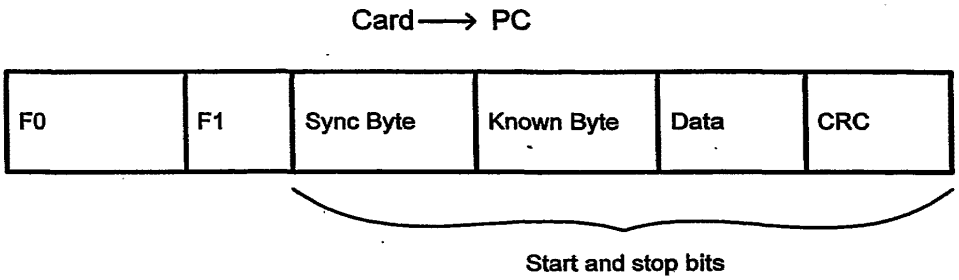


FIG. 5(A)

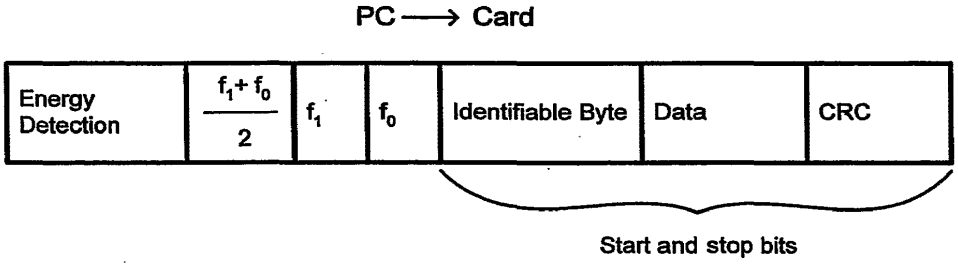


FIG. 5(B)

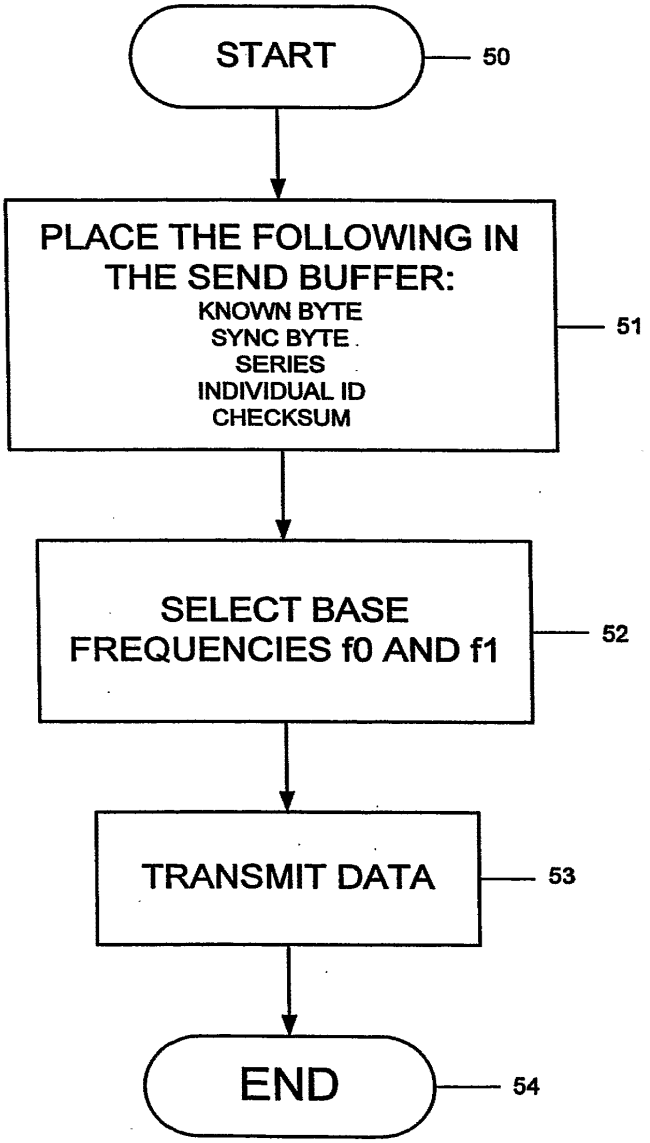

START
50
PLACE THE FOLLOWING IN THE SEND BUFFER:
KNOWN BYTE
SYNC BYTE
SERIES
INDIVIDUAL ID
CHECKSUM
51
SELECT BASE FREQUENCIES f0 AND f1
52
TRANSMIT DATA
53
END
54

FIG. 6(A)

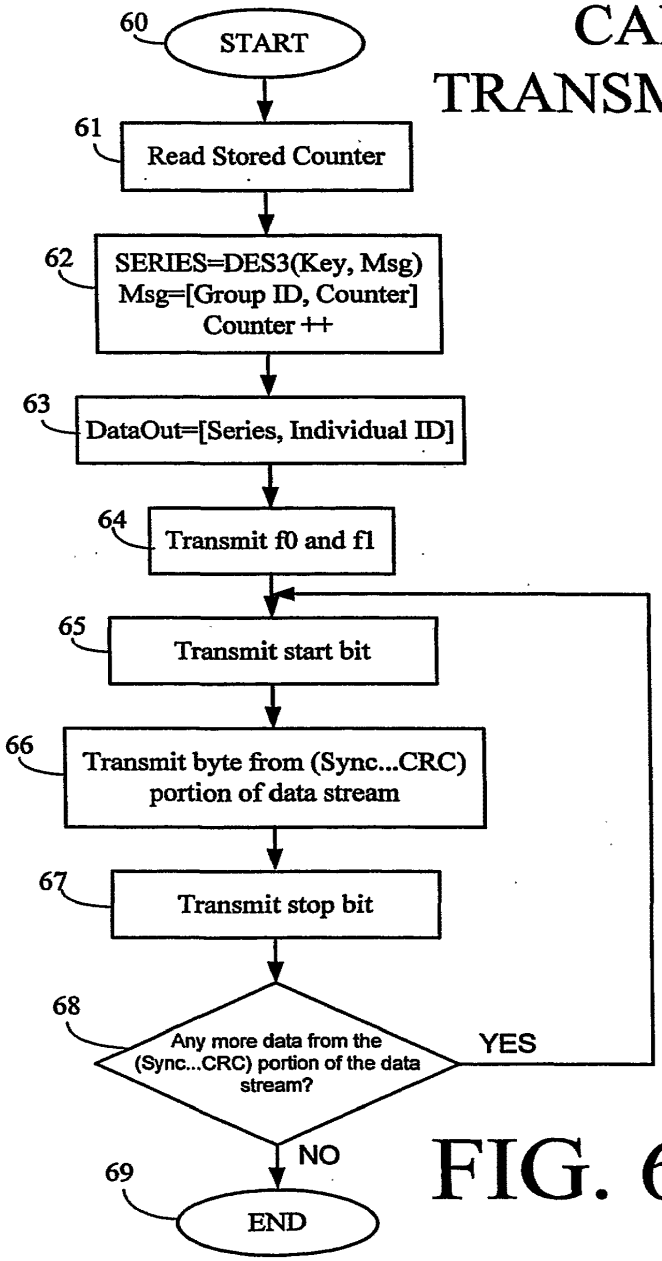

CARD TRANSMISSION
60
START
61
Read Stored Counter
62
SERIES=DES3(Key, Msg)
Msg=[Group ID, Counter]
Counter ++
63
DataOut=[Series, Individual ID]
64
Transmit f0 and f1
65
Transmit start bit
66
Transmit byte from (Sync...CRC) portion of data stream
67
Transmit stop bit
68
Any more data from the (Sync...CRC) portion of the data stream?
YES
NO
69
END

FIG. 6(B)

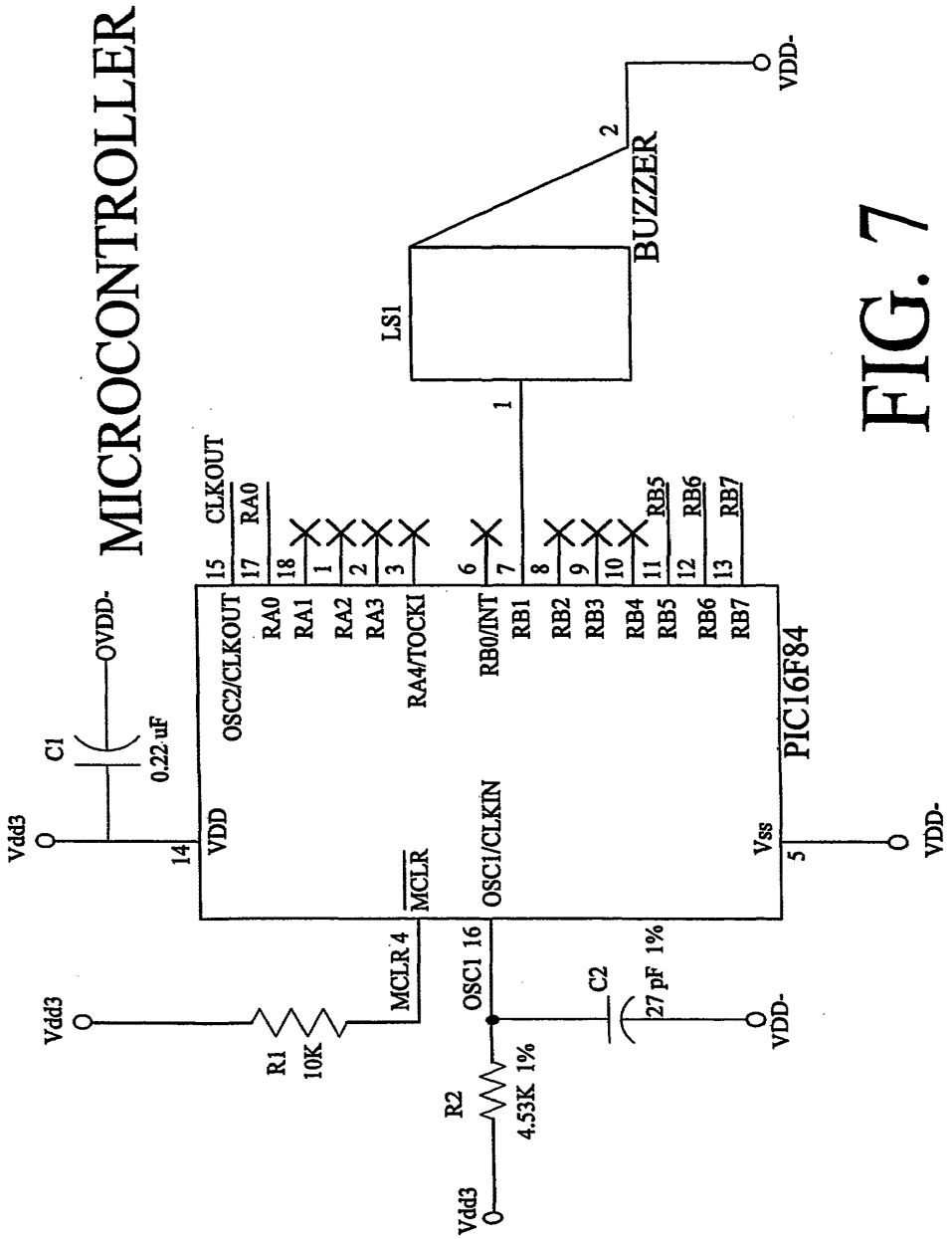

MICROCONTROLLER
PIC16F84
OSC2/CLKOUT
RA0
RA1
RA2
RA3
RA4/TOCKI
RB0/INT
RB1
RB2
RB3
RB4
RB5
RB6
RB7
VDD
MCLR
OSC1/CLKIN
Vss
CLKOUT
C1
0.22 uF
OVDD-
Vdd3
VDD-
LS1
BUZZER
R1
10K
R2
4.53K 1%
C2
27 pF 1%
MCLR 4
OSC1 16
14
15
17
18
1
2
3
6
7
8
9
10
11
12
13
5

FIG. 7

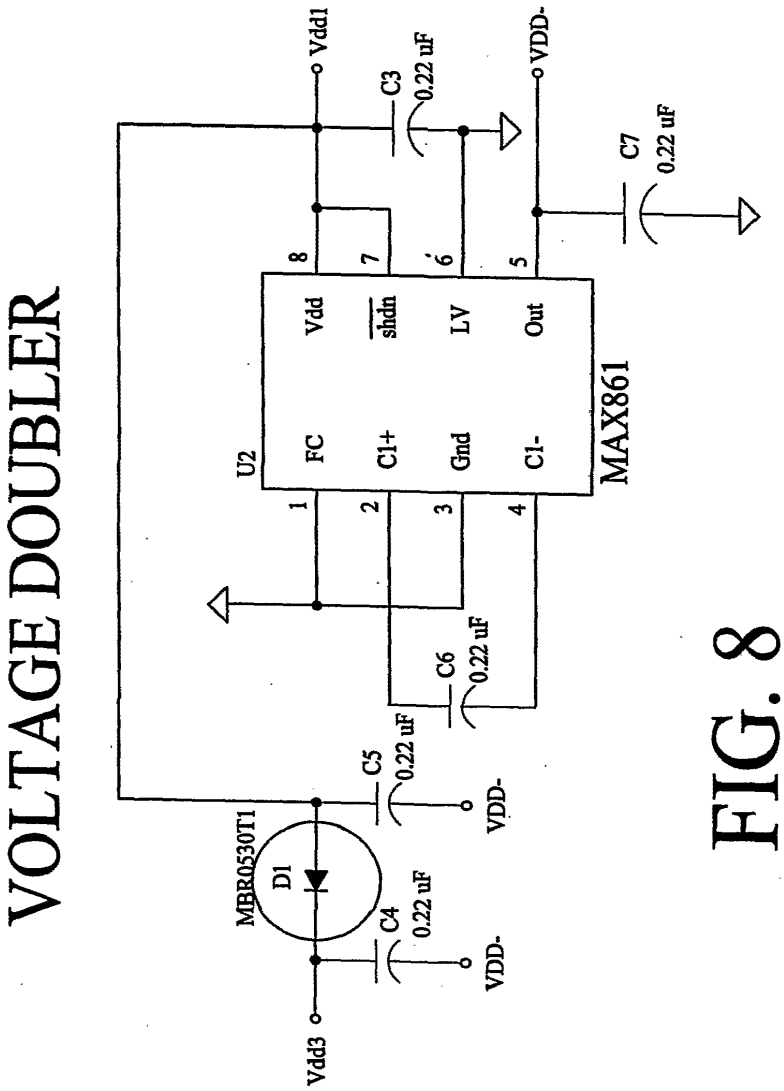

VOLTAGE DOUBLER
Vdd1
C3
0.22 uF
VDD-
C7
0.22 uF
U2
FC
C1+
Gnd
C1-
Vdd
shdn
LV
Out
MAX861
1
2
3
4
8
7
6
5
C6
0.22 uF
C5
0.22 uF
VDD-
MBR0530T1
D1
C4
0.22 uF
VDD-
Vdd3

FIG. 8

POWER AND SWITCHING CIRCUIT

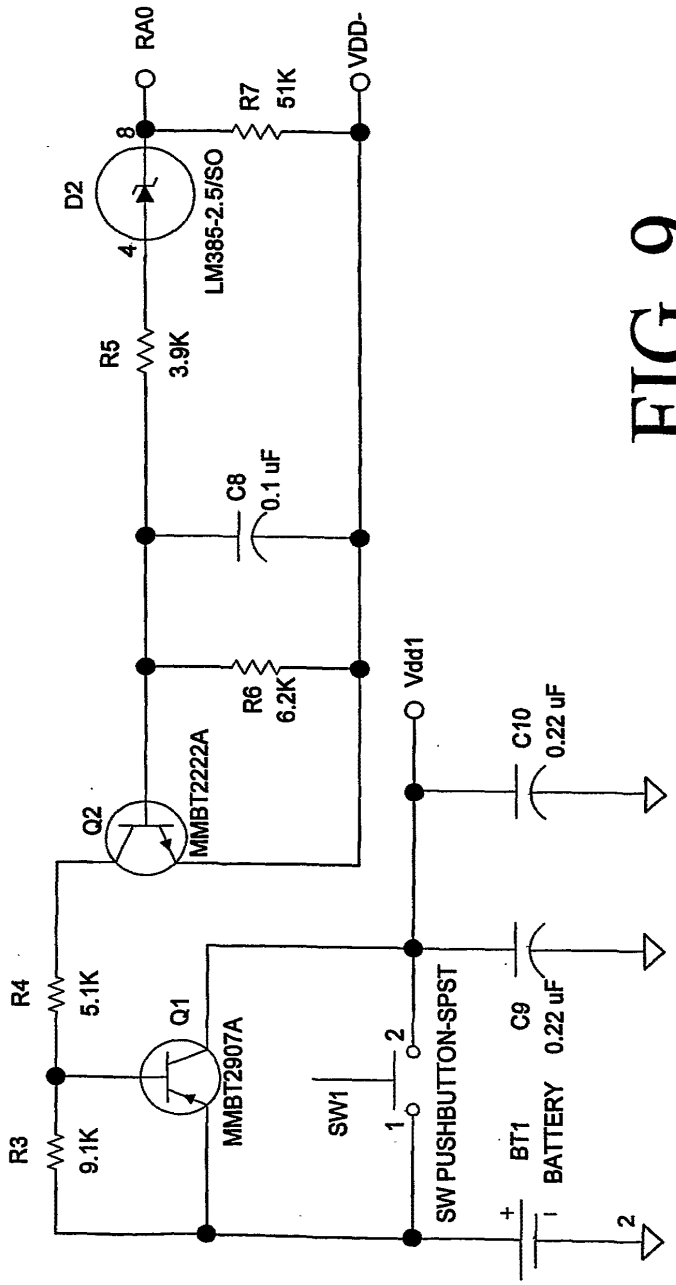


FIG. 9

SMART CARD CONNECTOR

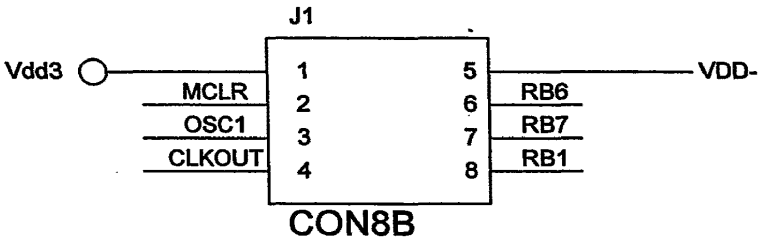


FIG. 10

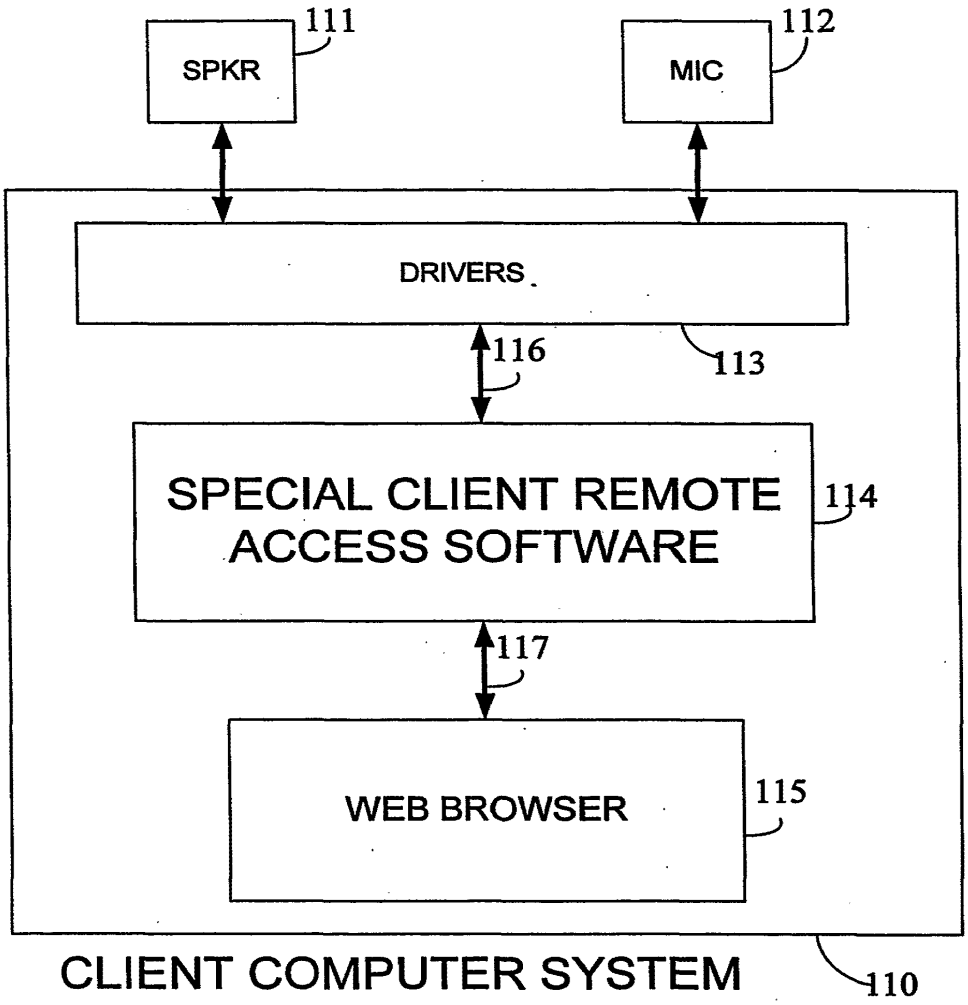

111
SPKR
112
MIC
DRIVERS
116
113
SPECIAL CLIENT REMOTE ACCESS SOFTWARE
114
117
WEB BROWSER
115
CLIENT COMPUTER SYSTEM
110

FIG. 11

CARD RECEPTION SOFTWARE

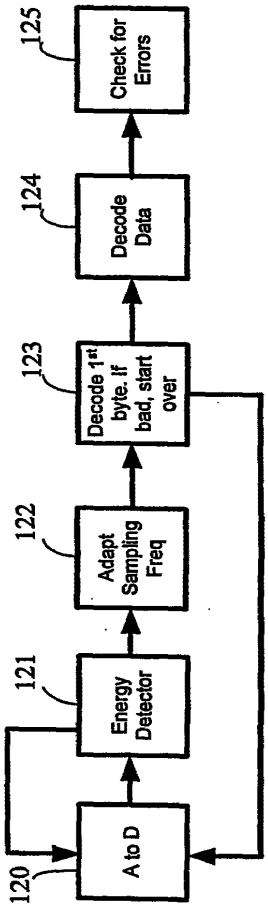
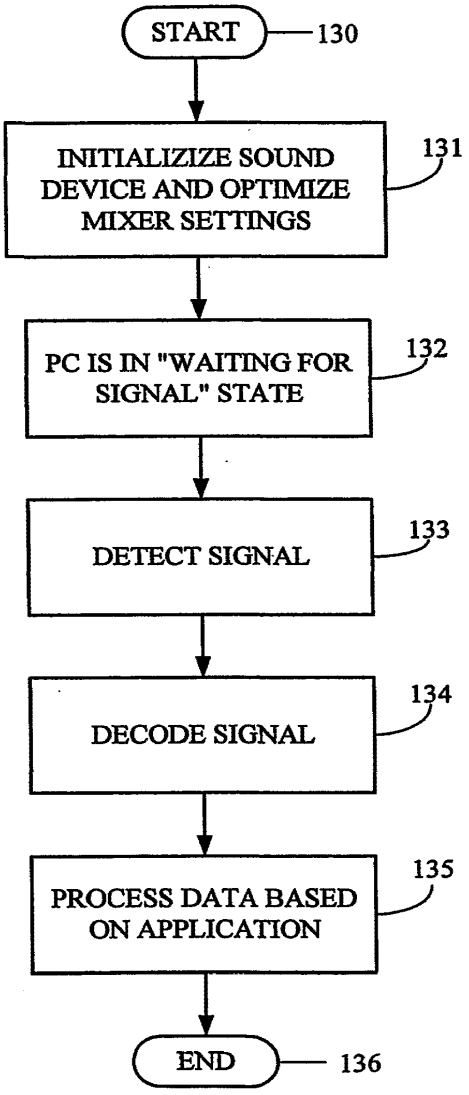


FIG. 12



PC RX SOFTWARE

FIG. 13

SIGNAL DECODER

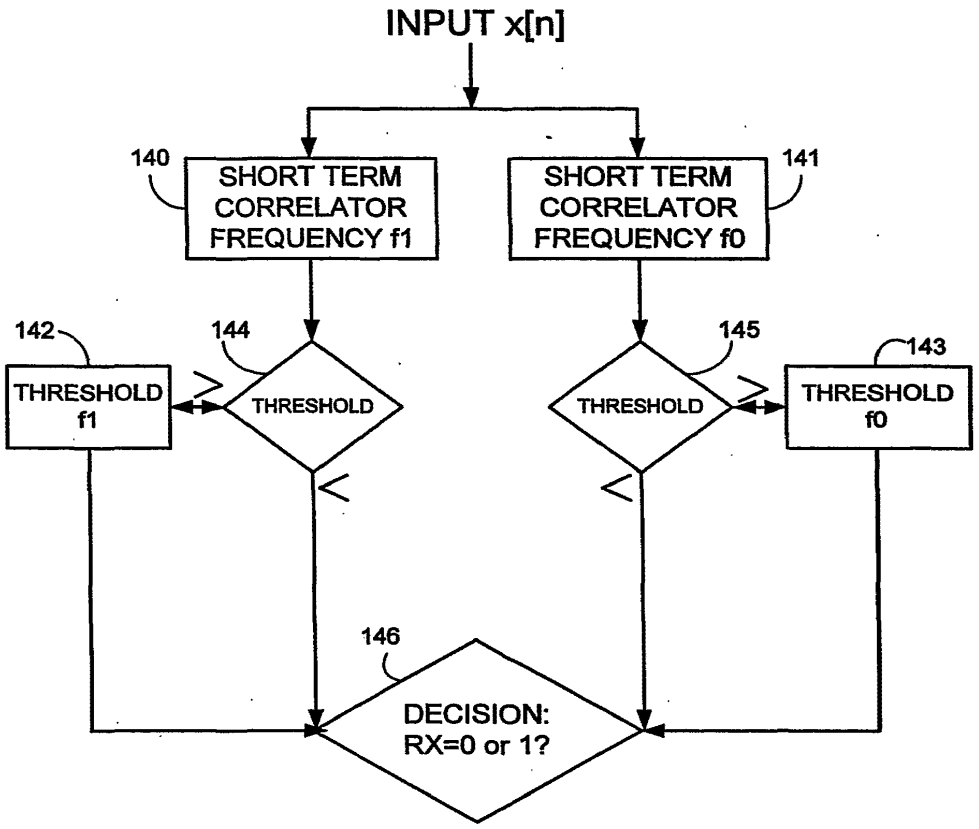
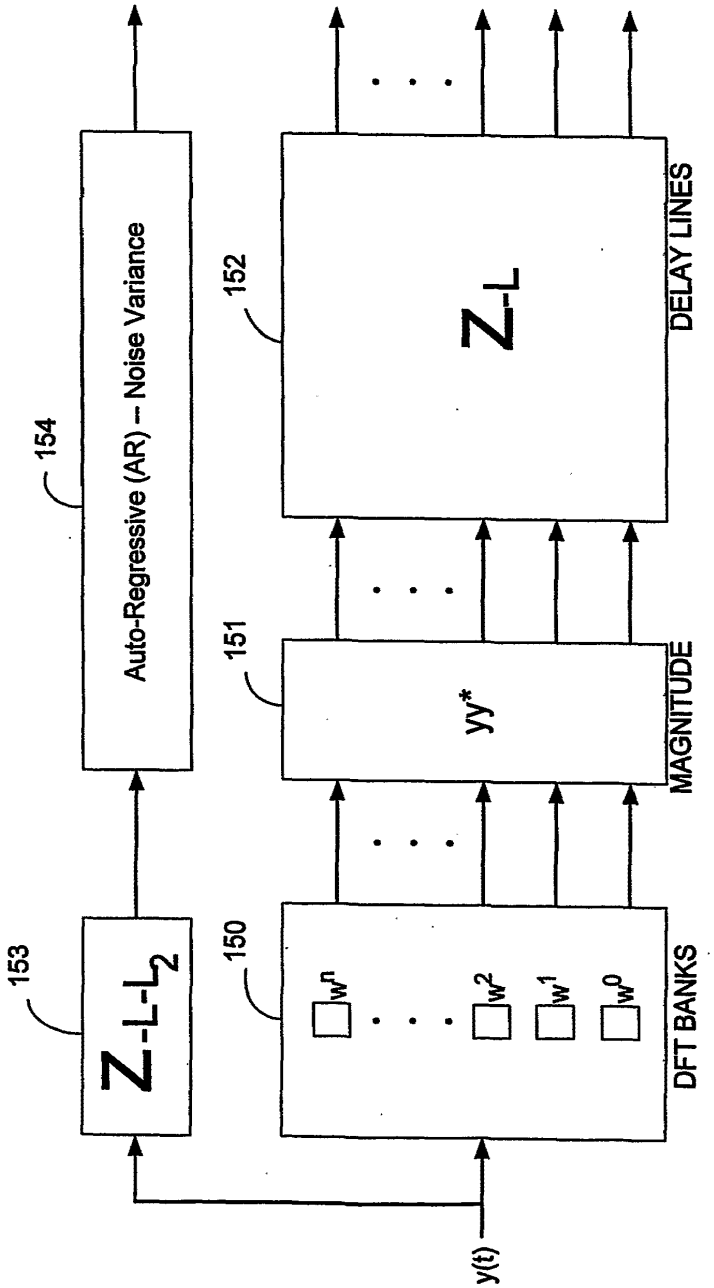


FIG. 14

FIG. 15


SIGNAL DETECTION
y(t)
150
DFT BANKS
151
MAGNITUDE
yy*
152
DELAY LINES
Z_{-L}
153
Z_{-L-L_2}
154
Auto-Regressive (AR) -- Noise Variance

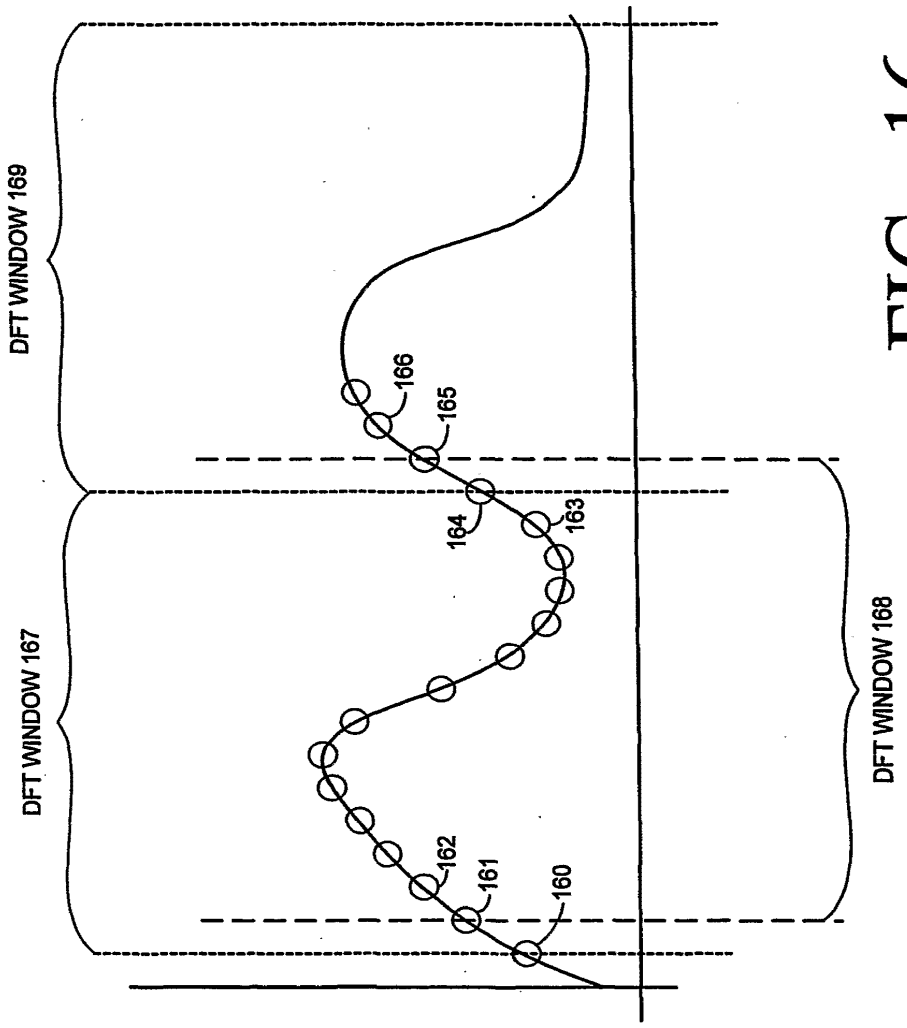

DFT WINDOW 169
DFT WINDOW 167
DFT WINDOW 168
166
165
164
163
162
161
160

FIG. 16

ALTERNATIVE EMBODIMENT
-- ONE-WAY TX HARDWARE

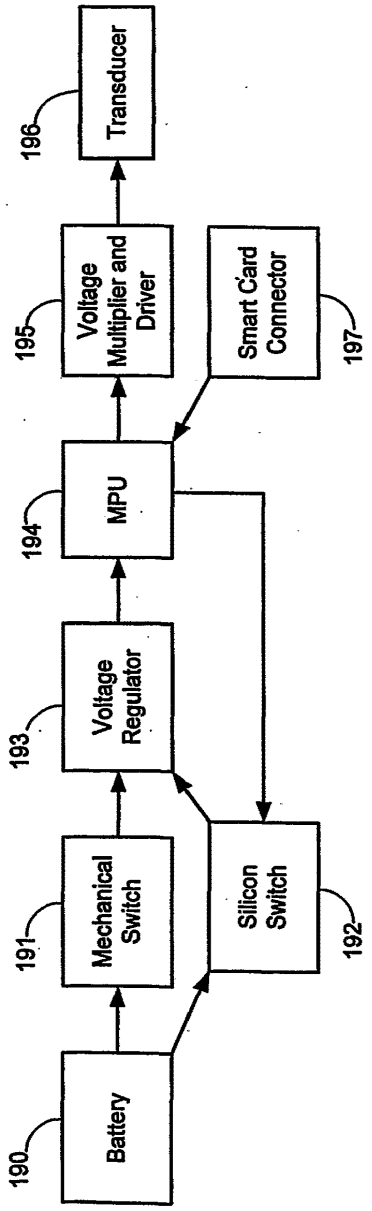
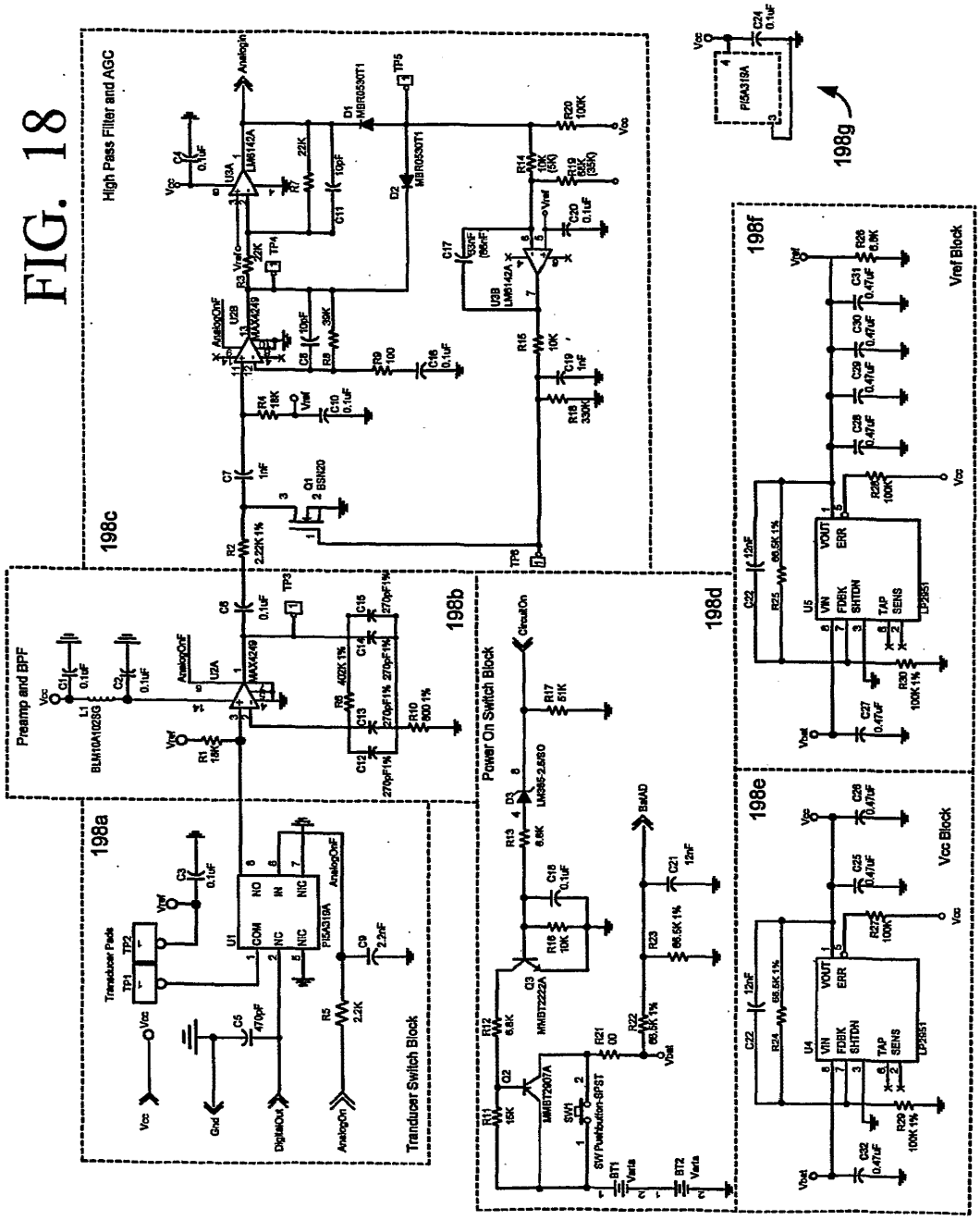


FIG. 17

FIG. 18


198a
Tranducer Switch Block
198b
Preamp and BPF
198c
High Pass Filter and AGC
198d
Power On Switch Block
198e
Vcc Block
198f
Vref Block
198g

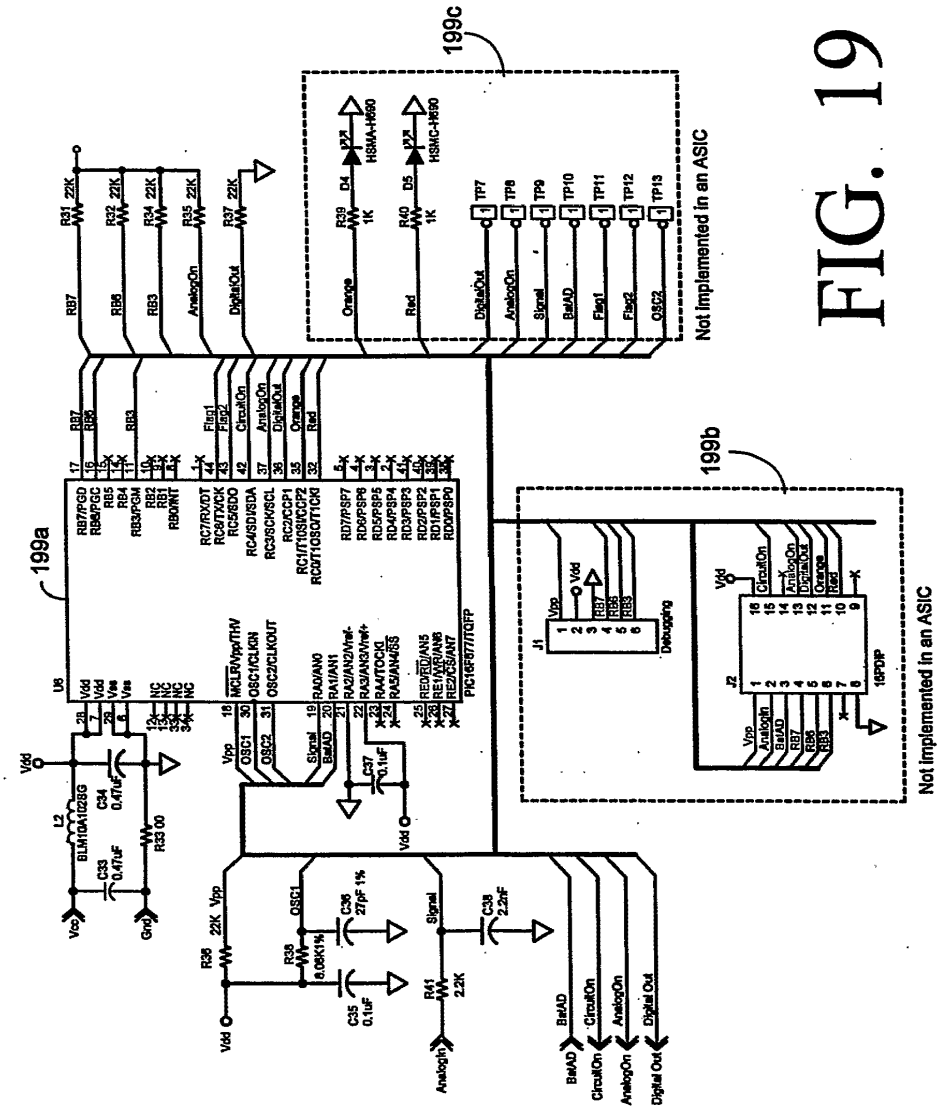

199a
199b
199c
Not implemented in an ASIC
Not implemented in an ASIC
PIC16F877/TQFP
Debugging
16PDIP
HSMA-H690
HSMC-H690

FIG. 19

CARD ARCHITECTURE
-- ANALOG RECORDING

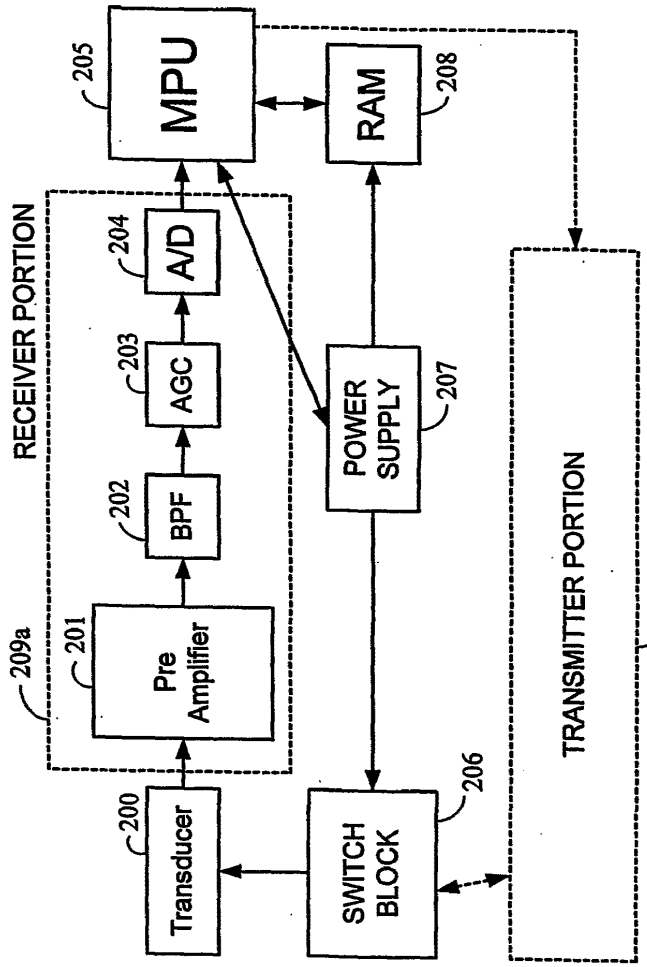


FIG. 20

SERVER ARCHITECTURE

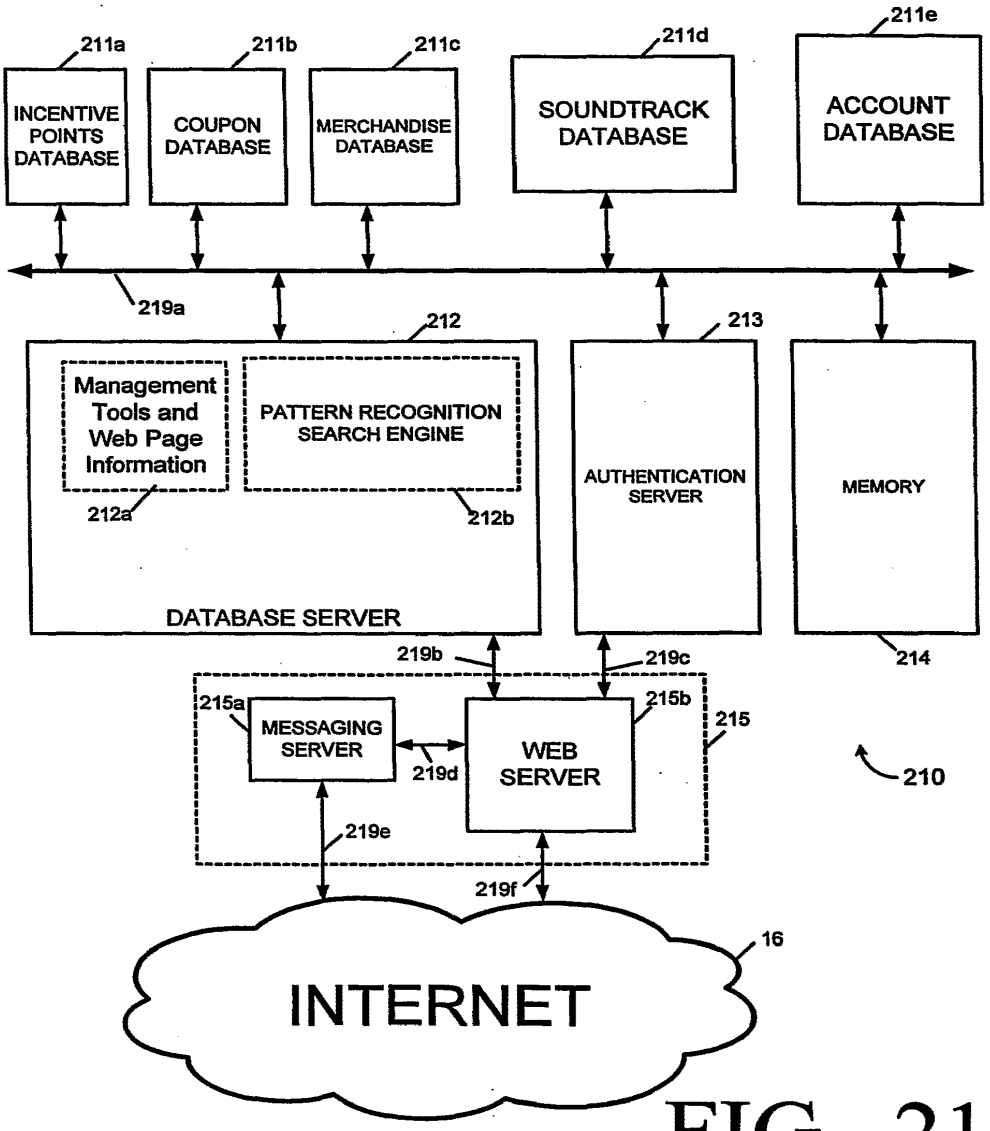


FIG. 21

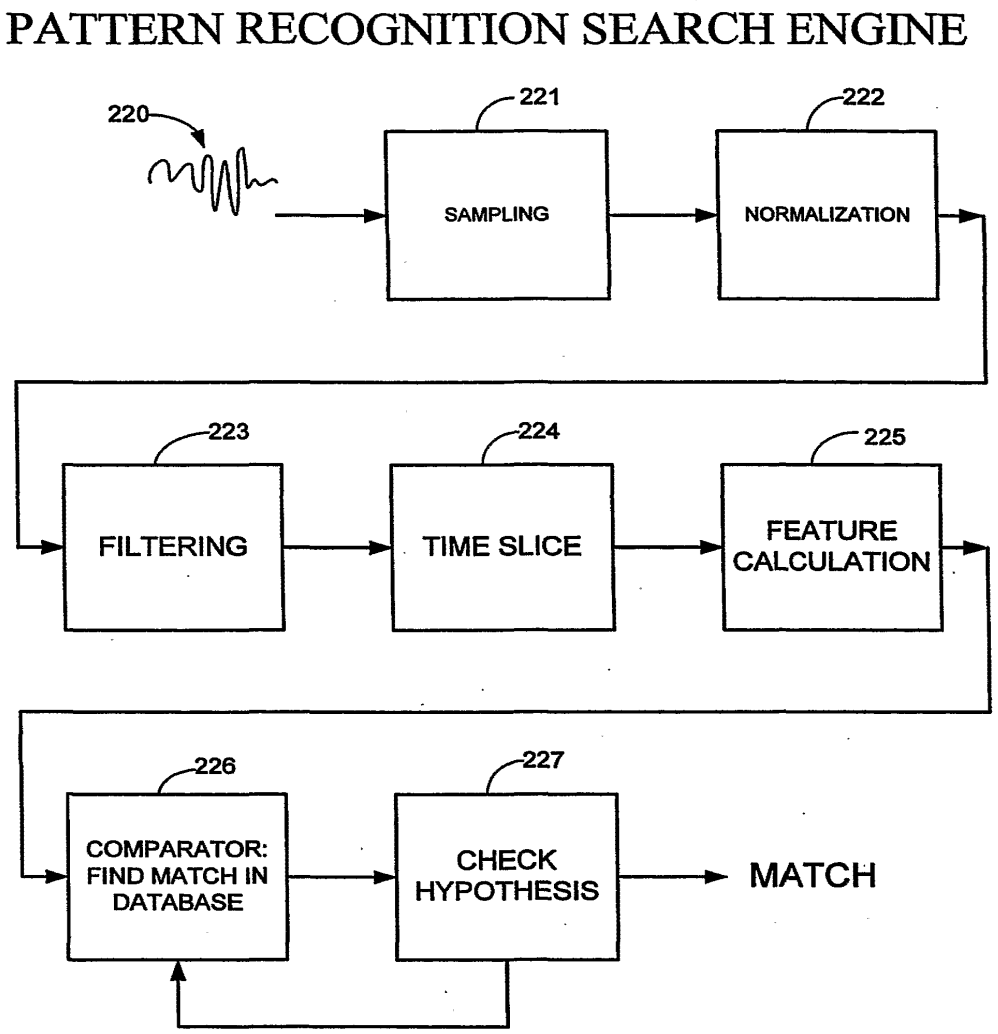

PATTERN RECOGNITION SEARCH ENGINE
220
221
SAMPLING
222
NORMALIZATION
223
FILTERING
224
TIME SLICE
225
FEATURE CALCULATION
226
COMPARATOR: FIND MATCH IN DATABASE
227
CHECK HYPOTHESIS
MATCH

FIG. 22

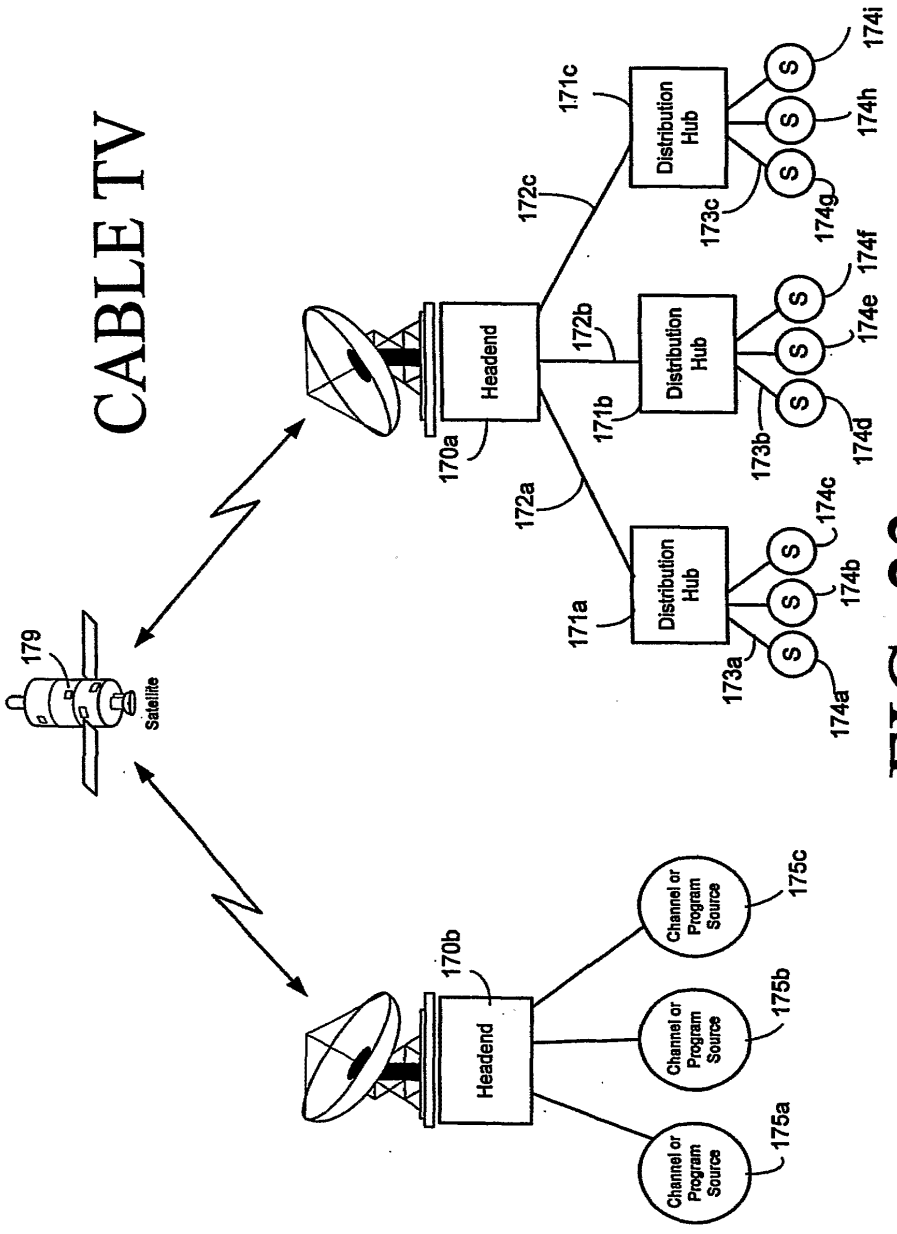

CABLE TV
179
Satellite
170a
Headend
170b
Headend
171a
Distribution Hub
171b
Distribution Hub
171c
Distribution Hub
172a
172b
172c
173a
173b
173c
174a
174b
174c
174d
174e
174f
174g
174h
174i
175a
Channel or Program Source
175b
Channel or Program Source
175c
Channel or Program Source

FIG. 23

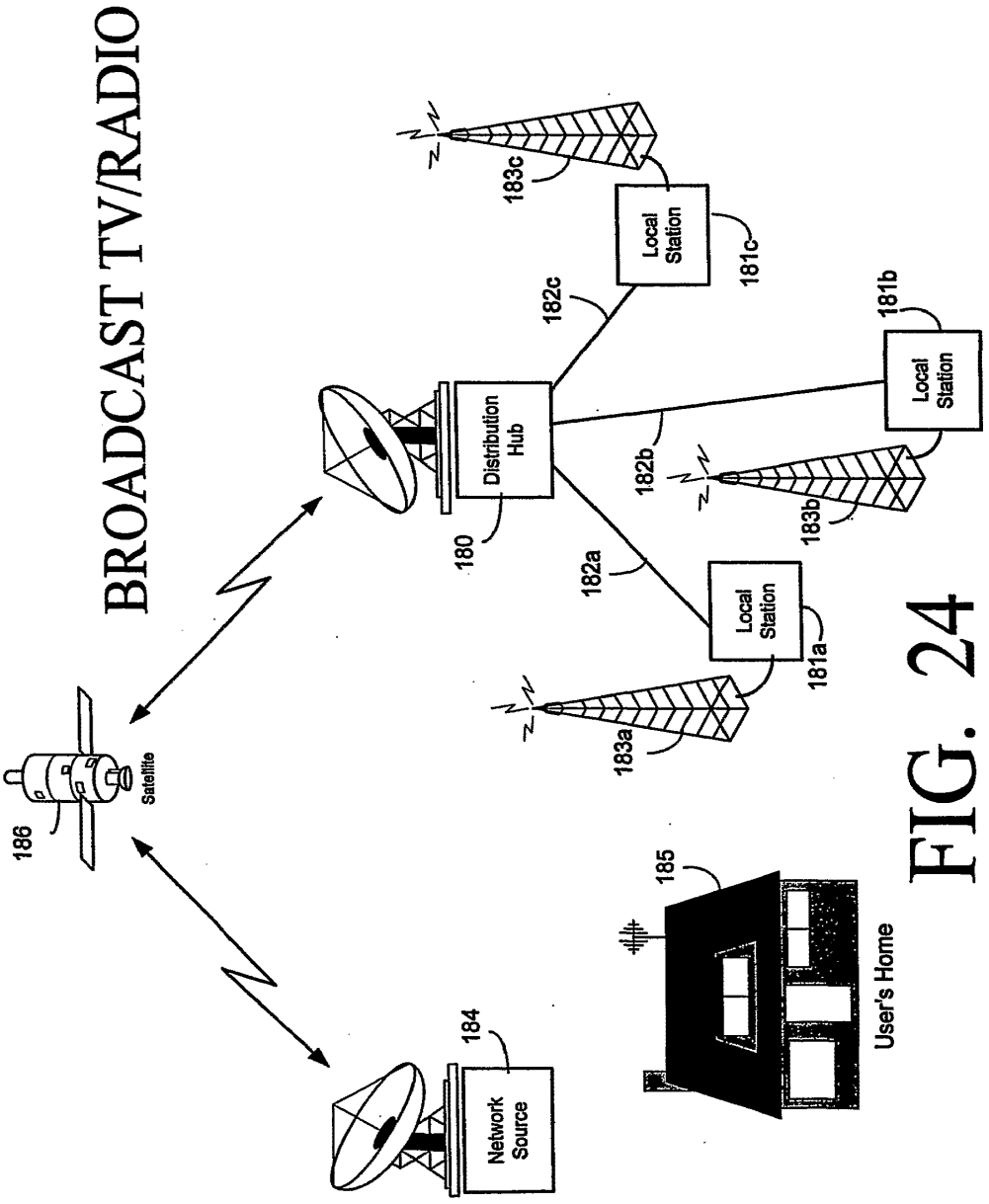

BROADCAST TV/RADIO
Satellite
186
Network Source
184
Distribution Hub
180
Local Station
181a
Local Station
181b
Local Station
181c
182a
182b
182c
183a
183b
183c
185
User's Home

FIG. 24

COMPONENT LAYOUT #1

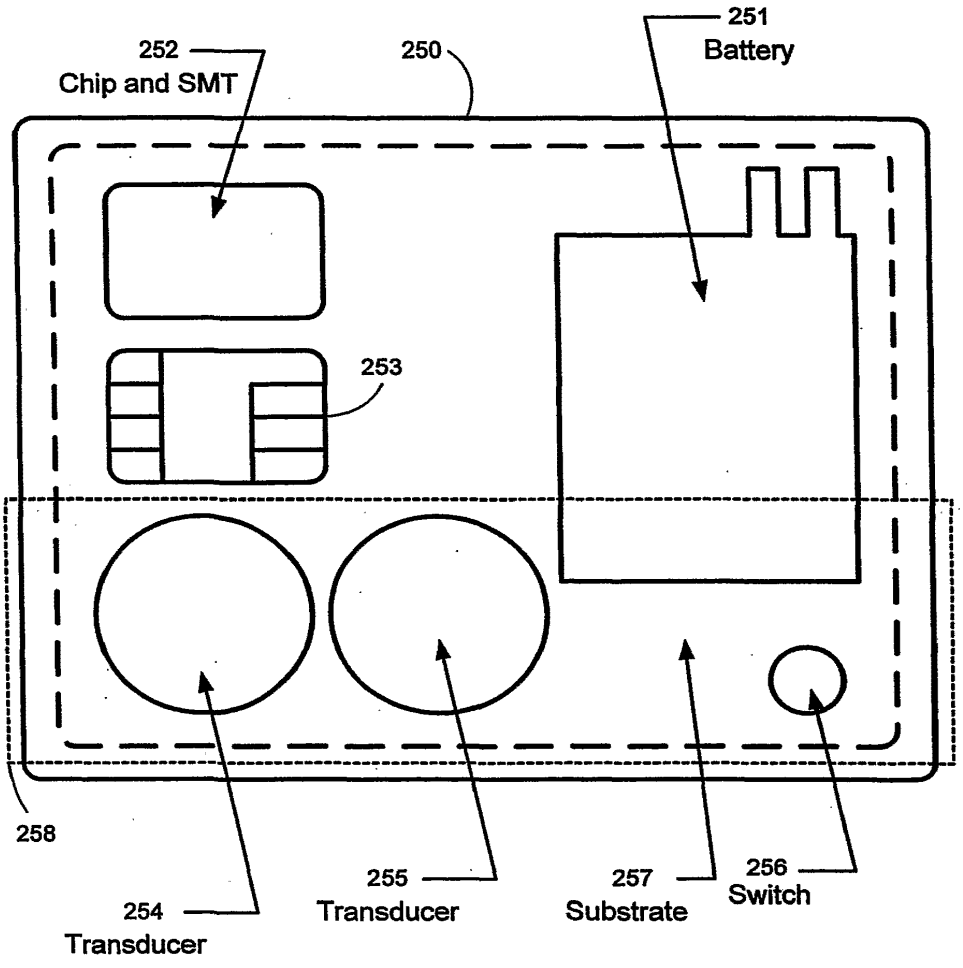


FIG. 25(A)

COMPONENT LAYOUT #2

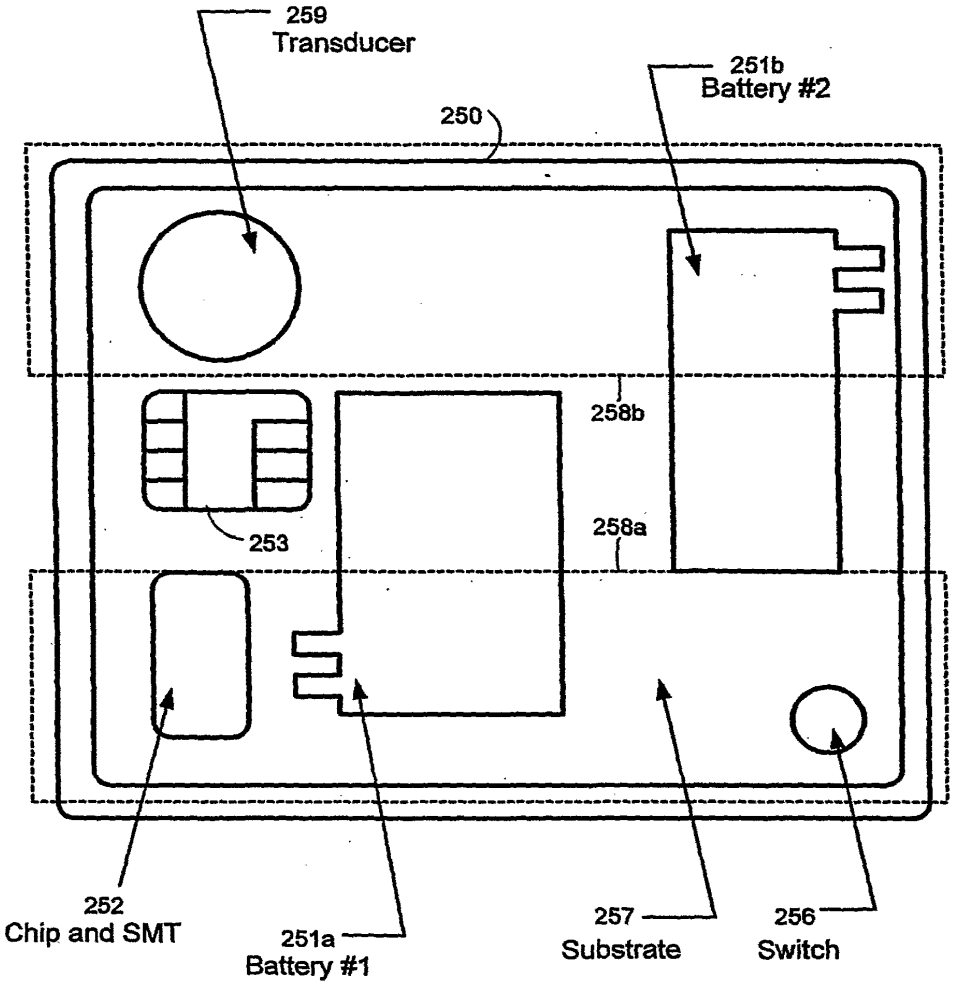


FIG. 25(B)

COMPONENT LAYOUT #3

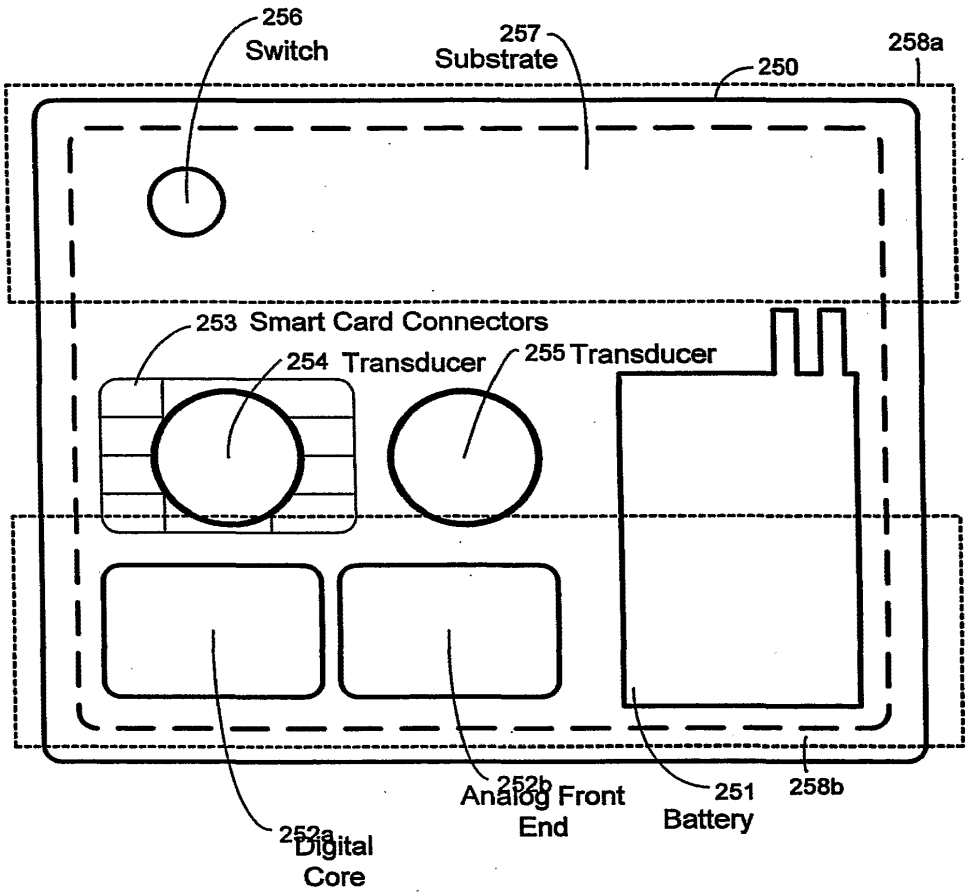


FIG. 25(C)

CARD FABRICATION

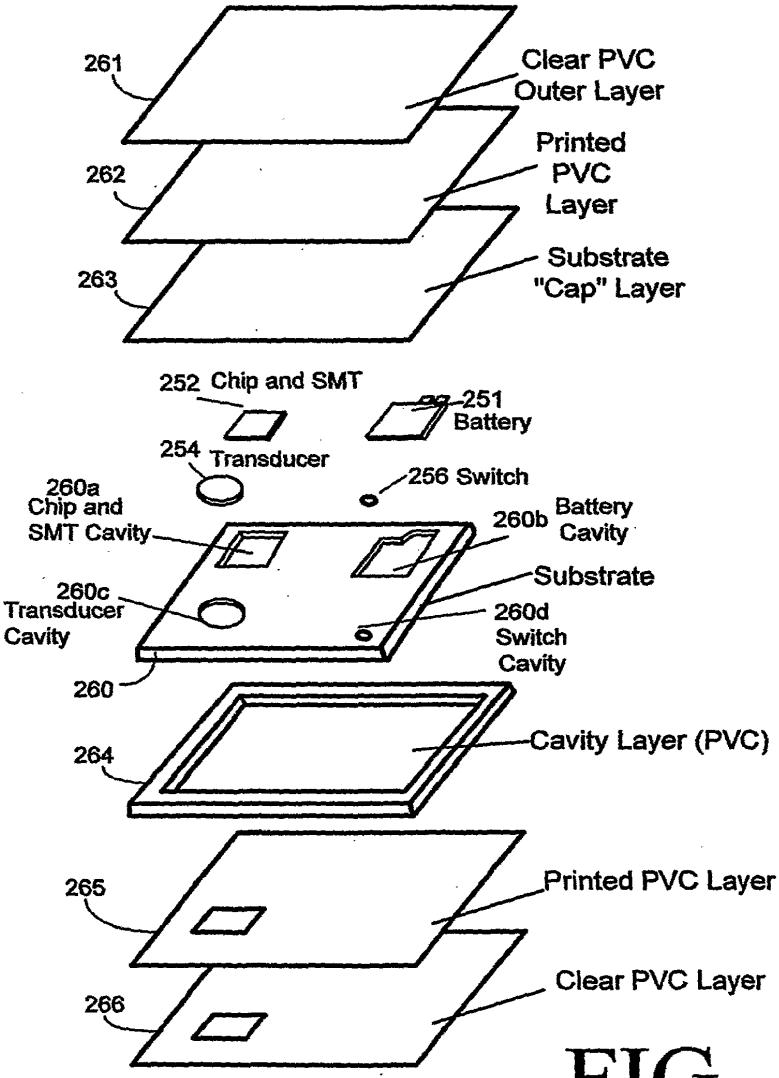


FIG. 26

TRANSDUCER FABRICATION

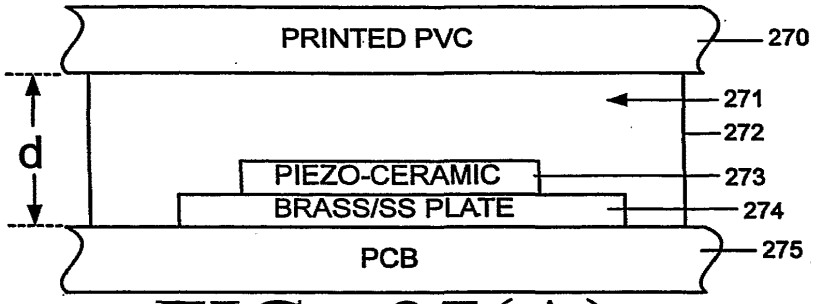


FIG. 27(A)

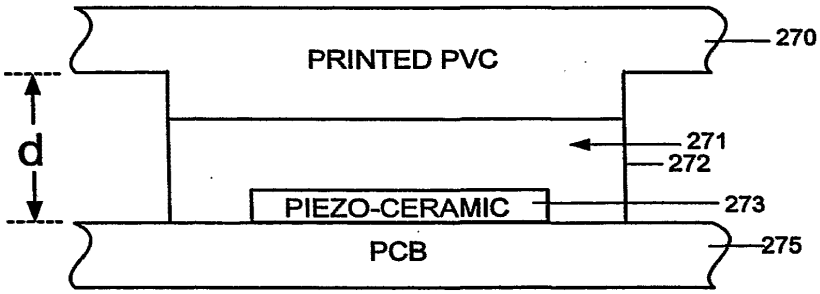


FIG. 27(B)

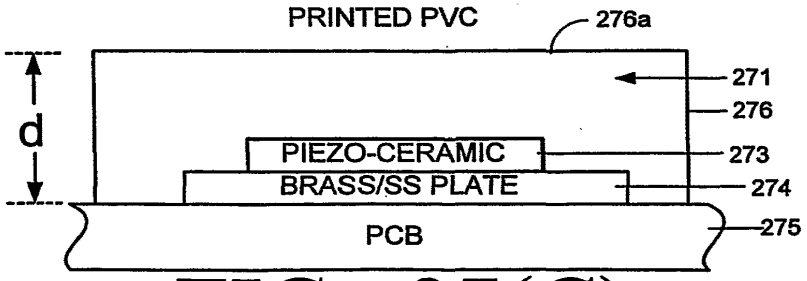


FIG. 27(C)

MULTI-MODE SWITCH

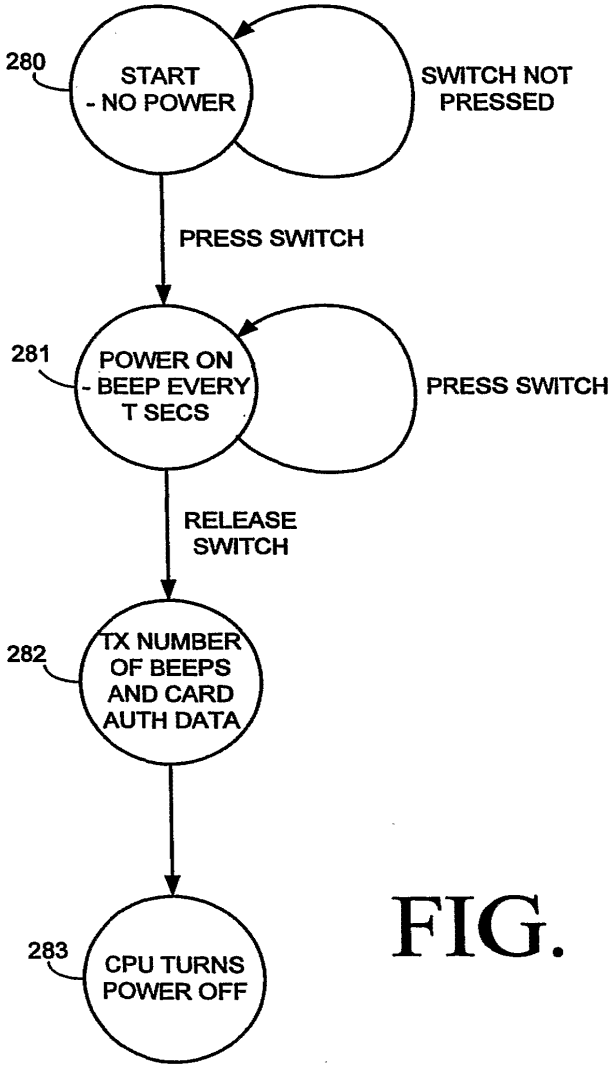


FIG. 28

E-WALLET SYSTEM

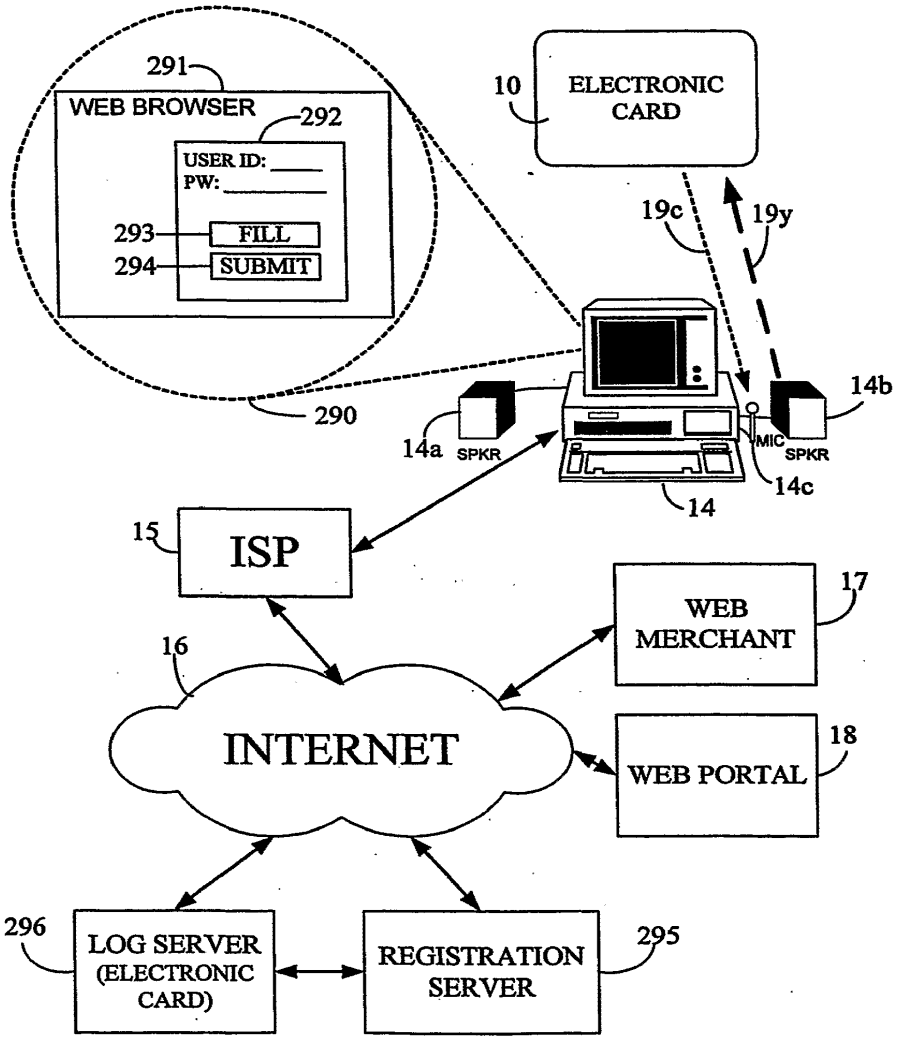
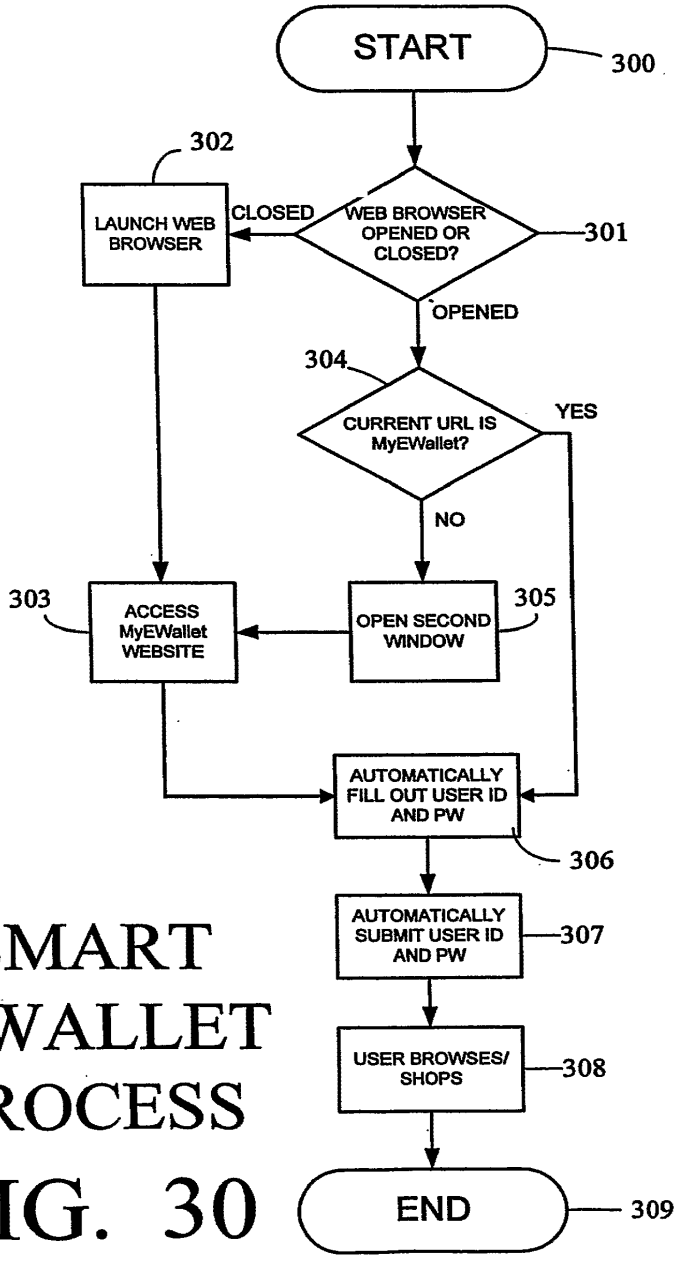


FIG. 29



SMART E-WALLET PROCESS

FIG. 30

CREDIT CARD TRANSACTION MODEL

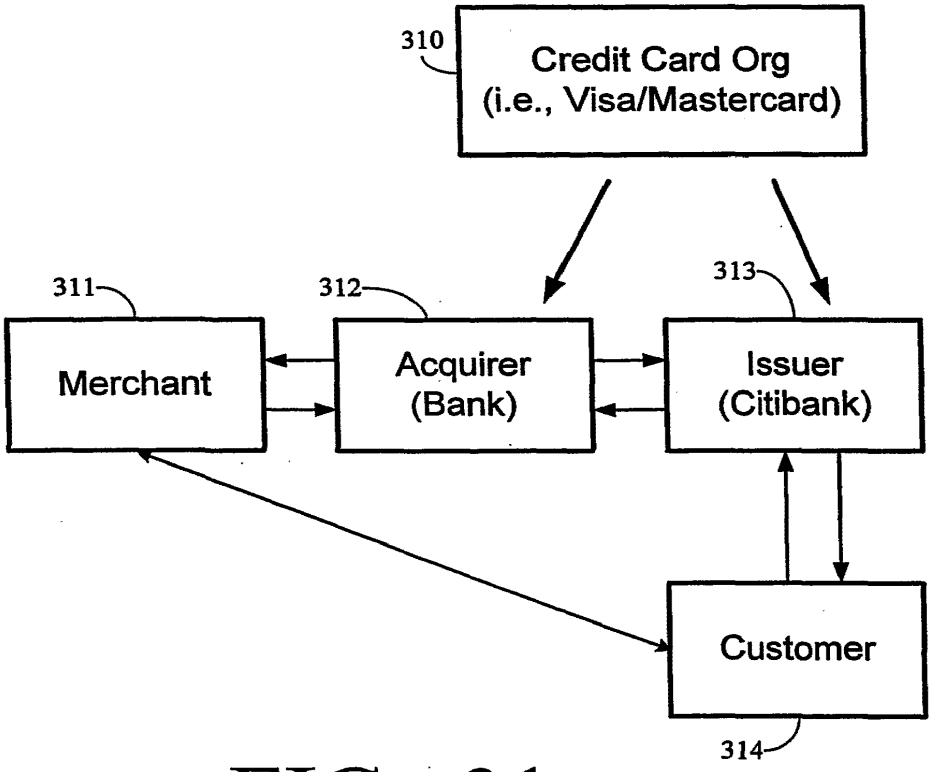


FIG. 31

ON-LINE AUTHENTICATION

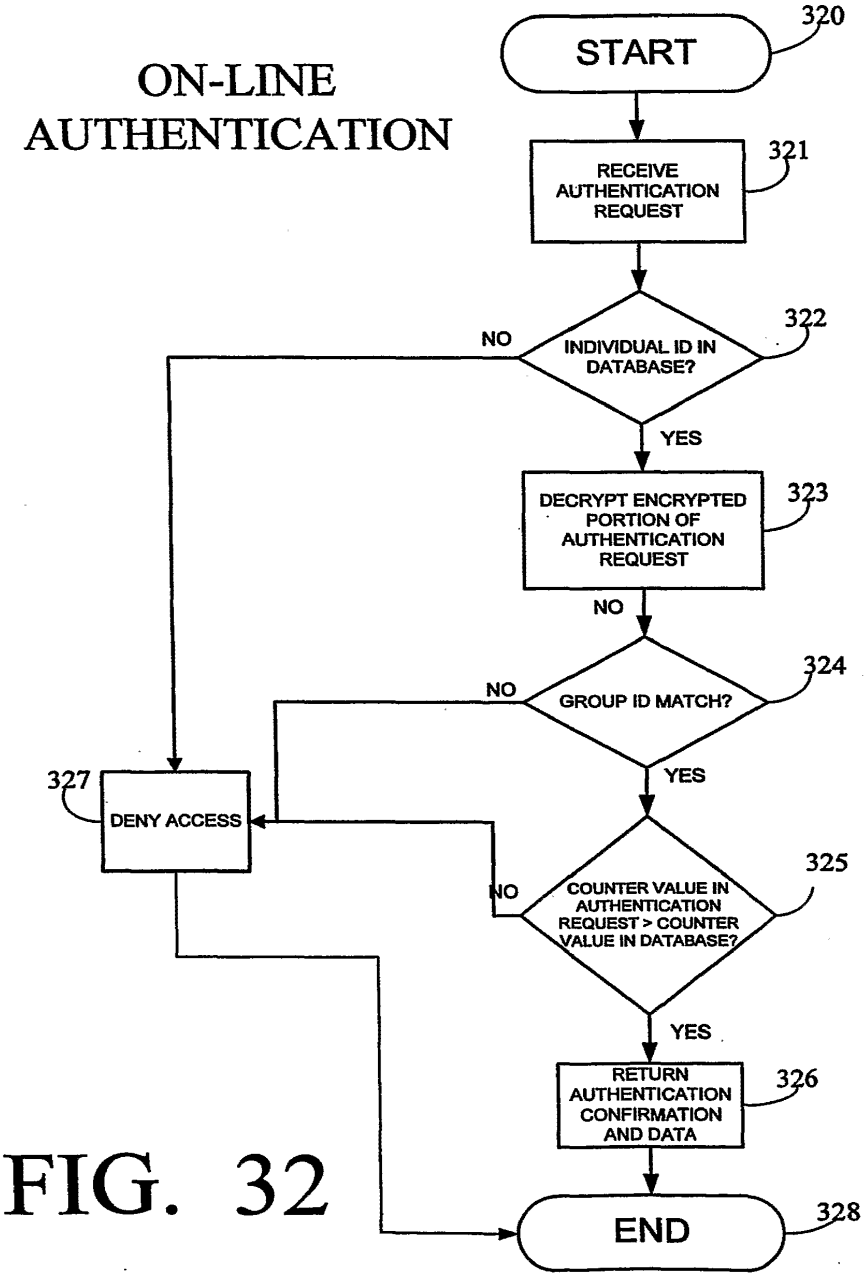


FIG. 32

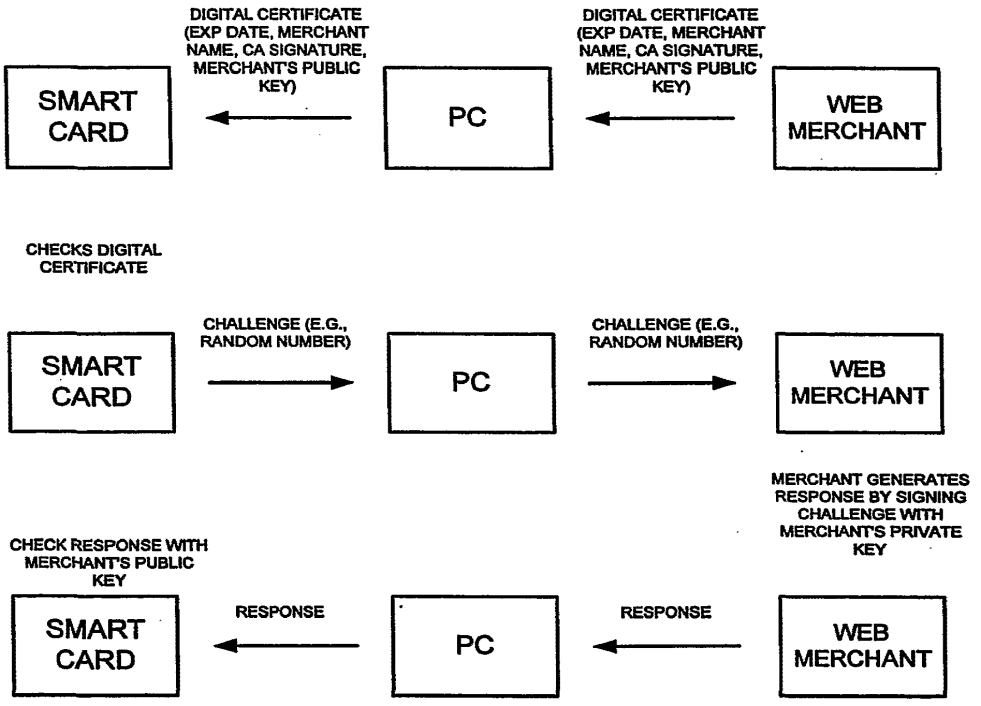

CHALLENGE-RESPONSE:
CUSTOMER CHECKS MERCHANT
DIGITAL CERTIFICATE (EXP DATE, MERCHANT NAME, CA SIGNATURE, MERCHANT'S PUBLIC KEY)
DIGITAL CERTIFICATE (EXP DATE, MERCHANT NAME, CA SIGNATURE, MERCHANT'S PUBLIC KEY)
SMART CARD
PC
WEB MERCHANT
CHECKS DIGITAL CERTIFICATE
CHALLENGE (E.G., RANDOM NUMBER)
CHALLENGE (E.G., RANDOM NUMBER)
SMART CARD
PC
WEB MERCHANT
MERCHANT GENERATES RESPONSE BY SIGNING CHALLENGE WITH MERCHANT'S PRIVATE KEY
CHECK RESPONSE WITH MERCHANT'S PUBLIC KEY
RESPONSE
RESPONSE
SMART CARD
PC
WEB MERCHANT

FIG. 33

CHALLENGE-RESPONSE: MERCHANT CHECKS CUSTOMER

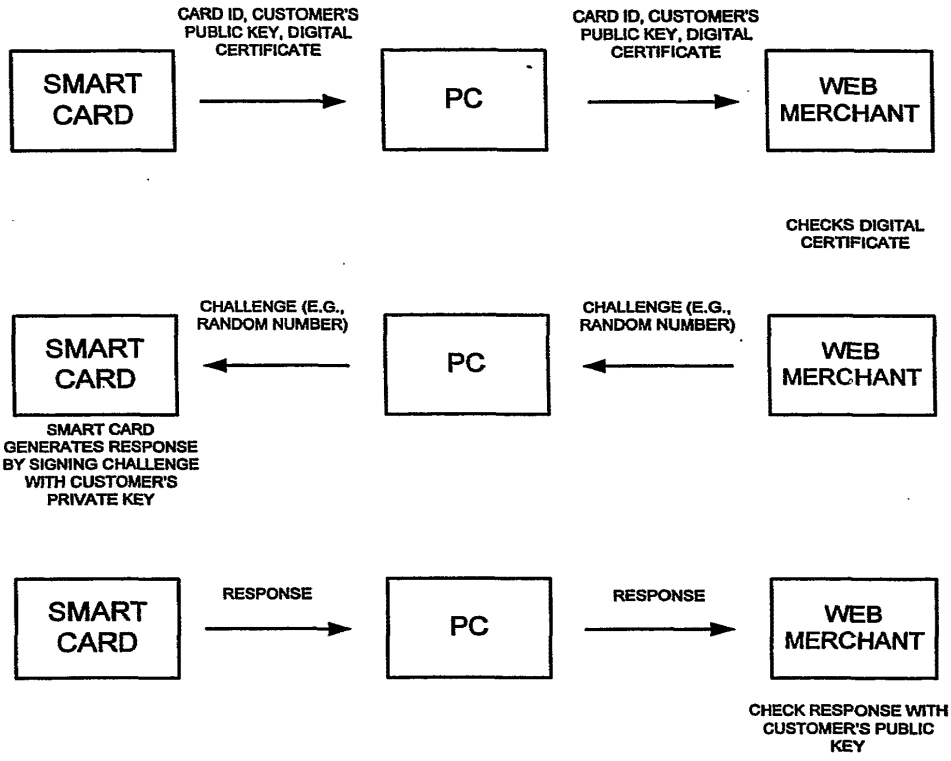


FIG. 34

CONCURRENT CHALLENGE-RESPONSE: MERCHANT AND CUSTOMER CHECK EACH OTHER

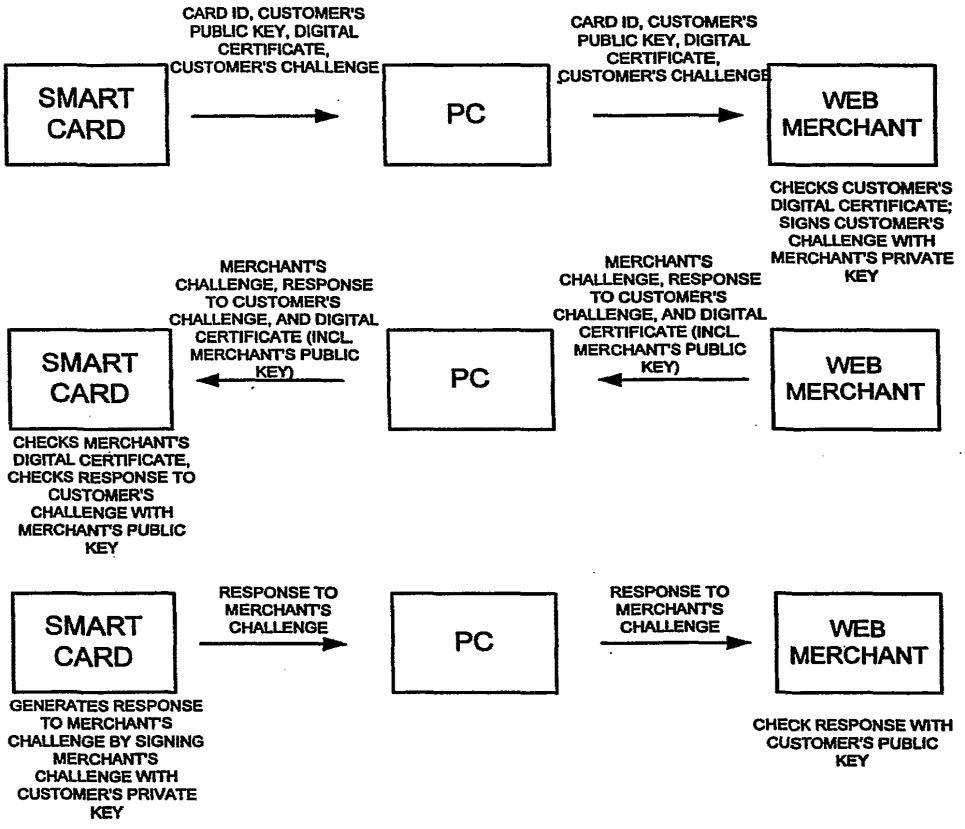


FIG. 35

CSP EMBODIMENT

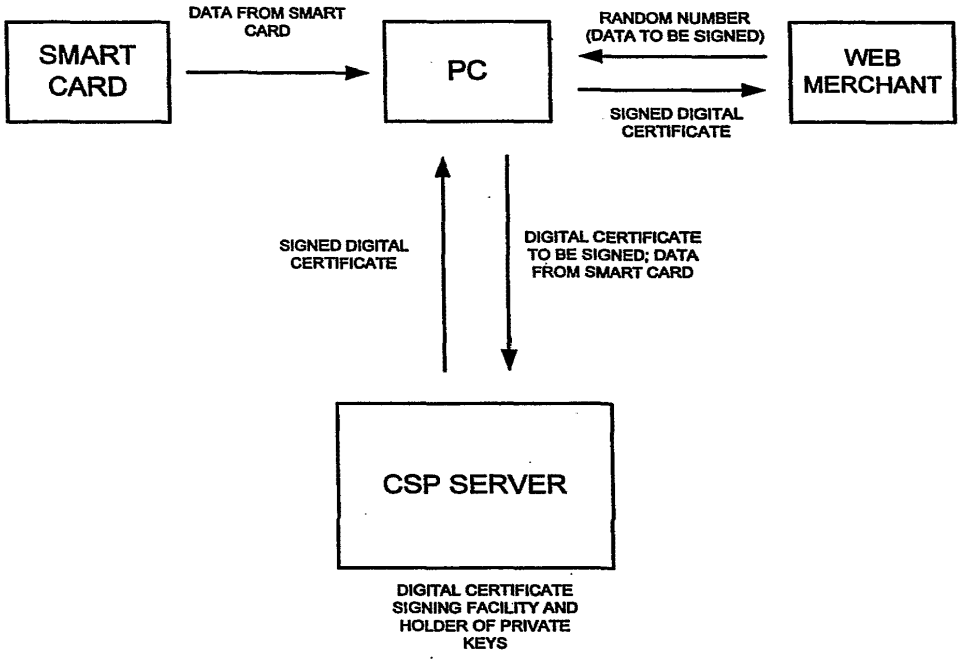


FIG. 36

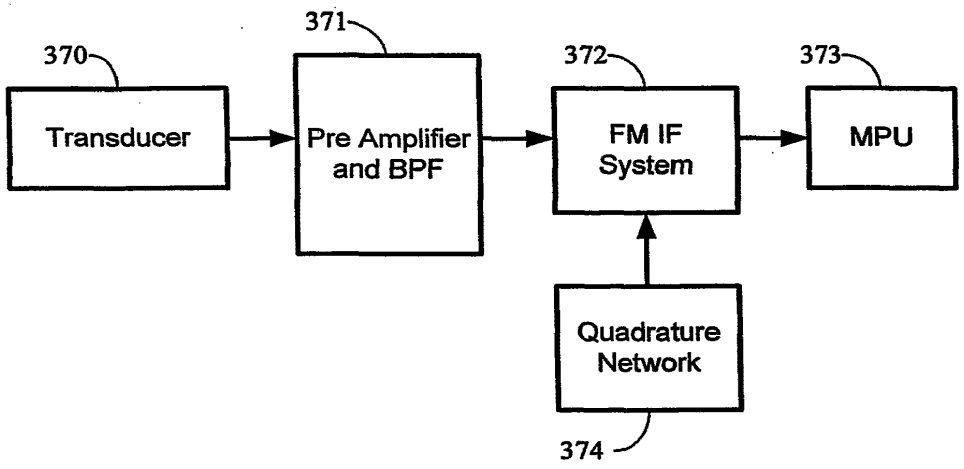

FM IF System for RF Decoding (1)
370
Transducer
371
Pre Amplifier and BPF
372
FM IF System
373
MPU
Quadrature Network
374

FIG. 37

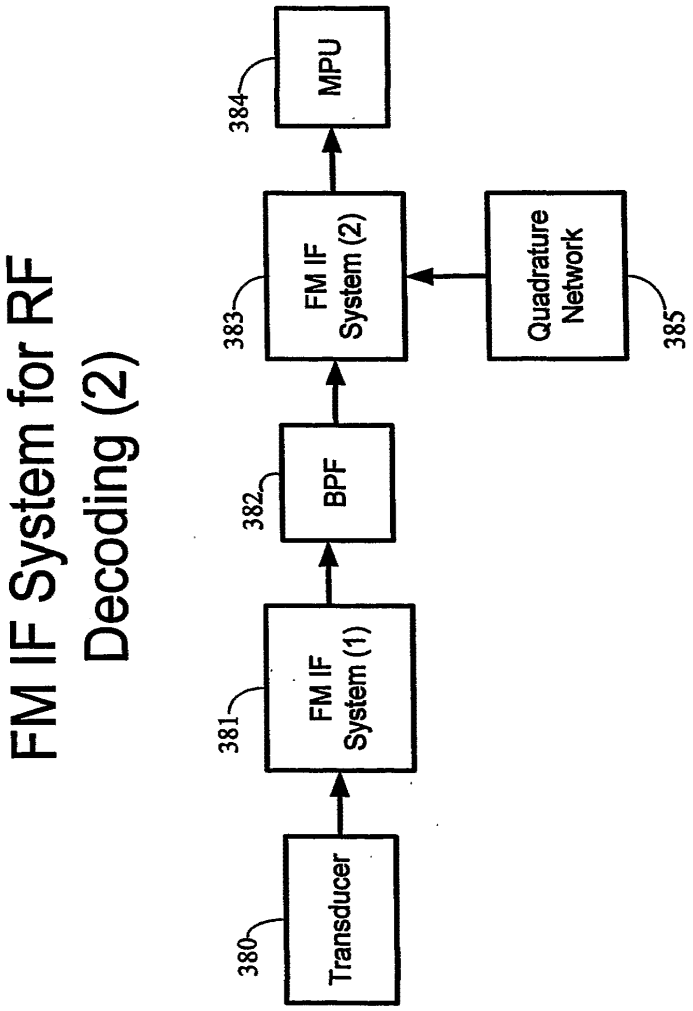

FM IF System for RF Decoding (2)
Transducer
380
FM IF System (1)
381
BPF
382
FM IF System (2)
383
MPU
384
Quadrature Network
385

FIG. 38

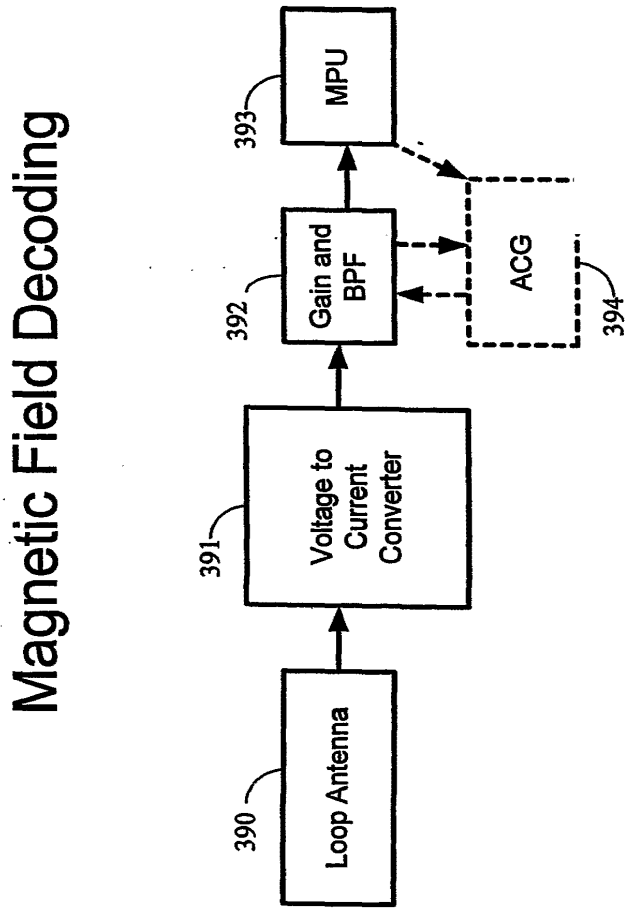

Magnetic Field Decoding
Loop Antenna
390
Voltage to Current Converter
391
Gain and BPF
392
MPU
393
ACG
394

FIG. 39

Using Hardware PLL for Decoding

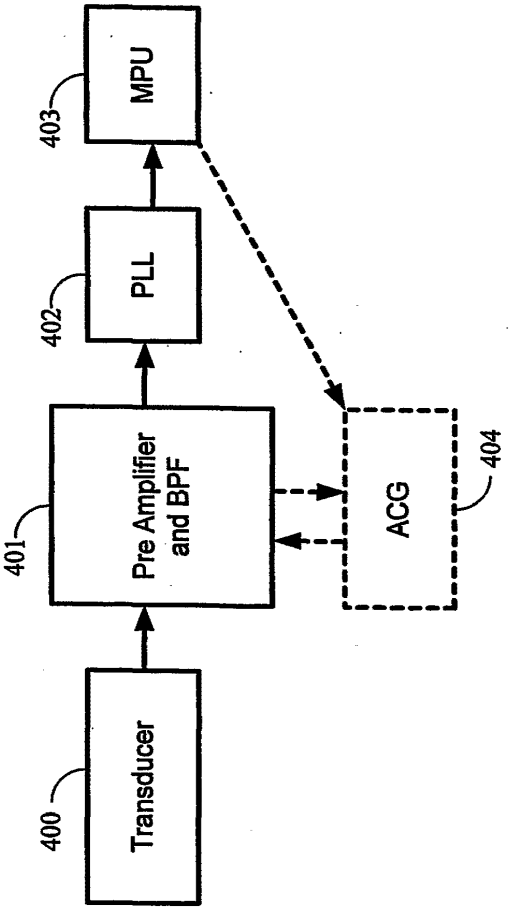


FIG. 40

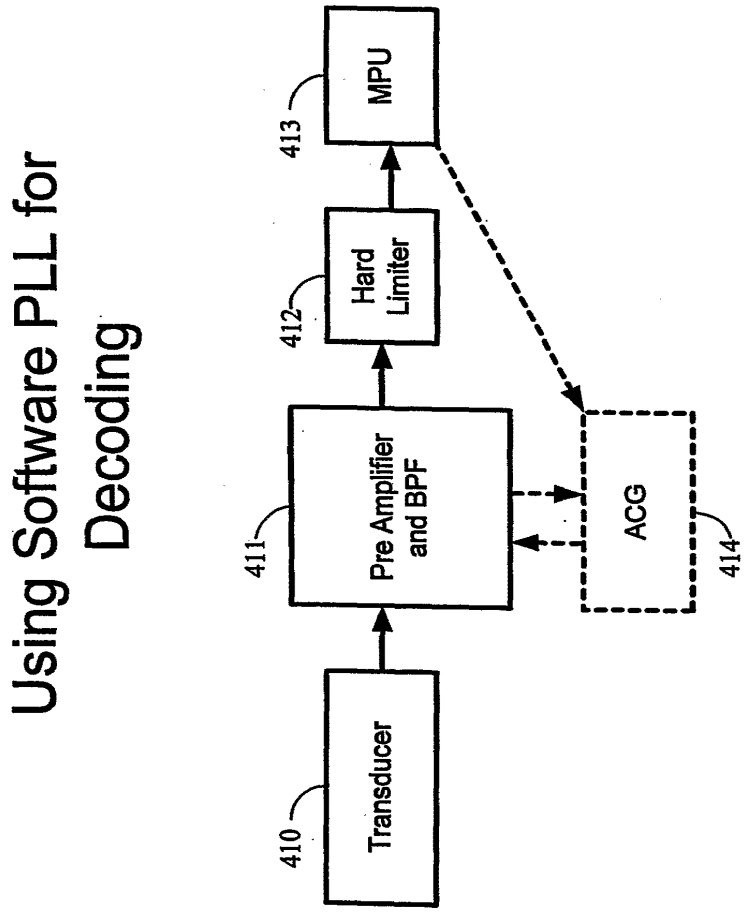

Using Software PLL for Decoding
Transducer
410
Pre Amplifier and BPF
411
Hard Limiter
412
MPU
413
ACG
414

FIG. 41

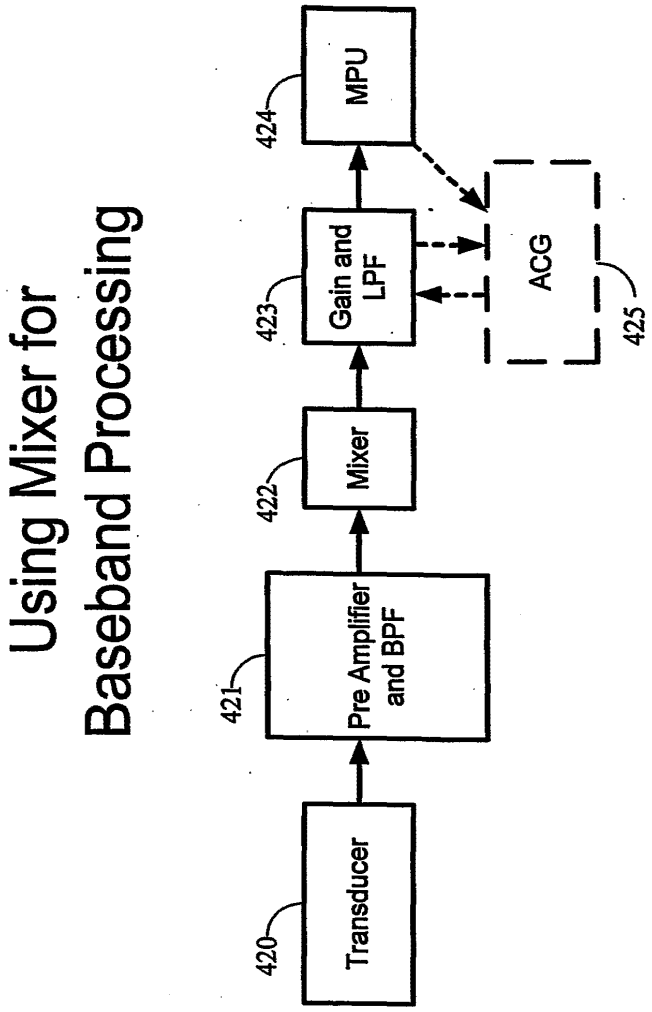

Using Mixer for Baseband Processing
Transducer
420
Pre Amplifier and BPF
421
Mixer
422
Gain and LPF
423
MPU
424
ACG
425

FIG. 42

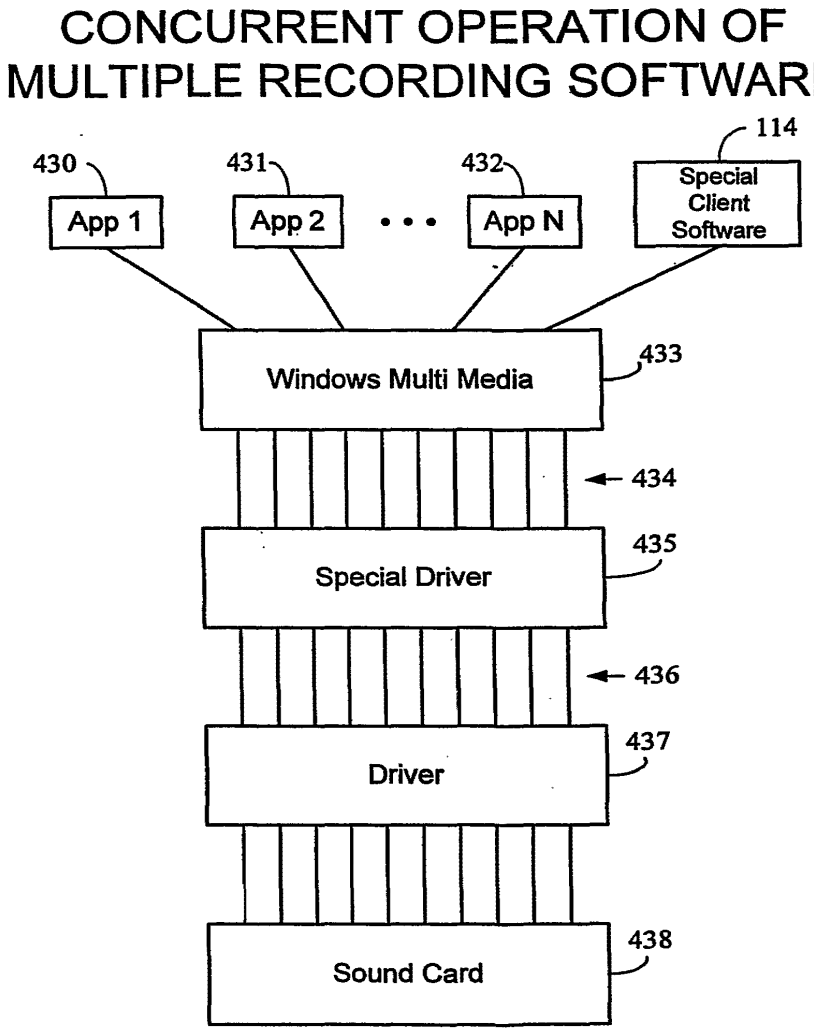

CONCURRENT OPERATION OF MULTIPLE RECORDING SOFTWARE
430
431
432
114
App 1
App 2
App N
Special Client Software
Windows Multi Media
433
434
Special Driver
435
436
Driver
437
Sound Card
438

FIG. 43

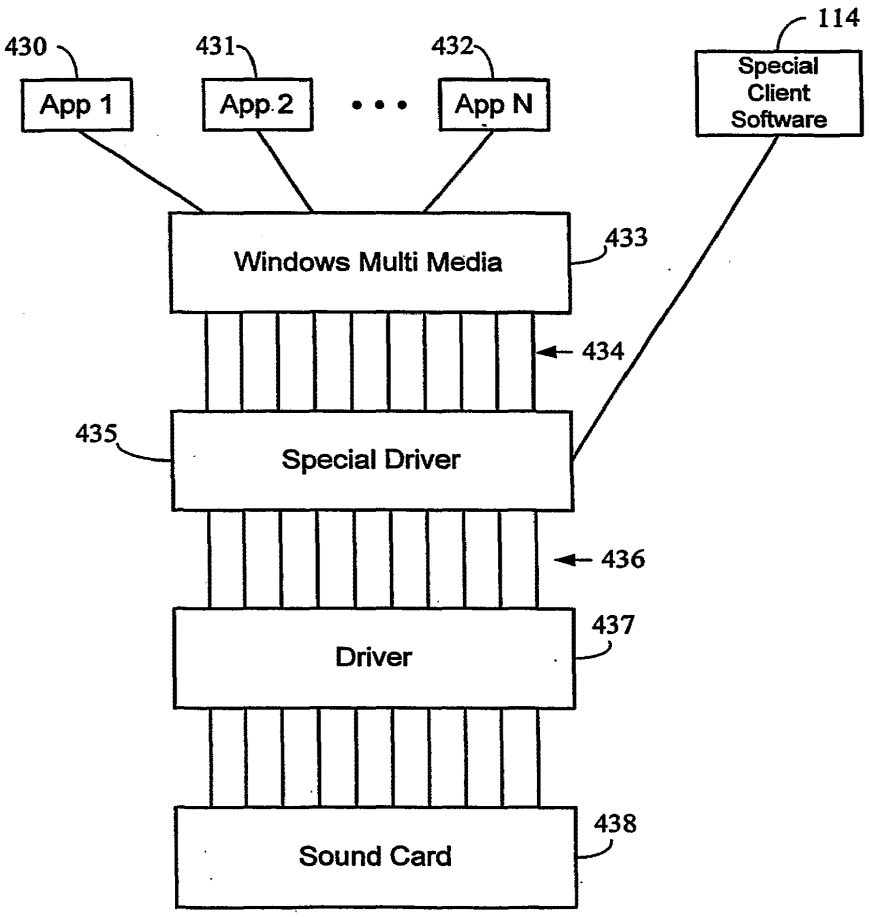

CONCURRENT OPERATION OF MULTIPLE RECORDING SOFTWARE
430
431
432
114
App 1
App 2
App N
Special Client Software
Windows Multi Media
433
434
435
Special Driver
436
437
Driver
438
Sound Card

FIG. 44

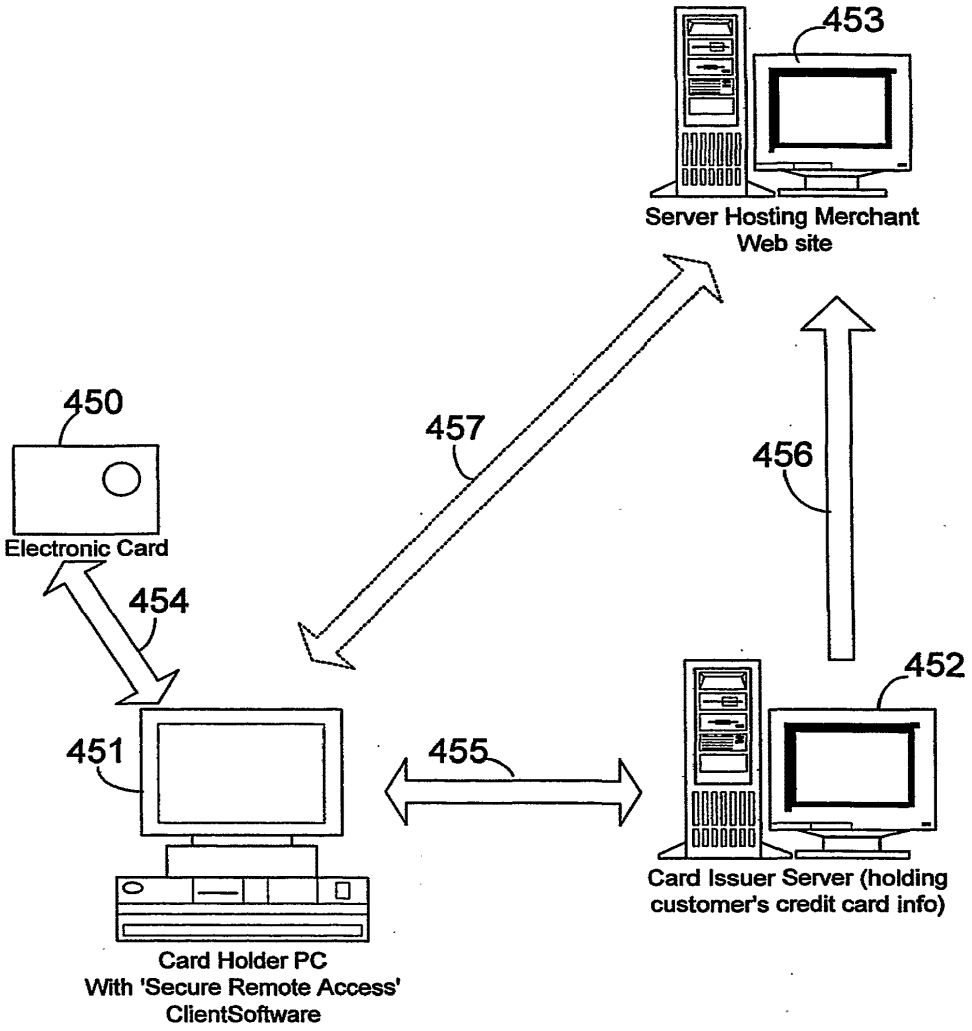

453
Server Hosting Merchant Web site
450
Electronic Card
457
456
454
452
451
455
Card Issuer Server (holding customer's credit card info)
Card Holder PC With 'Secure Remote Access' ClientSoftware

FIG. 45

APPLICATIONS

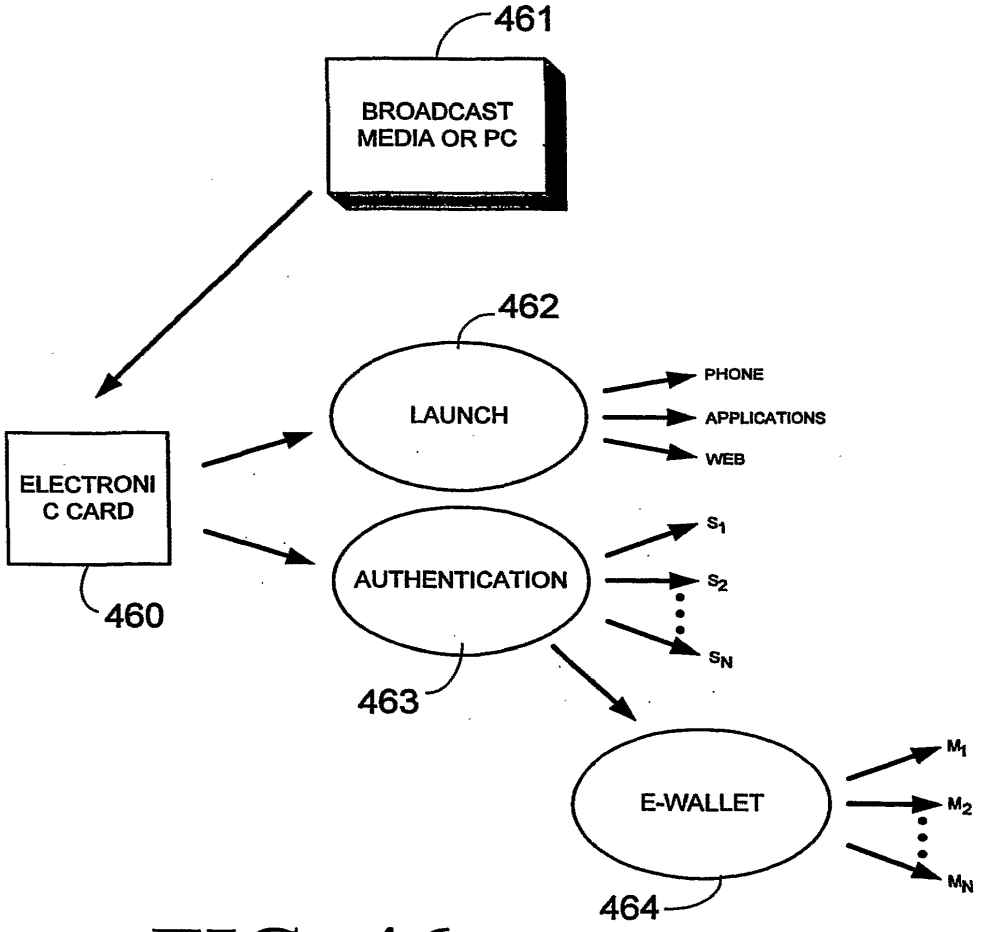


FIG. 46

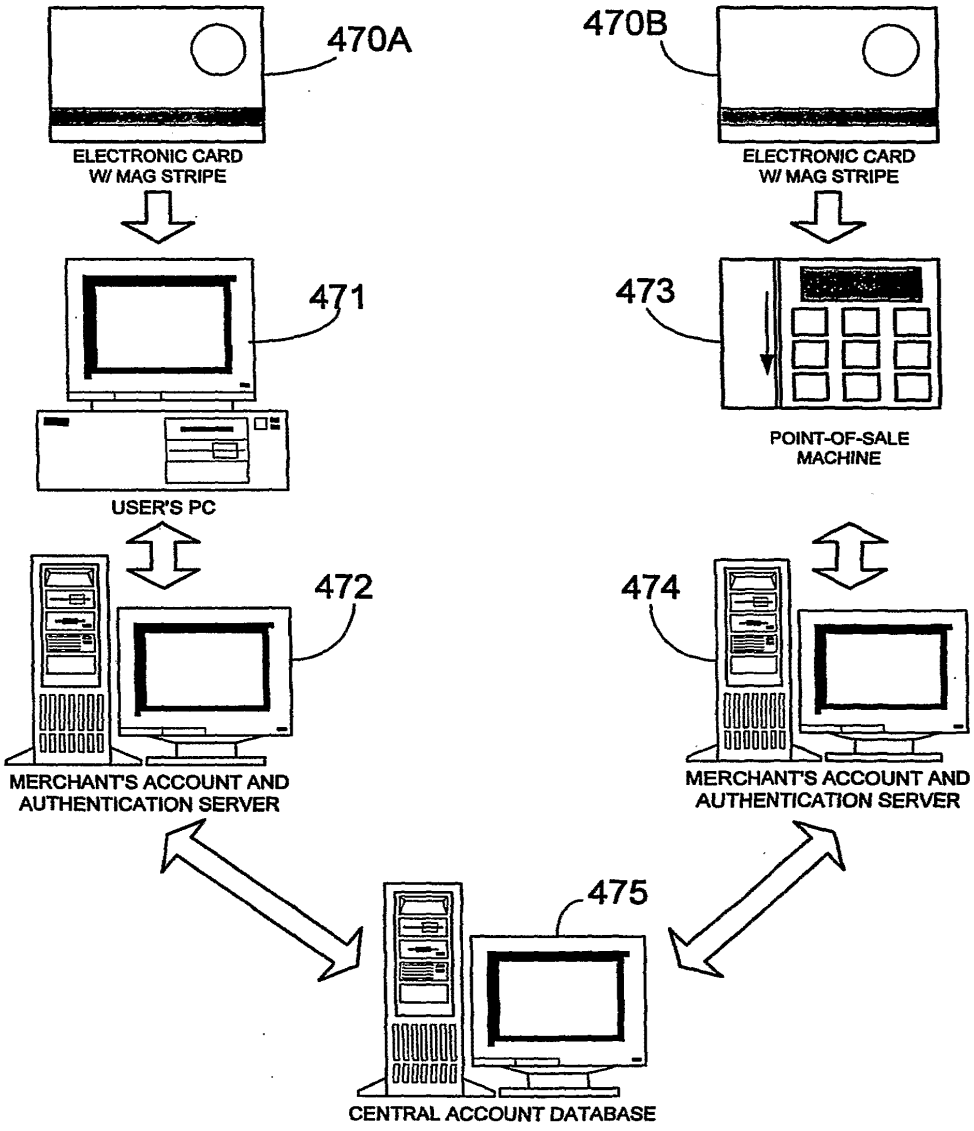

470A
ELECTRONIC CARD
W/ MAG STRIPE
470B
ELECTRONIC CARD
W/ MAG STRIPE
471
USER'S PC
473
POINT-OF-SALE
MACHINE
472
MERCHANT'S ACCOUNT AND
AUTHENTICATION SERVER
474
MERCHANT'S ACCOUNT AND
AUTHENTICATION SERVER
475
CENTRAL ACCOUNT DATABASE

FIG. 47

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2012 (15.11.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/154915 A1

(51) International Patent Classification:
G06Q 40/02 (2012.01)

(21) International Application Number:
PCT/US2012/037237

(22) International Filing Date:
10 May 2012 (10.05.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/484,588	10 May 2011 (10.05.2011)	US
61/484,566	10 May 2011 (10.05.2011)	US
61/484,576	10 May 2011 (10.05.2011)	US
61/484,547	10 May 2011 (10.05.2011)	US

(71) Applicant *(for all designated States except US)*: **DYNAMICS INC.** [US/US]; 493 Nixon Road, Cheswick, PA 15024 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MULLEN, Jeffrey, D.** [US/US]; 731 South Negley Avenue, Apartment #2, Pittsburgh, PA 15232 (US). **RIGATTI, Christopher, J.** [US/US]; 321 Jacksonia Street, Pittsburgh, PA 15212 (US). **WALLACE, Michael, T.** [US/US]; 202 North Trailwood Road, Payson, AZ 15024 (US).

(74) Agent: **WALLACE, Michael, T.**; 493 Nixon Road, Cheswick, PA 15024 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: SYSTEMS, DEVICES, AND METHODS FOR MOBILE PAYMENT ACCEPTANCE, MOBILE AUTHORIZATIONS, MOBILE WALLETS, AND CONTACTLESS COMMUNICATION MECHANISMS

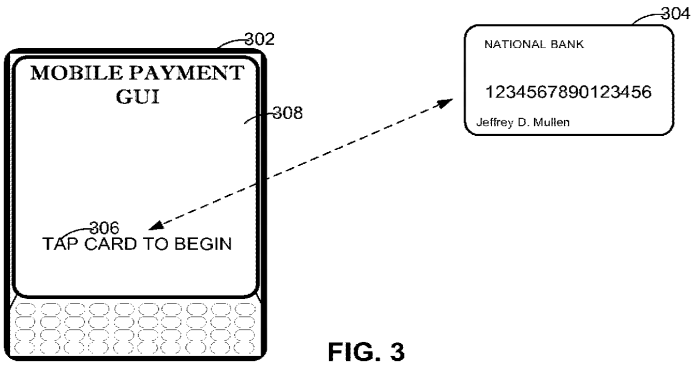


FIG. 3

(57) **Abstract**: A mobile device may provide payment acceptance and/or payment authorization for purchases, payments and/or money transfers by accepting payment information from a powered, or a non-powered, card using a contactless communication channel formed between the card and the mobile device. The payment information may be communicated by the mobile device to network entities that may be used to settle/authorize such purchase, payment and/or money transfer transactions. Physical cards may be presented to a mobile device to establish a contactless communication channel between the physical card and the mobile device. Information communicated by the physical card may be received, stored, and used by the mobile device to generate a mobile wallet of virtual cards.

WO 2012/154915 A1

D/007 PCT

SYSTEMS, DEVICES, AND METHODS FOR MOBILE PAYMENT ACCEPTANCE, MOBILE AUTHORIZATIONS, MOBILE WALLETS, AND CONTACTLESS COMMUNICATION MECHANISMS

Background of the Invention

[0001] This invention relates to mobile devices and related systems.

Summary of the Invention

[0002] A mobile device is provided that may be used as a point-of-sale terminal. A contactless communication channel may, for example, be formed between the mobile device and a payment card to communicate payment information from the payment card to the mobile device. The mobile device may, for example, use the communicated payment information to complete a purchase transaction that may be initiated by the mobile device. Accordingly, for example, no payment information need reside on the mobile terminal to complete a payment transaction. Instead, an application may be remotely activated, or a user of a mobile device may activate an application on the mobile device, that allows the mobile device to accept payment

information directly from a payment card before and/or during a payment transaction.

[0003] A mobile device may, for example, provide a browsing activity where goods and/or services may be located for purchase on a website (e.g., an Amazon or eBay website). An application may, for example, be executed on a mobile device that may communicate with a checkout application running on a website. Payment information may be exchanged directly from a user's payment card to the checkout application using the user's mobile device. In so doing, for example, a mobile device may be used as a contactless payment acceptance terminal.

[0004] A user may be provided an option of storing payment information associated with a payment card within a memory of the mobile device. Accordingly, for example, a mobile device may store payment information associated with one or more payment accounts. In so doing, for example, a mobile device may store multiple payment accounts that may be recalled from a memory of the mobile device at the user's request to complete a payment transaction.

[0005] A mobile device may detect the presence of a card that is brought within a communication distance of a contactless interface of the mobile device. For example, a card having RFID capability may communicate with an RFID device of a mobile device when the card comes within a distance (e.g., up to 2 inches) of the mobile device. Accordingly, for example, a card type (e.g., a powered card or a non-powered card) may be identified by the mobile device.

[0006] A non-powered card may, for example, communicate one, two, and/or three tracks of magnetic

stripe data to a mobile device via a contactless interface of the mobile device. Accordingly, a processor of a mobile device may identify an account type (e.g., credit or debit) that may be associated with the non-powered card by inspection of magnetic stripe data (e.g., account number) received from the non-powered card.

[0007] A powered card may, for example, communicate information (e.g., information within discretionary data fields) to a contactless interface of a mobile device. In so doing, for example, the additional information may be analyzed by a processor of the mobile device to determine that a detected card is a powered card having increased capability. Accordingly, for example, a user of a powered card may select a feature (e.g., pay with credit) on the powered card and a processor of a mobile device may detect that such a feature is selected based upon an analysis of information (e.g., discretionary data) received from the powered card.

[0008] A mobile device may validate a payment card. For example, a mobile device may request entry of a PIN after a payment card is presented to the mobile device and payment information is communicated to the mobile device by the payment card. Once entered, a mobile device may, for example, access a server associated with the payment card's issuing entity to validate the PIN. Alternately, for example, a processor of a mobile device may compare the PIN entry against local memory contents of the mobile device to validate the entered PIN.

[0009] As per another example, a mobile device may validate a payment card by requiring that the physical

payment card be present during a payment transaction. Accordingly, for example, a mobile device may require that a physical payment card be tapped against the mobile device so that a contactless communication channel may be formed between the payment card and the mobile device to verify the identity of the payment card. Accordingly, for example, identifying information communicated by the payment card to the mobile device may be compared against information previously stored within a memory of the mobile device that may be associated with the payment card.

[0010] One or more payment cards may, for example, be presented to a mobile device to complete a purchase transaction. Accordingly, for example, split-payment options may be offered by a mobile device. In so doing, for example, a first payment card may be tapped against a mobile device and accepted by the mobile device as a first form of partial payment, a second payment card may be tapped against a mobile device and accepted by the mobile device as a second form of partial payment, and so on. A mobile device may, for example, allow a user to select an amount for each partial payment and may settle each partial payment amount with each respective issuer of each payment card presented for partial payment.

[0011] A mobile device may provide checkout options to a user. For example, a mobile device may allow a user to associate purchase categories (e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile device so that the user may prepare a more detailed accounting of his or her expenditures. As per another example, a rewards card may be tapped against a mobile device so that rewards card

information may be credited with purchases transacted by the mobile device.

[0012] A mobile device may provide receipt delivery options to a user. For example, a mobile device may allow a user to select one of many receipt delivery options (e.g., text messaging, email or autonomous delivery to accounting software executed by a processor of the mobile device). Other receipt options may be provided by a mobile device in a graphical format (e.g., a barcode) so that proof-of-purchase may be verified by a reader (e.g., a barcode reader).

[0013] Money transfers may, for example, be transacted by a mobile device. One or more payment accounts (e.g., a car account or a utility account) may be selected by a user of a mobile device to receive a payment transacted by the mobile device. Payment information may be recalled from memory and/or entered by a user of the mobile device and then communicated to network entities by the mobile device to complete payment transactions.

[0014] Person to person transfers may, for example, be transacted by a mobile device. A user of a mobile device may, for example, tap a payment card against the mobile device to communicate source account information to the mobile device where funds are to be withdrawn. A person receiving a transfer of funds may, for example, tap his or her payment card against a device (e.g., a mobile device) to communicate target account information where funds are to be deposited. A mobile device may, for example, gather source and target account information and communicate such information to network entities to complete the funds transfer transaction.

[0015] A mobile device may, for example, provide a scanning capability (e.g., via a camera) to scan images (e.g., barcodes) that may be analyzed by a processor of the mobile device. Accordingly, for example, a mobile device may be used to scan product information from a product tag (e.g., a barcode) to select an item for purchase. As items are selected for purchase, scanned information is processed and displayed by the mobile device to produce a summary of items that may be selected for purchase. The mobile device may, for example, collect payment information from a payment card via a contactless communication channel and then use the payment information to complete a purchase transaction for the items scanned by the mobile device.

[0016] A mobile device may access electronic billing information via one or more communication capabilities of the mobile device. A merchant (e.g., a restaurant) may provide access to an electronic tab generated by the merchant (e.g., a bill generated by a restaurant for a dinner for two). Items billed by the merchant may be accessed by a user of a mobile device and displayed by the mobile device to produce a summary of items billed. The mobile device may, for example, collect payment information from a payment card via a contactless communication channel and then use the payment information to complete a purchase transaction for the billed items.

[0017] Any mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may be a point-of-sale terminal. Accordingly, for example, a mobile device may accept payment information from any payment card, communicate such payment

information via a network, complete a settlement process with network entities (e.g., an issuer or a payment server) on such a network, and provide results (e.g., an electronic receipt) of the completed purchase transaction to a user of the mobile device.

[0018] A mobile device may include a contactless communication device. Accordingly, for example, a mobile device may communicate with any card having contactless communication capability. For example, a card (e.g., a non-powered card) may include a near-field communication device (e.g., an RFID tag) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. In so doing, for example, a non-powered card may communicate one, two, and/or three tracks of magnetic stripe information to a mobile device before and/or during a purchase transaction conducted by the mobile device.

[0019] A card (e.g., a powered card) may include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device. A powered card may, for example, include a battery, a processor, memory, and a manual input interface (e.g., one or more buttons) that may allow a user of the powered card to programmably communicate information to a mobile device. For example, a powered payment card may include a feature associated with a button that allows a user to, for example, pay with credit or pay with debit. Accordingly, for example, a powered payment card may communicate such a payment selection within discretionary data fields of one or more tracks of magnetic stripe data.

[0020] A powered card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the powered card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device and processed by a processor of the mobile device as data communicated by the powered card.

[0021] A powered card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the powered card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a powered card as data communicated by a mobile device.

[0022] A powered card may, for example, include a light source (e.g., an LED) to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the powered card. A powered card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the powered card through a contactless communication channel. A mobile

device may, for example, include sound emission capabilities that may be detected by a microphone of a powered card as data communicated by the mobile device through a contactless communication channel.

[0023] A user may communicate information directly from a card to a memory location of a mobile device via a contactless communication channel between the card and the mobile device. Accordingly, for example, a mobile device may store information (e.g., payment information) associated with one or more cards (e.g., one or more payment cards) that have been presented within a proximity to the mobile device. In so doing, for example, a mobile device may be a mobile wallet having multiple accounts (e.g., payment, identification, and travel accounts) stored within a memory of the mobile wallet where each account may be recalled from a memory of the mobile wallet at the user's request to perform a function (e.g., to complete a payment transaction).

[0024] A mobile device may detect the presence of a card that is brought within a communication distance of a contactless interface of the mobile device. A card may, for example, provide RFID capability that may communicate with an RFID device of a mobile device when the card comes within a communication distance of the mobile device. Accordingly, for example, a card type may be identified by the mobile device and information associated with the card type may be communicated from the card to the mobile device. Information received by the mobile device from the card may be autonomously categorized by the mobile device in accordance with a card type and the information may be stored and

displayed to a user in accordance with the categorization.

[0025] A card (e.g., a non-powered payment card) may, for example, communicate one, two, and/or three tracks of magnetic stripe data to a mobile device via a contactless interface. Accordingly, for example, a processor of a mobile device may identify a card type (e.g., a payment card) by analyzing the magnetic stripe data received from the card. A processor of a mobile device may, for example, determine an account type (e.g., credit or debit) that may be associated with the non-powered payment card by inspection of magnetic stripe data (e.g., account number) received from the non-powered card.

[0026] A powered card may, for example, communicate information to a contactless interface of a mobile device. In so doing, for example, additional information (e.g., information presented in discretionary data) may be identified by a processor of the mobile device to determine that a detected card is a powered card having increased capability. Accordingly, for example, a user of a powered card may select a feature (e.g., pay with credit) on the powered card and a processor of a mobile device may detect that such a feature is selected based upon an analysis of the information received from the powered card.

[0027] A mobile device may, for example, validate a payment card. For example, a mobile device may request entry of a PIN after a payment card is presented to the mobile device. Once a PIN is entered, a mobile device may, for example, access a server associated with the issuing entity to validate the PIN. A processor of a mobile device may, for example, compare the PIN entry

against memory contents of the mobile device to locally validate the entered PIN.

[0028] Data received from a card may, for example, be encrypted. Accordingly, for example, data received from a card may be stored in an encrypted state and decrypted upon receipt of a decryption key. A decryption key may, for example, be received from a sponsoring entity of the card (e.g., a card issuer's server). Decrypted data may, for example, be destroyed such that each usage of encrypted data may require a decryption key prior to usage. Alternately, for example, decrypted data may be stored within a protected memory of the mobile device and kept for future use.

[0029] A user of a mobile device may, for example, extract physical, or real, cards (e.g., payment, identification, travel, and rewards cards) from the user's physical wallet or purse and may convert each physical card into a virtual equivalent card that resides electronically within the mobile device. Accordingly, for example, each physical card (e.g., a powered card or a non-powered card) may be brought within a proximate, or touching, relationship with a mobile device to create a contactless communication channel. Card information (e.g., cardholder data, card data, and card configuration data) may, for example, be communicated by the card to the mobile device via such a contactless communication channel. In so doing, for example, a virtual card may be created within the mobile device that is both visibly and functionally equivalent to its physical counterpart.

[0030] A non-powered card may, for example, be virtually rendered onto a display of a mobile device in

a manner that resembles its physical counterpart. Card and cardholder information may, for example, be communicated by the non-powered card to the mobile device and rendered onto a virtual card that may be displayed by a processor of the mobile device. Accordingly, for example, the functionality of the physical card (e.g., a non-powered payment card) may be imparted to the virtual card by the mobile device when the mobile device communicates information (e.g., payment information) that may be associated with the non-powered payment card. As per one example, a mobile device may communicate payment information associated with a virtual card that may be displayed on a GUI of the mobile device when the mobile device is brought within a communication distance of a merchant terminal to complete a purchase transaction (e.g., an RFID device of the mobile device may communicate with an RFID device of a merchant terminal to exchange payment information between the mobile device and the merchant terminal to complete the purchase transaction). As per another example, a mobile device may communicate payment information associated with a virtual card when the mobile device accesses a network entity (e.g., a payment server) via a wireless network (e.g., a cellular network or a Wi-Fi hotspot) to complete a purchase transaction using the communicated payment information.

[0031] A powered card may, for example, be virtually rendered onto a display of a mobile device in a manner that resembles its physical counterpart. A powered card may, for example, be virtually rendered onto a display of a mobile device in a manner that provides user interface functionality that may be associated

with the physical counterpart. A powered card may, for example, communicate configuration information (e.g., button placement and associated functionality, display placement and associated functionality and input/output functionality) to a processor of a mobile device and the processor may render such a configuration onto a virtual card such that the configuration of the virtual card provides substantially identical functionality as compared to its physical counterpart.

[0032] As per one example, a powered card (e.g., a powered payment card) may include one or more buttons that when activated determine a method of payment to be used to complete a transaction (e.g., pressing one button may invoke a credit payment transaction while pressing another button may invoke a debit payment transaction). Accordingly, for example, a virtual card may be rendered onto a display of a mobile device that includes the same functionality, such that when one virtual button is touched on the virtual card, a credit payment message is communicated by the mobile device and when another virtual button is touched on the virtual card, a debit payment message is communicated by the mobile device.

[0033] As per another example, a powered card may be programmed for a particular feature by pressing a button on the powered card associated with that feature. Accordingly, for example, a powered card may communicate information associated with a selected feature to a mobile device and a processor of the mobile device may render a virtual card on a GUI of the mobile device in accordance with the selected feature. In so doing, for example, a powered card may be selected as a powered payment card with a debit feature

and the selected feature may be communicated to a mobile device (e.g., the debit feature may be communicated to a mobile device within a discretionary data field of a magnetic stripe message). The resulting virtual payment card rendered onto a display of the mobile device may, for example, provide a virtual payment card having a fixed payment feature (e.g., a fixed debit payment feature).

[0034] A mobile device may, for example, challenge a user of the mobile device to enter a password (e.g., a PIN) that may be associated with a card. A mobile device may, for example, require a password before a virtual card may be created and stored within the mobile device. A mobile device may, for example, allow a virtual card to be created and stored within a mobile device, but may challenge a user of the mobile device to enter a password associated with the virtual card before it can be recalled from a memory of the mobile device and used (e.g., used to complete a purchase transaction).

[0035] A user may, for example, participate in the personalization of a virtual card that may be stored within a memory of a mobile device. A mobile device may, for example, store various logos (e.g., issuer logos, network brand logos, and merchant logos) within a memory of the mobile device and may allow a user of the mobile device to use a GUI of the mobile device to personalize an appearance of a virtual card with such logos. Accordingly, for example, a user may perform drag-and-drop operations, alphanumeric entry operations, and any other operation to personalize an appearance of a virtual card stored within a memory of the mobile device.

[0036] A processor of a mobile device may, for example, organize two or more virtual cards for display on a GUI of the mobile device. A mobile device may, for example, keep track of a number of usages of one or more virtual cards and may sort such virtual cards within a list of displayed virtual cards so that a user may easily access his or her most used virtual card from a top of the displayed list. A mobile device may, for example, track a location of a user of the mobile device and organize a list of virtual cards in accordance with such a location. Accordingly, for example, a user may be shopping within a general merchandise store (e.g., Target), a processor of the user's mobile device may track the user's position to the Target store and the processor of the user's mobile device may display a virtual card (e.g., a Target gift card) at the top of a displayed list of virtual cards based upon the user's location. In so doing, for example, a virtual card most pertinent to the user's location may be sorted to the top of a displayed list of virtual cards for easy and convenient access by the user.

[0037] A user may, for example, select one virtual card from a list of virtual cards presented by a GUI of a mobile device and may perform one of many operations on the selected virtual card. A user may, for example, conduct a purchase transaction using a virtual payment card selected from a list of virtual cards. Accordingly, for example, a user may place a mobile device within a vicinity of a merchant terminal and may communicate payment information associated with a selected payment card to the merchant terminal. As per another example, payment information associated with a

selected virtual card may be communicated to a network entity (e.g., a payment server or an issuer's server) by the mobile device to complete a purchase transaction.

[0038] A mobile device may, for example, receive an electronic receipt for the purchase transaction either via a communication channel established between the mobile device and the merchant terminal or via other communication channels (e.g., text messaging or email exchange with a network entity such as a payment server). A user may, for example, view documents (e.g., receipts or bank statements) that may be associated with a virtual card. Accordingly, for example, a mobile device may collect and store documents associated with a virtual payment card and may display the associated documents upon request from the user. A GUI of a mobile device may, for example, allow a user to annotate documents that may be associated with a virtual card (e.g., a user may make a note that may be electronically attached to an electronic receipt that may be associated with a virtual payment card).

[0039] Other cards (e.g., other virtual cards) may be associated with a selected virtual card and those associations may be viewed from a GUI of the mobile device. For example, a payment card may be associated with a rewards card, such that in response to a request from a user of a mobile device, a processor of the mobile device may display the associations to the payment card and may use the associated virtual cards in support of a purchase transaction (e.g., the associated rewards card may be used during a payment transaction conducted with the selected virtual payment

card so that the rewards account may accrue rewards points for the purchase transaction).

[0040] A mobile device may, for example, allow a user of the mobile device to cancel an account that may be associated with a virtual card stored within the mobile device. Accordingly, for example, a virtual payment card may be stored within a mobile device and may be associated with a payment account that is administered by an issuing entity of the payment account. A mobile device may, for example, communicate with such an issuing entity to cancel a payment account that may be associated with a virtual payment card stored within the mobile device. A mobile device may, for example, negotiate with other issuing entities to determine when new payment card offers may be available and to allow a user of the mobile device to accept such payment card offers. Once accepted, a user of a mobile device may conduct other transactions with the newly accepted payment card offers (e.g., account balance(s) associated with existing virtual cards may be transferred to the newly accepted payment card via a request made by the mobile device and an issuing server).

[0041] Any mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may be a mobile wallet. Accordingly, for example, a mobile device may accept payment and other information from any payment card, store and display such information as a virtual card on a GUI of the mobile device, communicate such payment information via a wired and/or a wireless network, complete a settlement process with network entities (e.g., an

issuer or a payment server) on such a network, and provide results (e.g., an electronic receipt) of the completed purchase transaction to a display of the mobile device.

[0042] A mobile device may include a contactless communication device. Accordingly, for example, a mobile device may communicate with any card having contactless communication capability. For example, a card (e.g., a non-powered card) may include a near-field communication device (e.g., an RFID tag) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. In so doing, for example, a non-powered card may communicate one, two, and/or three tracks of magnetic stripe information to a mobile device before and/or during a purchase transaction conducted by the mobile device.

[0043] A card (e.g., a powered card) may include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device. A powered card may, for example, include a battery, a processor, memory, and a manual input interface (e.g., one or more buttons) that may allow a user of the powered card to programmably communicate information to a mobile device. For example, a powered payment card may include a feature associated with a button that allows a user to, for example, pay with credit or pay with debit. Accordingly, for example, a powered payment card may communicate such a payment selection within discretionary data fields of one or more tracks of magnetic stripe data.

[0044] A powered card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the powered card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device and processed by a processor of the mobile device as data communicated by the powered card.

[0045] A powered card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the powered card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a powered card as data communicated by a mobile device.

[0046] A powered card may, for example, include a light source (e.g., an LED) to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the powered card. A powered card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the powered card through a contactless communication channel. A mobile

device may, for example, include sound emission capabilities that may be detected by a microphone of a powered card as data communicated by the mobile device through a contactless communication channel.

[0047] A mobile device may be used as an authorization terminal to conduct transactions (e.g., purchase transactions) using the mobile device. Purchase transactions may, for example, be completed by a mobile device using payment information stored within a memory of the mobile device. In order to conduct a purchase transaction, a processor of a mobile device may, for example, first require security credentials to authorize a purchase transaction. Security credentials may, for example, be any type of information that may be communicated to a mobile device by a contactless device using a contactless communication channel (e.g., an RFID communication channel).

[0048] Security credentials may, for example, be payment information that may be communicated to a processor of a mobile device by a payment card (e.g., a powered or a non-powered payment card). Accordingly, for example, if payment information communicated to a processor of a mobile device by a physical payment card matches payment information previously stored within a memory of the mobile device, the mobile device may authorize the purchase transaction.

[0049] As per an example, a mobile device may receive payment information (e.g., a payment account number and an expiration date) from a payment card via a contactless communication channel and may store such payment information within a memory of the mobile device for future use. Prior to conducting a requested purchase transaction, a processor of a mobile device

may first require that a physical payment card be used to authorize the purchase transaction. Accordingly, for example, the same physical payment card that was used to originally communicate payment information to a processor of the mobile device may be required to once again communicate payment information in order to authorize the purchase transaction. Upon verification that the newly communicated payment information matches at least a portion of payment information contained within a memory of the mobile device, the mobile device may authorize the payment transaction.

[0050] A powered card may, for example, communicate security credentials that may contain a dynamic security code and other information (e.g., at least a portion of a payment account number or a cardholder's name). Accordingly, for example, an application executed by a processor of a mobile device may synchronize with a dynamic security code generation algorithm that may be executed by a processor of the powered card. In so doing, for example, a processor of the mobile device may generate a dynamic security code in accordance with the security code generation algorithm and may compare the generated dynamic security code to a security code received from a powered card during authorization of a purchase transaction. If a match exists, for example, the purchase transaction may be authorized by the mobile device.

[0051] A mobile device may, for example, communicate security credentials received from a physical card via a contactless communication channel to a network entity (e.g., an authorization server). Accordingly, for example, the authorization server may analyze the

received security credentials and may either confirm or deny that the security credentials are authentic. A message may, for example, be communicated from the authorization server to the mobile device to either authorize or deny the purchase transaction.

[0052] A mobile device may, for example, arrange security credentials (e.g., payment information) stored within a memory of the mobile device as one or more virtual payment cards that may be provided on a display of the mobile device. Accordingly, for example, a user of a mobile device may select one or more virtual cards from a displayed list of virtual cards for use during a purchase transaction. In so doing, for example, a user may retrieve a physical payment card from his or her wallet that corresponds to the virtual payment card selected for use and may communicate (e.g., via a contactless communication channel) payment information from the physical payment card to a processor of the mobile device. Upon verification that the communicated payment information matches at least a portion of payment information stored within a memory of the mobile device, a processor of the mobile device may authorize the purchase transaction using the stored payment information.

[0053] A physical payment card may, for example, be used as a master physical payment card to authorize purchase transactions that are to be completed by the mobile device using stored payment information that does not match payment information received from the physical payment card. For example, a master physical payment card may be associated with a particular issuer and a mobile device may store several virtual cards within a memory of the mobile device having the same

issuer. Upon receipt of payment information from the master physical payment card, a processor of a mobile device may authorize purchase transactions using one or more virtual cards stored within a memory of the mobile device that may share the same issuer as the issuer of the master physical payment card.

[0054] Other devices (e.g., RFID enabled keys) may, for example, communicate security credentials via a contactless communication channel to a processor of a mobile device to authorize other transactions (e.g., non-purchase transactions) that may be conducted by the mobile device. Accordingly, for example, a processor of a mobile device may communicate commands to a wireless device (e.g., a user's car) to perform certain functions (e.g., start the engine of the user's car). In so doing, for example, a user may present an ignition key to the mobile device to communicate security credentials (e.g., a key code matched to the user's car) from the ignition key to the mobile device to authorize the requested function. Upon verification that the key code matches the key code of the user's car, for example, a processor of the mobile device may authorize the requested function and may communicate the associated command to the user's car to execute the requested function.

[0055] Any function may, for example, be authorized to be performed by a processor of a mobile device. Accordingly, for example, any decision to perform a function by a mobile device may be authorized by a processor of the mobile device. In so doing, for example, any function (e.g., checking a balance of a banking account or transitioning from paper bank statements to e-statements) that may be performed by a

processor of a mobile device may be authorized by the processor upon verification that security credentials (e.g., a bank account number) communicated to the processor from a contactless communication device (e.g., a bank card associated with the bank account) matches at least a portion of security credentials (e.g., banking information) that may be stored within a memory of the mobile device.

[0056] Any mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may be an authorization terminal. Accordingly, for example, any mobile device may accept payment information from any physical payment card, store such payment information within a memory of the mobile device, require that the same (or associated) physical payment card communicate payment information to a processor of the mobile device, and complete a purchase transaction with network entities (e.g., an issuer or a payment server) upon verification that the communicated payment information matches at least a portion of payment information stored within a memory of the mobile device.

[0057] A mobile device may include a contactless communication device. Accordingly, for example, a mobile device may communicate with any card having contactless communication capability. For example, a card (e.g., a non-powered card) may include a near-field communication device (e.g., an RFID tag) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. In so doing, for example, a non-powered card may communicate one,

two, and/or three tracks of magnetic stripe information to a processor of a mobile device before and/or during a purchase transaction conducted by the mobile device.

[0058] A card (e.g., a powered card) may include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device. A powered card may, for example, include a battery, a processor, memory, and a manual input interface (e.g., one or more buttons) that may allow a user of the powered card to programmably communicate information to a mobile device. For example, a powered payment card may include a feature associated with a button that allows a user to, for example, pay with credit or pay with debit. Accordingly, for example, a powered payment card may communicate such a payment selection within discretionary data fields of one or more tracks of magnetic stripe data.

[0059] A powered card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the powered card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device and processed by a processor of the mobile device as data communicated by the powered card.

[0060] A powered card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a

display of a mobile device and information may be communicated from the mobile device to the powered card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a powered card as data communicated by a mobile device.

[0061] A powered card may, for example, include a light source (e.g., an LED) to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the powered card. A powered card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the powered card through a contactless communication channel. A mobile device may, for example, include sound emission capabilities that may be detected by a microphone of a powered card as data communicated by the mobile device through a contactless communication channel.

[0062] A card may include a dynamic magnetic communications device, which may take the form of a magnetic encoder or a magnetic emulator. A magnetic encoder, for example, may be utilized to modify information that is located on a magnetic medium, such that a magnetic stripe reader may then be utilized to read the modified magnetic information from the magnetic medium. A magnetic emulator, for example, may be provided to generate electromagnetic fields that directly communicate data to a read-head of a magnetic stripe reader. A magnetic emulator, for example, may

communicate data serially to a read-head of the magnetic stripe reader. A magnetic emulator, for example, may communicate data in parallel to a read-head of the magnetic stripe reader.

[0063] All, or substantially all, of the front surface, as well as the rear surface, of a card may be implemented as a display (e.g., bi-stable, non bi-stable, LCD, or electrochromic display). Electrodes of a display may be coupled to one or more touch sensors, such that a display may be sensitive to touch (e.g., using a finger or a pointing device) and may be further sensitive to a location of the touch. The display may be sensitive, for example, to objects that come within a proximity of the display without actually touching the display.

[0064] A dynamic magnetic stripe communications device may be implemented on a multiple layer board (e.g., a two-layer flexible printed circuit board). A coil for each track of information that is to be communicated by the dynamic magnetic stripe communications device may then be provided by including wire segments on each layer and interconnecting the wire segments through layer interconnections to create a coil. For example, a dynamic magnetic stripe communications device may include two coils such that two tracks of information may be communicated to two different read-heads included in a read-head housing of a magnetic stripe reader. A dynamic magnetic communications device may include, for example, three coils such that three tracks of information may be communicated to three different read-heads included in a read-head housing of a magnetic stripe reader.

[0065] Input and/or output devices may be included on a card, for example, to facilitate data exchange with the card. For example, an integrated circuit (IC) may be included on a card and exposed from the surface of the card. Such a chip (e.g., an EMV chip) may communicate information to a chip reader (e.g., an EMV chip reader). A contactless device (e.g., one or more RFID antennas and one or more associated RFID chips) may be included in a card, for example, to exchange information with an RFID device.

[0066] One or more detectors may be provided in a card, for example, to sense the presence of an external object, such as a person or device, which in turn, may trigger the initiation of a communication sequence with the external object. The sensed presence of the external object may then be communicated to a processor of the card, which in turn may direct the exchange of information between a card and the external object. Accordingly, timing aspects of the information exchange between an external object and the various I/O devices provided on a card may also be determined by circuitry (e.g., a processor) provided on a card.

[0067] The sensed presence of the external object or device may include the type of object or device that is detected and, therefore, may then determine the type of communication that is to be used with the detected object or device. For example, a detected object may include a determination that the object is a read-head housing of a magnetic stripe reader. Such an identifying detection, for example, may activate a dynamic magnetic stripe communications device so that information may be communicated to the read-head of the magnetic stripe reader. Information may be

communicated by a dynamic magnetic stripe communications device, for example, by re-writing magnetic information on a magnetic medium that is able to be read by a magnetic stripe reader or electromagnetically communicating data to the magnetic stripe reader.

[0068] As per another example, a detected object may include a determination that the object is an RFID enabled device. Such an identifying detection, for example, may cause RFID data to be communicated by a processor of a card to an RFID chip of a card. The RFID data may be temporarily contained within the RFID chip until the RFID data is communicated to a detected RFID device by an RFID antenna on the card. The RFID data may, for example, be erased from the RFID chip after being communicated to the RFID device.

[0069] A card may, for example, be an assembly of multiple printed circuit boards, electronics, one or more RFID antennas, and one or more associated RFID chips. An RFID antenna may, for example, be fabricated on one printed circuit board and an associated RFID chip may, for example, be attached to a separate printed circuit board. Communications (e.g., RFID data transfer between the RFID chip and the RFID antenna) may, for example, be transferred between separate printed circuit boards via conductive paths established between the separate printed circuit boards. An RFID antenna and an associated RFID chip may, for example, reside on the same printed circuit board so as to reduce a number of conductive traces that may be required between separate printed circuit boards.

[0070] A card assembly may, for example, be laminated such that all printed circuit boards,

electronic circuitry and components are covered in a polymer. For example, an electronics package may be provided between two layers of polymer and a liquid polymer may be introduced between these layers and hardened to form a card. A laminated card assembly may, for example, be devoid of electrical contacts on either surface of the laminated card. A laminated card assembly may, for example, provide electrical contacts (e.g., EMV chip contacts) on one or more surfaces of a laminated card assembly.

[0071] A mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may include one or more RFID antennas and associated RFID chips. Accordingly, for example, any mobile device may establish an RFID communication channel with any other RFID enabled device (e.g., an RFID enabled card). A computing device, such as a desktop computer, may be an RFID enabled device. Accordingly, for example, any RFID enabled device (e.g., an RFID enabled card or an RFID enabled mobile device) may establish an RFID communication channel with any RFID enabled computing device.

Brief Description of the Drawings

[0072] The principles and advantages of the present invention can be more clearly understood from the following detailed description considered in conjunction with the following drawings, in which the same reference numerals denote the same structural elements throughout, and in which:

[0073] FIG. 1 is an illustration of a mobile devices constructed in accordance with the principles of the present invention;

[0074] FIG. 2 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0075] FIG. 3 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0076] FIG. 4 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0077] FIG. 5 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0078] FIG. 6 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0079] FIG. 7 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0080] FIG. 8 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0081] FIG. 9 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0082] FIG. 10 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0083] FIG. 11 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0084] FIG. 12 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0085] FIG. 13 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0086] FIG. 14 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0087] FIG. 15 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0088] FIG. 16 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0089] FIG. 17 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0090] FIG. 18 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0091] FIG. 19 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0092] FIG. 20 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0093] FIG. 21 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0094] FIG. 22 is an illustration of a mobile funds transfer system constructed in accordance with the principles of the present invention;

[0095] FIG. 23 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0096] FIG. 24 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0097] FIG. 25 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0098] FIG. 26 is a flow chart of processes constructed in accordance with the principles of the present invention;

[0099] FIG. 27 is an illustration of a mobile devices constructed in accordance with the principles of the present invention;

[0100] FIG. 28 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0101] FIG. 29 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0102] FIG. 30 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0103] FIG. 31 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0104] FIG. 32 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0105] FIG. 33 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0106] FIG. 34 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0107] FIG. 35 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0108] FIG. 36 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0109] FIG. 37 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0110] FIG. 38 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0111] FIG. 39 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0112] FIG. 40 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0113] FIG. 41 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0114] FIG. 42 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0115] FIG. 43 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0116] FIG. 44 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0117] FIG. 45 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0118] FIG. 46 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0119] FIG. 47 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0120] FIG. 48 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0121] FIG. 49 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0122] FIG. 50 is an illustration of a mobile application constructed in accordance with the principles of the present invention;

[0123] FIG. 51 is a flow chart of processes constructed in accordance with the principles of the present invention;

[0124] FIG. 52 is an illustration of mobile devices constructed in accordance with the principles of the present invention;

[0125] FIG. 53 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0126] FIG. 54 is an illustration of a mobile authorization system constructed in accordance with the principles of the present invention;

[0127] FIG. 55 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0128] FIG. 56 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0129] FIG. 57 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0130] FIG. 58 is an illustration of a mobile authorization system constructed in accordance with the principles of the present invention;

[0131] FIG. 59 is an illustration of a mobile authorization system constructed in accordance with the principles of the present invention;

[0132] FIG. 60 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0133] FIG. 61 is a flow chart of processes constructed in accordance with the principles of the present invention;

[0134] FIG. 62 is an illustration of cards constructed in accordance with the principles of the present invention;

[0135] FIG. 63 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0136] FIG. 64 is an illustration of mobile devices constructed in accordance with the principles of the present invention;

[0137] FIG. 65 is an illustration of a card constructed in accordance with the principles of the present invention;

[0138] FIG. 66 is an illustration of a card constructed in accordance with the principles of the present invention;

[0139] FIG. 67 is an illustration of a card constructed in accordance with the principles of the present invention;

[0140] FIG. 68 is an illustration of a card constructed in accordance with the principles of the present invention;

[0141] FIG. 69 is an illustration of a card constructed in accordance with the principles of the present invention;

[0142] FIG. 70 is an illustration of a card constructed in accordance with the principles of the present invention;

[0143] FIG. 71 is an illustration of a system constructed in accordance with the principles of the present invention;

[0144] FIG. 72 is an illustration of a system constructed in accordance with the principles of the present invention; and

[0145] FIG. 73 is an illustration of process flow charts constructed in accordance with the principles of the present invention.

Detailed Description of the Invention

[0146] FIG. 1 shows mobile device 100. Mobile device 100 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, mobile device 100 may be operated in a mobile environment while a user of mobile device 100 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 100 may perform multiple functions

simultaneously (e.g., a person may carry on a conversation while at the same time browsing and purchasing products on the internet).

[0147] Mobile device 100 may include audio processing devices (e.g., microphone 108 and speaker 110). Accordingly, for example, mobile device 100 may receive voice commands from a user via microphone 108 and may process such commands to perform a function. For example, a user may place mobile device 100 into a desired operational mode by speaking a command into microphone 108 that is associated with the desired operational mode. In so doing, for example, mobile device 100 may engage in hands-free operation by receiving voice commands via microphone 108 and performing functions associated with the received voice commands.

[0148] Mobile device 100 may receive data input via microphone 108. For example, a voice-band modem may generate signals in a voice-band frequency range that may be received by microphone 108. A processor of mobile device 100 may interpret the received audible information as data signals and may process the data signals as, for example, data values and/or control data input.

[0149] Mobile device 100 may include camera 102. Camera 102 may capture one or more frames of video data and store the video data within a memory of mobile device 100. Accordingly, for example, a processor of mobile device 100 may receive one or more frames of video information via camera 102 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 100 may receive optical information that is sensed by camera

102 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 100 as data values and/or control data.

[0150] Mobile device 100 may include manual input interface 112. Manual input interface 112 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 100 may enter information into mobile device 100 via manual interface 112 to cause a processor of mobile device 100 to enter a particular mode of operation. Manual interface 112 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile device 100) during a particular mode of operation of mobile device 100.

[0151] Mobile device 100 may include display 104. Display 104 may provide visible information that may be utilized by a user during interaction with mobile device 100. A portion or all of display 104 may be touch sensitive such that objects making contact with display 104 or objects coming within a proximity of display 104 may be detected by a processor of mobile device 100. Accordingly, for example, mobile payment graphical user interface 106 may be provided by display 104 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, textual input

boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 100.

[0152] FIG. 1 shows architecture 150. User interface 152 may, for example, be included within architecture 150 to allow user interaction with architecture 150. For example, a dedicated key pad or keyboard may be included within user interface 152 to allow alphanumeric data entry into architecture 150.

[0153] Architecture 150 may include one or more displays 154. Display 154 may, for example, be touch-sensitive. Accordingly, for example, display 154 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 154. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of display 154 may be detected by processor 158 as alphanumeric data entry.

[0154] Alphanumeric entry boxes may, for example, be rendered onto display 154. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 152 and/or a virtual keypad rendered onto display 154 to select alphanumeric characters to be placed within the alphanumeric entry box in accordance with a character position identified by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 158 may receive alphanumeric characters as typed into a alphanumeric entry box of display 154 and may use such alphanumeric characters as data input.

[0155] Display 154 may, for example, provide data output from architecture 150. For example, display 154 may communicate data using a series of light pulses. Accordingly, for example, processor 158 may cause one or more portions of display 154 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 154 via light pulses having varying characteristics. Display 154 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0156] Architecture 150 may include one or more transceivers 156. Transceiver 156 may communicate information to and/or may receive information from one or more devices. Transceiver 156 may, for example, communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly, for example, transceiver 156 may allow a mobile device (e.g., mobile device 100 of FIG. 1) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 100 of FIG. 1) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 156 may exchange information with one or more other mobile devices via one or more associated cellular stations.

[0157] Transceiver 156 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 156 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 156 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 100 of FIG. 1) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network.

[0158] Architecture 150 may include contactless communication device 162, which may communicate via any one or more contactless communication methodologies, such as for example, near field communications (e.g., RFID), Bluetooth, touch simulation, light pulsing (e.g., via an LED), and electromagnetic data communication (e.g., via a dynamic magnetic stripe communications device). Accordingly, for example, contactless communication device 162 may be compatible with any contactless device, such as for example, an RFID enabled payment card and a contactless reader (e.g., a magnetic stripe reader or an NFC reader).

[0159] A non-powered card may, for example, communicate with contactless communications device 162.

Contactless communication device 162 may, for example, establish a carrier field (e.g., an RF field) that may be modulated by a device (e.g., an RFID tag) of a non-powered payment card. In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by contactless communications device 162 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 162 by modulating the RF field produced by contactless communications device 162.

[0160] A powered card may, for example, communicate with contactless communication device 162. A powered card may, for example, include a processor, a battery, a memory, wireless communications devices (e.g., a dynamic magnetic stripe communications device or RFID) and other electronics (e.g., buttons) that may allow a user to interact with the powered card to perform one or more functions. Accordingly, for example, a powered card may be used to communicate specific information to contactless communication device 162 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 162 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications.

[0161] Contactless communication device 162 may receive variable data sets from a powered card based upon, for example, manual input provided to a powered card. For example, a button associated with an on-line

purchase may be pressed on the powered card that causes a variable data set (e.g., account number and expiration date) to be communicated from the powered card to contactless communication device 162.

[0162] Discretionary data may, for example, be communicated by a powered card based upon which button was pressed on the powered card. In so doing, for example, a security code (e.g., "111") may be communicated within a discretionary data field when a button associated with a particular feature (e.g., pay with credit) is pressed on the powered card. As per another example, a different security code (e.g., "222") may be communicated within a discretionary data field when a button associated with a different feature (e.g., pay with debit) is pressed on the powered card. Accordingly, for example, processor 158 may identify what type of device may be in communication with contactless communication device 162 by analyzing the data communicated to contactless communication device 162.

[0163] Architecture 150 may include memory 160 and/or processor 158 may include internal memory. Accordingly, for example, application code may be stored within memory 160 and/or processor 158 and executed by processor 158 in support of functions performed by architecture 150. For example, an application (e.g., a graphical user interface) may be executed by architecture 150 and displayed onto display 154, which may be used to interact with a user of a mobile device (e.g., mobile device 100 of FIG. 1). Persons skilled in the art will appreciate that executable application code may be communicated to architecture 150 via any one or more interfaces of

architecture 150 (e.g., user interface 152, display 154, transceiver 156, and/or contactless communication device 162).

[0164] Application data (e.g., payment card data) may be stored within memory 160 and accessed by processor 158 during operation. For example, payment card data may be stored within memory 160 and recalled by processor 158 during a financial transaction being conducted by a mobile device (e.g., mobile device 100 of FIG. 1). Once recalled, processor 158 may communicate the payment card data via transceiver 156 and/or contactless communication device 162 to complete a financial transaction.

[0165] FIG. 2 shows network topology 200 that may include, for example, mobile device 202 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile device 202 may, for example, include a contactless interface that may initiate, sustain, and/or terminate communication channel 226 between contactless device 204 and mobile device 202. Contactless device 204 and mobile device 202 may communicate via channel 226 using any number of contactless mediums, which may include for example, visible, audible, capacitive, electromagnetic, magnetic, and/or RF mediums.

[0166] Mobile device 202 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 212 and/or payment network 214) and/or one or more wireless networks (e.g., mobile network 210). Mobile device 202 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile device 202 to communicate

information (e.g., voice and data) to cellular network access infrastructure 206 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 206 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0167] Mobile device 202 may, for example, communicate with wireless access point 208 over a wireless interface (e.g., a Bluetooth interface or a Wi-Fi interface). Accordingly, for example, mobile device 202 may access one or more wired networks (e.g., IP network 212 and/or payment network 214) and/or one or more wireless networks (e.g., mobile network 210) without the need to first gain access to cellular network access infrastructure 206.

[0168] Contactless device 204 may, for example, be a powered card or a non-powered card (e.g., a powered payment card or a non-powered payment card). Accordingly, for example, payment information (e.g., a payment account number and a card expiration date) may be communicated from contactless device 204 to mobile device 202 in support of a financial transaction being conducted by mobile device 202. In so doing, for example, items for purchase on IP network 212 (e.g., the internet) may be accessed by a browser of mobile device 202 via an access point (e.g., wireless access point 208 or cellular network access infrastructure 206). Mobile device 202 may, for example, complete a purchase transaction by first obtaining required payment information from contactless device 204 and

then communicating such payment information to network entities (e.g., payment server 216 and/or issuer 220).

[0169] Payment server 216 may, for example, contact issuer 220 via a network (e.g., payment network 214) with payment information received from mobile device 202 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile device 202 via any one or more delivery options (e.g., via a short messaging service of mobile network 210 or an email delivery service of IP network 212).

[0170] A payment receipt may, for example, be provided to mobile device 202 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile device 202 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0171] A mobile device (e.g., mobile device 224) may, for example, include a contactless communication device (e.g., an RFID) that may initiate, sustain, and/or terminate contactless communication channel 228 with merchant terminal 218. Accordingly, for example, mobile device 224 may communicate payment information to merchant terminal 218 to complete a financial transaction. In so doing, for example, mobile device 224 may first receive payment information via contactless communication channel 230 from contactless device 222 (e.g., a non-powered card), temporarily store the received payment information within a memory of mobile device 224, and forward the payment information onto merchant terminal 218 to complete a financial transaction. As per another example, mobile device 224 may provide previously stored financial

information associated with one or more payment cards (e.g., one or more non-powered payment cards). Accordingly, for example, payment information may be recalled from a memory of mobile device 224 and communicated to merchant terminal 218 via contactless communication channel 228 to complete a financial transaction using merchant terminal 218.

[0172] FIG. 3 shows system 300, which may include mobile device 302 and payment card 304. Mobile device 302 may, for example, be a laptop computer, a PDA, a mobile telephonic device (e.g., a smartphone), an MP3 player, a GPS, or any other mobile device. Display 308 may be a touch-sensitive display (e.g., sensitive to a change in capacitance). Payment card 304 may, for example, be a powered payment card or a non-powered payment card.

[0173] Mobile device 302 and payment card 304 may each include a contactless communication device (e.g., RFID) that may communicate via a contactless communication channel that may be formed between mobile device 302 and payment card 304 after coming into proximity to one another. Payment card 304 may, for example, be tapped onto display 308 of mobile device 302 to establish a proximity relationship that forms a communication channel between payment card 304 and mobile device 302. As per another example, payment card 304 may be brought within a proximity distance (e.g., up to two inches) of mobile device 302 to establish a contactless communication channel between mobile device 302 and payment card 304.

[0174] A processor of mobile device 302 may, for example, execute application code that may generate a graphical user interface (GUI) onto display 308 of

mobile device 302. Message 306 of a GUI may invite a user of mobile device 302 to begin a mobile payment by tapping a payment card against display 308. As per another example, by tapping payment card 304 against mobile device 302, mobile device 302 may autonomously determine that a mobile payment is desired and then generate a mobile payment GUI onto display 302.

[0175] Mobile device 302 may, for example, autonomously determine a type of card that may be tapped against it. For example, a processor of mobile device 302 may receive payment card data that may be indicative of a non-powered payment card (e.g., payment card data received from a non-powered card may not provide a security code associated with the card). As per another example, a processor of mobile device 302 may receive data that may be indicative of a powered card (e.g., payment card data received may contain a dynamically generated security code). Payment card data received from a powered card may, for example, include a dynamic security code that may change depending upon a type of transaction being conducted (e.g., debit or credit transaction).

[0176] As per another example, payment card 304 may be a powered payment card that may include electronics to simulate a human touch (e.g., payment card 304 may generate a change in capacitance that may be sensed by display 308). Through a series of simulated touches, payment card 304 may communicate a series of data bits to display 308, which may then be processed by a processor of mobile device 302. In so doing, for example, a contactless communication channel may be established where data is transferred from payment card

304 to mobile device 302 via a series of simulated touches.

[0177] Payment card 304 may, for example, include a light sensor. Accordingly, for example, payment card 304 may be sensitive to light pulses generated within a region of display 308. The light sensor of payment card 304 may receive a series of light pulses, which may be construed by a processor of payment card 304 as data generated by mobile device 302. In so doing, for example, payment card 304 may receive an optical data stream represented by a series of light pulses generated by display 308. As such, a two-way communication channel may be formed, where simulated touches may generate a data stream from payment card 304 to mobile device 302 and light pulses may generate a data stream from mobile device 302 to payment card 304.

[0178] FIG. 4 shows GUI 400, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 400 may, for example, generate results of a card detection operation that may be performed by a processor of a mobile device. For example, card information may be exchanged between a card and a mobile device via a contactless communication channel that may identify a type of card that is being presented to the mobile device. Any type of card may be detected by a processor of a mobile device, such as for example, an airline card, a travel card, a bank card, a healthcare card, an identification card, and a loyalty rewards card. A card number communicated to a mobile device may, for example, be indicative of a card type (e.g., bank card 404) that is presented to a mobile device. Accordingly, for

example, a processor of a mobile device may identify a card type presented to the mobile device by analyzing a card number received from the card and may indicate the identified card type via GUI 400 (e.g., the identified card type may be generated onto GUI 400 having a different graphical presentation than the other card types listed).

[0179] A GUI may, for example, provide navigation aids. A GUI may, for example, provide navigation aids that may be touch sensitive. For example, GUI 400 may include navigation aids 406 and 408 to enable a user to revert to a previous GUI or advance to a subsequent GUI. Accordingly, for example, a user may touch an area on a display of a mobile device that displays a navigation aid to activate the touched navigation aid. In so doing, for example, a user may touch navigation aid 406 to revert to the previous GUI or a user may touch navigation aid 408 to advance to the next GUI.

[0180] FIG. 5 shows GUI 500, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 500 may, for example, generate results of a payment card detection operation that may be performed by a processor of a mobile device. A non-powered payment card may, for example, communicate a single payment card number that may be associated with a number of payment options (e.g., debit, credit, or points). Accordingly, for example, GUI 500 may be generated to allow a user an opportunity to select which payment option (e.g., credit option 502) from a number of payment options is to be used to settle a payment transaction. Once identified, a payment option selection (e.g., credit option 502) may be communicated by a mobile device to

an issuer of the payment card to settle the transaction using the selected payment option.

[0181] As per another example, a powered payment card may include a user interface to allow a user to select from a number of payment options. A button on a powered payment card may, for example, be associated with one payment method (e.g., pay with credit) and another button may, for example, be associated with another payment method (e.g., pay with points). Data associated with the selected payment method may be communicated from a powered payment card to a mobile device. Accordingly, for example, a processor of a mobile device may detect the payment method communicated by a powered payment card (e.g., as communicated within a discretionary data field) and may autonomously generate a graphical representation of the payment method selected (e.g., GUI 500 may autonomously generate a graphical representation that credit method 502 was selected).

[0182] FIG. 6 shows GUI 600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 600 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. A mobile device may, for example, challenge a user of the mobile device to enter a PIN that may be associated with a payment card (e.g., VISA credit 602) that was previously presented to the mobile device for payment. GUI 600 may, for example, generate virtual pin pad 606 that may include touch-sensitive buttons having alphanumeric indicia associated with each button. A user may touch one or more buttons of pin pad 606 that may correspond to respective characters of a PIN and an

indication of the user's selection may appear within area 604. Characters displayed within area 604 may, for example, be hidden for security purposes.

[0183] Activation of virtual button 608 may, for example, cause a processor of a mobile device to compare a PIN entered by a user of the mobile device to a PIN that may be associated with the payment card presented to the mobile device for payment. The PIN may, for example, be stored within protected memory of the mobile device, so that a processor of the mobile device may locally determine the validity of the PIN entered. Alternately, for example, the mobile device may communicate the PIN to the issuing bank for a remote validation of the PIN entered. Persons skilled in the art will appreciate that a user interface (e.g., a keypad or keyboard) of a mobile device may be used instead of virtual pin pad 606 to enter the one or more characters of a PIN.

[0184] FIG. 7 shows GUI 700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 700 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. A mobile device may, for example, challenge a user of the mobile device to enter a security code that may be associated with a payment card (e.g., VISA credit 702) that was previously presented to the mobile device for payment. Such a security code (e.g., a CVV code) may, for example, be printed on the back of the payment card.

[0185] GUI 700 may, for example, generate virtual pin pad 706 that may include touch-sensitive buttons having alphanumeric indicia associated with each

button. A user may touch one or more buttons of pin pad 706 that may correspond to respective characters of a security code and an indication of the user's selection may appear within area 704. Characters displayed within area 704 may, for example, be hidden for security purposes.

[0186] Activation of virtual button 708 may, for example, cause a processor of a mobile device to compare a security code entered by a user of the mobile device to a security code that may be associated with the payment card presented to the mobile device for payment. The security code may, for example, be stored within protected memory of the mobile device, so that a processor of the mobile device may locally determine the validity of the security code entered. Alternately, for example, the mobile device may communicate the security code to the issuing bank for a remote validation of the security code entered. Persons skilled in the art will appreciate that a user interface (e.g., a keypad or keyboard) of a mobile device may be used instead of virtual pin pad 706 to enter the one or more characters of a security code.

[0187] FIG. 8 shows GUI 800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 800 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. A mobile device may, for example, maintain memory of one or more payment cards previously presented to the mobile device for payment. A mobile device may, for example, allow a user to store payment information within the mobile device that may be associated with a payment card to be used at some point in the future.

[0188] Accordingly, for example, a user may recall payment information previously stored in memory of a mobile device in order to complete a purchase transaction using the mobile device. In order to validate that a user of a mobile device is actually the owner of payment information recalled from memory of the mobile device, GUI 800 may challenge the user to present the physical payment card whose associated payment information was recalled from memory. In so doing, for example, GUI 800 may prevent a fraudulent user of a mobile device from authorizing a purchase using payment information stored in memory of the mobile device that is not owned by the fraudulent user.

[0189] A user may, for example, be required to present a physical payment card to GUI 800 by placing (or tapping) the physical payment card within a proximity of a display of a mobile device that is generating GUI 800. In so doing, for example, a contactless communication channel (e.g., an RFID communication channel) may be established between the physical payment card and the mobile device, such that payment information may be communicated from the physical payment card to the mobile device. Upon verification that the communicated payment information matches payment information stored in memory of the mobile device, the payment information may be validated and authorized to be communicated from the mobile device to a network entity (e.g., a payment server or the issuer of the payment card) for settlement of the purchase transaction.

[0190] FIG. 9 shows GUI 900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 900 may, for

example, include validation area 902 as generated by a processor of a mobile device. Validation area 902 may, for example, include one or more data exchange areas (e.g., data exchange areas 904 and 906). Icon 904 may, for example, be generated by GUI 900 within an area of a display of a mobile device that may be sensitive to touch (e.g., an area that may be sensitive to a capacitance change). Area 906 may, for example, be generated by GUI 900 within an area of a display of a mobile device that may generate pulses of light.

[0191] A powered payment card may be validated for use by a mobile device through an exchange data with the powered payment card via data exchange areas 904 and 906. For example, a powered payment card may be pressed against validation area 902 so that a touch simulation device of the powered payment card aligns with data exchange area 904 and a light sensing device aligns with data exchange area 906. Accordingly, for example, the powered payment card may communicate information to a processor of a mobile device by simulating a series of touches in data exchange area 904 and data may be communicated to the powered payment card by a processor of the mobile device by generating a series of light pulses in data exchange area 906. In so doing, for example, a mobile device and a powered payment card may exchange validation information so that payment card information stored within the mobile device may be validated for use.

[0192] A mobile device may, for example, include a motion capture device (e.g., a camera) and a powered payment card may, for example, include a light source (e.g., an LED). Accordingly, for example, information (e.g., validation information) may be exchanged between

a mobile device and a powered payment card such that information communicated by the powered payment card may be communicated as a series of light pulses while the camera of the mobile device captures the series of light pulses. A processor of the mobile device may construe the series of light pulses as information that may be used, for example, as validation information.

[0193] FIG. 10 shows GUI 1000 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1000 may be generated, for example, after payment card information has been communicated by either of a non-powered payment card or a powered payment card to a mobile device. A user of a mobile device may, for example, elect whether to store such payment card information within a memory location of the mobile device. If a user chooses not to store payment information received from a payment card (e.g., as elected by selection of radio button 1004), a mobile device may delete all payment information previously received from a payment card after the payment information is used to complete a purchase transaction. Accordingly, a user wishing to use the same payment card to complete a payment transaction in the future is required to present the payment card to the mobile device so that the payment card may communicate payment card information to the mobile device in order to complete the payment transaction. If a user chooses to store payment information received from a payment card (e.g., as elected by selection of radio button 1002), a mobile device may store a portion of, or all, payment information previously received from a payment card in accordance with a user's preference.

[0194] FIG. 11 shows GUI 1100 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1100 may, for example, offer storage options to a user of a mobile device that has elected to store a portion of, or all, payment card information previously communicated to the mobile device by a non-powered card or a powered card. A data storage option may, for example, be selected by a user of a mobile device (e.g., by touching a portion of text box 1102) that stores only a portion (e.g., an expiration date and payment card account number) of the payment card information into a memory of the mobile device. Accordingly, for example, a payment card may communicate one, two, and/or three tracks of magnetic stripe data to a mobile device, but the only payment information stored within a memory of the mobile device upon selection of text box 1102 is the expiration date and the payment card account number. All remaining information that may have been communicated by the payment card to the mobile device may be deleted by the mobile device.

[0195] Selection of text box 1104 may, for example, cause all payment information communicated by a payment card to a mobile device to be stored within a memory of the mobile device. Accordingly, for example, a mobile device may use a portion or all of the payment information stored within its memory to complete a purchase transaction. However, payment card validation information (e.g., a PIN or security code) may still be required to be entered by a user of the mobile device before the mobile device may complete a purchase transaction with the stored payment information.

[0196] Selection of box 1106 may, for example, cause all payment information communicated by a payment card to a mobile device to be stored within a memory of the mobile device. All validation information (e.g., a PIN or security code) that may be entered by a user of the mobile device to validate payment information received from a payment card may also be stored within a memory of the mobile device. Accordingly, for example, a mobile device may use a portion or all of the payment information, including validation information, stored within its memory to complete a purchase transaction.

[0197] Selection of box 1108 may, for example, cause all payment information, including discretionary data fields, communicated by a payment card to a mobile device to be stored within a memory of the mobile device. A powered payment card may, for example, allow a user of the powered payment card to select one or more options that may be associated with the powered payment card. A powered payment card may, for example, communicate indicia associated with the one or more selected options within discretionary data fields of magnetic stripe data that may be communicated to a mobile device.

[0198] For example, a user of a powered payment card may elect to pay for a purchase using rewards points by pressing a button on the powered payment card that is associated with a rewards points payment option. Accordingly, for example, a powered payment card may insert a rewards points payment code within a discretionary data field of a first, a second and/or a third track of magnetic stripe data and may communicate all track data, including the discretionary data field, to a mobile device. In so doing, for example, a

processor of a mobile device may detect such a payment code within a discretionary data field and may store payment information within a memory of the mobile device that is indicative of the rewards points payment code contained within the discretionary data field.

[0199] FIG. 12 shows GUI 1200 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1200 may, for example, offer a split-payment option to a user of a mobile device, such that the user may elect to split payment for a selected purchase between two or more payment accounts. The mobile device may, for example, communicate payment information for each of the selected split-payment accounts to respective network entities (e.g., issuer and payment servers) of the selected split-payment accounts in order to settle the amounts owing on each of the selected split-payment accounts.

[0200] A user may, for example, select option 1202 (e.g., by tapping a payment card against a display of a mobile device or by presenting a payment card within proximity to the mobile device). In so doing, for example, a contactless communication channel (e.g., an RFID communication channel) may be established between the payment card and the mobile device so that payment information associated with the payment card may be communicated by the payment card to the mobile device and used as a split-payment account for a selected purchase.

[0201] An alternate contactless communication channel may be established, for example, by pressing a payment card against portion 1208. Accordingly, for example, a payment card may communicate payment

information associated with the payment card to a processor of a mobile device by simulating a series of touches at a location within portion 1208 (e.g., at icon 1210) and the processor of the mobile device may communicate information to the payment card by generating a series of light pulses at a location within portion 1208 (e.g., at location 1212). In so doing, for example, payment information associated with the payment card may be received by a processor of a mobile device and used as a split-payment account to partially cover the purchase price of a selected purchase.

[0202] Other contactless communication channels may be established. For example, a processor of a payment card may communicate payment information to a mobile device by generating a series of light pulses (e.g., via an LED of the payment card), which may be captured by a camera of the mobile device and construed by a processor of the mobile device as payment information. As per another example, a payment card may communicate payment information using audible sounds that may be received by a microphone of a mobile device and construed by a processor of the mobile device as payment information.

[0203] A payment account may, for example, be selected from a memory of the mobile device (e.g., by selecting radio button 1204). Associated payment information may, for example, be selectively retrieved from a memory of the mobile device and used by the mobile device as a split-payment account in partial payment for a selected purchase. Alternately, for example, a split-payment option may be declined by a

user of a mobile device (e.g., by selecting radio button 1206).

[0204] FIG. 13 shows GUI 1300 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1300 may, for example, provide a summary of split-payment methods that may have been selected by a user of a mobile device. Portion 1302, for example, may display an amount owing for a particular selected purchase. Portions 1304-1308 may, for example, include an alphanumeric entry box to allow a user of a mobile device to input payment amounts (e.g., currency or points) that he or she wishes to apply towards a total amount owing as may be displayed in portion 1302. Portions 1304-1308 may, for example, include those payment accounts that a user of a mobile device previously selected as split-payment accounts.

[0205] Accordingly, for example, a user may elect to charge $10 against a VISA credit account, $35 against a M/C debit account, and 500 rewards points earned by the VISA credit account towards full payment of a $50 amount owing for a particular selected purchase. In so doing, for example, a mobile device may communicate with selected network entities (e.g., issuer and payment servers) to provide transaction information associated with each split-payment account selected, so that each amount owing may be settled.

[0206] Portions 1310-1314 may, for example, include alphanumeric entry boxes to allow a user of a mobile device to make comments on each account selected as a split-payment account. Accordingly, for example, a mobile device may communicate notes that may be entered by a user within portions 1310-1314 to, for example, a

payment server. In so doing, for example, receipts and/or account statements that may be generated by a network entity (e.g., an issuer or a payment server) may include such notes so that a user of a mobile device, upon receipt of such receipts and/or account statements, may be reminded of his or her thought process when such a split-payment was transacted.

[0207] FIG. 14 shows GUI 1400 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1400 may, for example, offer checkout options to a user of a mobile device to allow a level of integration between the user and one or more issuers of associated payment accounts used by the mobile device in settlement of a selected purchase.

[0208] For example, a user may utilize billing tag list 1402 to categorize a selected purchase into one of many purchase categories. A user's physical presence may, for example, be at a fast-food establishment where the user may select a food purchase from the fast-food establishment's website using a browser of the user's mobile device. Payment information used to settle a transaction associated with the selected food purchase may be collected and/or generated by the mobile device and forwarded onto a payment server and/or an associated issuer for settlement. In addition, the mobile device may forward a billing tag selected from billing tag list 1402 to the associated issuer, so that the associated issuer may label the selected transaction on a billing statement using the selected billing tag. In so doing, for example, a user may customize an accounting of the issuer's billing statement by using a mobile device to communicate

payment information and billing tags associated with selected purchases to track expenditures within the various purchase categories of billing tag list 1402.

[0209] A user of a mobile device may select receipt delivery options for each purchase that may be transacted using a mobile device. For example, a receipt delivery list may be generated by a processor of a mobile device so that a user of the mobile device may select a receipt delivery option. Accordingly, for example, the selected receipt delivery option along with payment information may be communicated by a mobile device to a payment server and the payment server (or other entity) may direct a delivery of the receipt based upon the receipt delivery option received.

[0210] A user may, for example, request delivery of a purchase receipt via text messaging (e.g., by selecting receipt delivery option 1406). In so doing, for example, a mobile device may complete a purchase transaction with an entity of a payment network (e.g., a payment server) and may further request that the payment server deliver a receipt to the mobile device in a text message format. Accordingly, for example, in addition to providing payment information to the payment server, a mobile device may also provide a text message address (e.g., an SMS text message address) to the payment server. In so doing, for example, the mobile device may receive a receipt of the completed purchase transaction from the payment server via a text message at the text message address provided by the mobile device.

[0211] As per another example, a multimedia message (e.g., an MMS message containing rich content) may be

received by a mobile device from a payment server in the form of, for example, a graphical image (e.g., barcode), such that the barcode may be used as a proof-of-purchase (e.g., proof-of-purchase of an airline ticket and an associated barcode that gains access by the user of the mobile device to a particular seating assignment on the airplane.)

[0212] A receipt (e.g., a receipt received via multimedia messaging) may, for example, provide rewards to a user of the mobile device for completing payment transactions via a mobile device. For example, a mobile device may communicate indicia to a payment server that identifies a payment transaction as a mobile payment transaction. The communicated mobile payment indicia may, for example, trigger a payment server to not only provide a receipt for the purchase transaction to the mobile device, but also to provide a multimedia game that may be executed by the mobile device. As per an example, an animated trivia question may be communicated to a mobile device via an MMS message upon completion of a mobile payment transaction. Upon successfully answering the animated trivia question, a user of the mobile device may receive another MMS message that contains a coupon for free merchandise from the merchant whose goods were just purchased. As per another example, a receipt received from a payment server may itself contain coupons for discounted or free merchandise without requiring that a user of the mobile device perform any further actions beyond completing a mobile payment purchase with a mobile device.

[0213] A user may, for example, request delivery of a purchase receipt via email (e.g., by selecting

receipt delivery option 1408). In so doing, for example, an email address associated with the user may be provided by the mobile device to a payment server in addition to any required payment information that may be required to complete a purchase transaction. Accordingly, for example, a payment server may address a receipt to an email address received from a mobile device during a mobile payment transaction.

[0214] A user may, for example, request delivery of a purchase receipt (e.g., by selecting receipt delivery option 1410) via a format that may be compatible with an accounting software package (e.g., QuickBooks). For example, a mobile device may allow a user to categorize a particular purchase within a particular expense account (e.g., an office supply expense account) during a purchase transaction. Once the purchase transaction is completed, an electronic receipt may be communicated to the mobile device that may be tagged with the categorized expense account (e.g., the accounting software package may have its own address that receipts may be delivered to). In so doing, for example, an accounting software package that may be executing on the mobile device may autonomously access the electronic receipt from its own address and may autonomously enter the expense in the correct category so that all purchases made by the mobile device may be correctly accounted for within the accounting software package.

[0215] A user may, for example, request delivery of a purchase receipt (e.g., by selecting receipt delivery option 1412) via a format that may be compatible with the bank that issued the selected payment account. Accordingly, for example, a payment server may forward

a receipt of the purchase transaction to the issuing bank and the issuing bank may format the receipt for delivery with the user's month-end account statement.

[0216] A user may, for example, enter comments about a purchase transaction that may be included within a receipt. For example, a user may enter comments 1404 that may remind the user to include the receipt within his or her tax records because the purchase may be deemed as tax deductible. Accordingly, for example, comments 1404 may accompany payment information communicated by a mobile device to a payment server. In so doing, for example, a payment server may add comments 1404 to a receipt generated by the payment server and may forward the receipt with the added comments to the user of the mobile device as dictated by the receipt delivery options requested by the user of the mobile device.

[0217] FIG. 15 shows GUI 1500 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1500 may, for example, offer a check-out option to a user of a mobile device, such that the user may elect to apply a rewards card to a selected purchase in order for the rewards card to accrue points for the purchase. The mobile device may, for example, submit rewards card information and transaction information to respective issuers of the rewards account so that the respective issuers may credit the rewards account accordingly.

[0218] A user may, for example, select option 1502 (e.g., by tapping a rewards card against a display of a mobile device or by presenting a rewards card within proximity to the mobile device). In so doing, for example, a contactless communication channel (e.g., an

RFID communication channel) may be established between the rewards card and the mobile device so that information associated with the rewards card may be communicated by the rewards card to the mobile device.

[0219] An alternate contactless communication channel may be established, for example, by pressing a rewards card against portion 1508. Accordingly, for example, a rewards card may communicate information associated with the rewards card to a processor of a mobile device by simulating a series of touches within portion 1508 (e.g., at icon 1510) and the processor of the mobile device may communicate information to the rewards card by generating a series of light pulses within portion 1508 (e.g., at location 1512). In so doing, for example, rewards information associated with the rewards card may be received by a mobile device and communicated to an issuer of the rewards card so that the rewards account may be updated with the purchase transaction information.

[0220] Other contactless communication channels may be established. For example, a processor of a rewards card may communicate rewards information to a mobile device by generating a series of light pulses (e.g., via an LED of the rewards card), which may be captured by a camera of the mobile device and construed by a processor of the mobile device as rewards information. As per another example, a payment card may communicate payment information using audible sounds that may be received by a microphone of a mobile device and construed by a processor of the mobile device as payment information.

[0221] A rewards account may, for example, be selected from a memory of the mobile device (e.g., by

selecting radio button 1504). Associated rewards information may, for example, be selectively retrieved from a memory of the mobile device and communicated by the mobile device to an issuer of the rewards account so that the rewards account may be credited with the selected purchase.

[0222] A user of a mobile device may, for example, place an order for a rewards card by selecting radio button 1506. Accordingly, for example, a mobile device may communicate payment information to a payment server to complete a purchase transaction and may also communicate a request that a rewards account be created. A payment server may, for example, forward the rewards account creation request to an issuer of a rewards account along with details of the purchase transaction, so that the issuer may first create the rewards account and may then credit the account according to the purchase transaction. Accordingly, for example, an electronic version of a newly created rewards card (e.g., a graphical representation of a newly created rewards card) may, for example, be communicated to a mobile device which may, for example, include a barcode representation of the rewards account information. In addition, rewards card information may, for example, be added to a memory of a mobile device for future access.

[0223] FIG. 16 shows GUI 1600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1600 may, for example, challenge a user of a mobile device to enter an access code that may be required to authenticate a purchase transaction. GUI 1600 may, for example, include virtual keyboard 1604 to allow a user of a

mobile device to enter such an access code. Alternately, for example, a manual input interface of a mobile device (e.g., a keyboard or a keypad) may be used to enter such an access code.

[0224] As a user of a mobile device enters each character of an access code, portion 1602 may reflect such entry. Such entries may, for example, be reflected within portion 1602 as protected characters (e.g., the actual value of each character may be blocked out) to protect the security and safety of the entered access code. Once an entered access code is verified and authenticated by a mobile device, the mobile device may complete the requested purchase transaction.

[0225] FIG. 17 shows GUI 1700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1700 may, for example, include portion 1702 that may display a graphical representation of a proof-of-purchase (e.g., a barcode). Such a proof-of-purchase may be communicated to a mobile device via a network entity (e.g., a payment server) upon completion of a purchase transaction by the mobile device.

[0226] Accordingly, for example, portion 1702 may graphically display a proof-of-purchase that may be recognized by a reader (e.g., a barcode reader). In so doing, for example, a system that may include a barcode reader may verify the validity of a proof-of-purchase barcode, which may then allow a user of a mobile device displaying such a barcode to enjoy the goods and/or services purchased by the user via the mobile device as acknowledged by the verified barcode. As per one example, such a verified barcode may allow entry onto

an airplane having a seat assignment that is encoded within the barcode. As per another example, a user may have made an on-line purchase of an appliance using his or her mobile device and may have requested pick-up of the purchased appliance at an appliance inventory warehouse. Upon arrival at the appliance inventory warehouse, a user may retrieve an electronic proof-of-purchase (e.g., a barcode) from a memory of the mobile device that was received by the user's mobile device upon completion of the appliance purchase transaction. A reader (e.g., a barcode reader) at the appliance inventory warehouse may read the user's barcode directly from a display of the user's mobile device, verify that a purchase was completed by the user's mobile device, and may authorize the appliance for pickup by the user.

[0227] FIG. 18 shows GUI 1800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1800 may, for example, enable a funds transfer to one or more financial accounts. GUI 1800 may, for example, enable a transfer of funds (e.g., by selecting radio button 1802) directly from one or more financial accounts into one or more financial accounts. GUI 1800 may, for example, generate a communication channel with a recipient of a funds transfer (e.g., by selecting radio button 1804) and may allow the recipient to interactively determine the financial account that is to receive the transferred funds.

[0228] FIG. 19 shows GUI 1900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1900 may, for example, enable a funds transfer to one or more

accounts. GUI 1900 may, for example, allow a user of a mobile device to select an object (e.g., by selecting an entry within menu list 1902) that may be associated with the funds transfer. GUI 1900 may, for example, allow a user to select an account (e.g., by selecting an entry within menu list 1904) that may be associated with the object selected within menu list 1902.

[0229] Accordingly, for example, a mobile device may include a memory within which a user may enter one or more potential recipients of a funds transfer. A processor of a mobile device may, for example, list each potential recipient of a funds transfer within menu list 1902. A user of a mobile device may, for example, select a recipient of a funds transfer by activating (e.g., touching) an entry within menu list 1902 that corresponds to the selected recipient. As per an example, a user's funds transfer recipient list, as may be reflected by menu list 1902, may include persons, financial accounts, inanimate objects, or any other type of object.

[0230] Once a selected funds transfer recipient is selected within menu list 1902, menu list 1904 may be populated. Accordingly, for example, a mobile device may include a memory within which a user may enter one or more accounts that may be associated with one or more potential recipients of a funds transfer. A processor of a mobile device may, for example, list each account in menu list 1904 that may be associated with the selected recipient of menu list 1902. A user of a mobile device may, for example, select an account for a funds transfer by activating (e.g., touching) an entry within menu list 1904 that corresponds to the selected account. As per an example, a user's funds

transfer account list, as may be reflected by menu list 1904, may include any account that may be associated with the selected recipient of menu list 1902.

[0231] FIG. 20 shows GUI 2000 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 2000 may, for example, enable a funds transfer from a source account (e.g., an account associated with a payment card that is tapped against a display of a mobile device) to a target account (e.g., a car loan account). Portion 2002 may, for example, list account details that may be associated with a target account (e.g., an account number associated with a car loan, the payoff amount, and the amount due). Portion 2002 may, for example, include details that may be associated with a target account that a mobile device has collected from a network entity (e.g., a bank) via a network connection between the mobile device and the network entity.

[0232] Portion 2004 (e.g., an alphanumeric entry box) may, for example, allow a user of a mobile device to enter an amount to be transferred (e.g., an amount that is equal to the minimum amount due on an installment payment agreement). GUI 2000 may, for example, request an identification of a source account from which the amount will be transferred. As per an example, a user of a mobile device may tap a payment card against a display of the mobile device to establish a contactless communication channel between the payment card and the mobile device within which payment information may be communicated from the payment card to the mobile device. As per another example, a payment card may communicate payment information to a mobile device via a series of touch

simulations (e.g., changes in capacitance generated by a payment card that may be detected by a touch-sensitive display of a mobile device). A series of light pulses, or audible information, for example, may be communicated by the payment card to the mobile device in order to communicate payment information.

[0233] GUI 2000 may, for example, display a summary of payment information that may have been received by a mobile device from a payment card via a contactless communication channel. For example, portion 2006 may be displayed by GUI 2000 to allow a user of a mobile device to confirm the identity of a payment account from which an amount of money will be transferred. Once confirmed, the mobile device may communicate with network entities (e.g., an issuer of the source account and a bank associated with the target account) to complete the money transfer.

[0234] FIG. 21 shows GUI 2100 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 2100 may, for example, enable a funds transfer to an account associated with a person. A recipient may, for example, interactively select an account into which the funds will be transferred. Accordingly, for example, contact list 2102 may be displayed by GUI 2100 as a list of potential recipients of a money transfer. Contact method list 2104 may, for example, by displayed by GUI 2100 as a list of methods that may be used to contact the recipient as selected within contact list 2102. In so doing, for example, a person within contact list 2102 (e.g., Trace) may be selected by a user of a mobile device to be the recipient of a funds transfer and the recipient may be contacted, for

example, in accordance with a method selected in contact method list 2104 (e.g., transfer alert).

[0235] FIG. 22 shows system 2200, which may include mobile device 2202, receiving device 2204, and network 2210. Mobile device 2202 may be a device used to coordinate a money transfer and receiving device 2204 may be a device used to coordinate receipt of a money transfer. Receiving device may, for example, be a mobile device. Receiving device, for example, may not be a mobile device (e.g., a desktop computer). Devices 2202-2204 may communicate via network 2210, which may include any combination of cellular network resources, wireless network resources, and/or wired network resources.

[0236] Mobile device 2202 may, for example, include a processor that may render money transfer GUI 2206 onto a display of mobile device 2202. GUI 2206 may, for example, pause while a user of mobile device 2202 selects a payment account from which a money transfer may be withdrawn. Accordingly, for example, mobile device 2202 may wait until a payment card is brought within a proximity to, or a touch relationship with, mobile device 2202 (e.g., a payment card may be tapped onto a display of mobile device 2202). Alternately, for example, a payment card may communicate with mobile device 2202 using any number of contactless methods (e.g., using light, sound, capacitive, magnetic or electromagnetic communication). In so doing, for example, mobile device 2202 may establish a contactless communication channel with a payment card in which payment information is communicated from the payment card to mobile device 2202 and is summarized onto GUI 2206 for review by a user of mobile device 2202. A

user of mobile device 2202 may enter an amount of money for transfer, may verify a money amount for transfer, and may enter a message to be communicated to receiving device 2204.

[0237] Mobile device 2202 may communicate payment information received from a payment card along with information received from a user of mobile device 2202 to a network entity (e.g., an issuer) where, for example, authorization of the transfer amount from the account selected is performed. Once authorized, mobile device 2202 may communicate a transfer alert along with a transfer alert message to receiving device 2204. Receiving device 2204 may, for example, present a transfer alert along with the associated transfer alert message onto GUI 2208. A user of receiving device 2204 may respond to the transfer alert message received from mobile device 2202 by sending an acknowledgment message to mobile device 2202 via network 2210.

[0238] A user of receiving device 2204 may, for example, be asked to enter account information that is to be used as the receiving account for the money transfer. Accordingly, for example, a user of receiving device 2204 may provide such account information any number of ways. For example, a payment card associated with a receiving account may be brought within a proximity, or a touching, relationship to receiving device 2204. In so doing, for example, a contactless communication channel (e.g., an RFID channel) may be formed to communicate such information. Alternately, a payment card may communicate with receiving device 2204 using any number of contactless methods (e.g., using light, sound, capacitive, magnetic or electromagnetic communication). A user of receiving

device 2204 may verify the receive account information as it may be displayed onto GUI 2208.

[0239] Receiving device 2204 may, for example, communicate information associated with a receiving account to mobile device 2202 via network 2210. Accordingly, for example, mobile device 2202 may coordinate the money transfer via network 2210 with network entities (e.g., an issuer of the account used to provide money to transfer and an issuer of the account used to receive money for transfer). Once the money transfer is completed, an acknowledgment message may be displayed onto GUI 2206 by a processor of mobile device 2202 and an acknowledgment message may be communicated by mobile device 2202 to receiving device 2204 and then displayed onto GUI 2208 by a processor of receiving device 2204.

[0240] FIG. 23 shows system 2300, which may include a mobile device 2302, a powered or non-powered payment card 2304, a remote application 2308 and network 2306. Mobile device 2302 may, for example, access remote application 2308 via network 2306 in order to complete a purchase transaction. Accordingly, for example, payment card 2304 may communicate payment information to mobile device 2302 via contactless communication channel 2312 and mobile device 2302 may communicate the payment information to remote application 2308 via communication channel 2310 to complete the purchase transaction.

[0241] Contactless communication channel 2312 may be any type of contactless communication channel, such as for example, an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel. Contactless communication channel 2312 may be a two-way

communication channel, where mobile device 2302 may communicate with payment card 2304 in order to, for example, enhance data communication between mobile device 2302 and payment card 2304.

[0242] As per one example, payment card 2304 may communicate payment information (e.g., one, two, and/or three tracks of magnetic stripe data) to mobile device 2302 after payment card 2304 is tapped against mobile device 2302. Remote application 2308 may, for example, be an on-line payment application that does not require a fully populated magnetic stripe message to complete a purchase transaction, but may only require a subset of a fully populated magnetic stripe message (e.g., account number and expiration date). Accordingly, for example, mobile device 2302 may filter payment information received from payment card 2304 to only include the subset of information that may be required by remote application 2308 and may communicate only the filtered payment information to remote application 2308 to complete the purchase transaction.

[0243] In general, for example, mobile device 2302 may filter payment information received from payment card 2304 into a filtered subset of payment data that may be required by remote application 2308 to complete a purchase transaction. In so doing, for example, mobile device 2302 may customize a payment message to remote application 2308 that includes only the filtered subset of data that is needed by remote application 2308 to complete the purchase transaction.

[0244] As per another example, mobile device 2302 may query payment card 2304 via contactless communication channel 2312 for only a subset of payment information that may be required by remote application

2308 to complete a purchase transaction. Accordingly, for example, a processor of payment card 2304 may receive the request and may only supply the requested payment information via contactless communication channel 2312 instead of communicating a complete magnetic stripe message.

[0245] FIG. 24 shows system 2400, which may include a mobile device 2402, a payment card 2404, a rewards card 2416, and items to be purchased 2410-2414. Mobile device 2402 may, for example, include a scanning device (e.g., a camera) that may be used to capture images (e.g., barcode images). Accordingly, for example, a user of mobile device 2402 may activate an application within mobile device 2402 that generates GUI 2408 and that activates a camera to capture barcode images. A processor of mobile device 2402 may, for example, analyze captured barcode images to extract information from the barcode images and construe the extracted information as data input. Accordingly, for example, a camera of mobile device 2402 may be used to scan barcodes of items that the user wishes to purchase and a processor of mobile device 2402 may analyze the scanned information to keep a running total of items selected for purchase. In so doing, for example, a user of mobile device 2402 may wander through a shopping market while scanning barcode labels of items for purchase (e.g., items 2410-2414).

[0246] Mobile device 2402 may access a network (e.g., a local Wi-Fi hotspot) within a shopping market to determine those items that may be offered at a discount to rewards members of the shopping market. Accordingly, for example, a user may scan barcode image 2418 of rewards card 2416 to obtain an instant credit

for discounted items for purchase. As per another example, rewards card 2416 may establish a contactless communication channel with mobile device 2402 so that rewards card 2416 may communicate rewards account information to mobile device 2402 via any one of a number of contactless communication mediums (e.g., RF, capacitive, audible, visible, electromagnetic, or magnetic communication mediums).

[0247] Once a user of mobile device 2402 finishes shopping, the user may present payment card 2404 to mobile device 2402 for payment. Accordingly, for example, contactless communication channel 2406 (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be created and payment information may be communicated from payment card 2404 to mobile device 2402 so that mobile device 2402 may complete the purchase transaction with a network entity (e.g., an issuer of payment card 2404).

[0248] FIG. 25 shows system 2500, which may include mobile device 2502 and payment card 2504. Mobile device 2502 may interact with a merchant establishment (e.g., a restaurant) to gain entry into a user's tab at the merchant's establishment (e.g., a food and alcohol bill generated by the restaurant). Accordingly, for example, a user may monitor each item on the bill, enter an additional amount into the bill (e.g., a tip), and then pay the bill all from the convenience of the user's mobile device 2502.

[0249] Interaction with a merchant establishment may be accomplished any number of ways. For example, mobile device 2502 may access a local Wi-Fi hotspot and may communicate information (e.g., an email address or text messaging address) to the merchant that identifies

a user of mobile device 2502. Accordingly, for example, a merchant may send a message (e.g., an email or text message) to the user-supplied address that may contain a link to the user's bill. A user may, for example, click on the link, enter a pass code to gain entry to the user's bill, and then monitor the bill being generated onto a display of mobile device 2502 via GUI 2508.

[0250] As per another example, mobile device 2502 may place a phone call to a merchant's phone number to establish a communication channel (e.g., a data call) between the merchant server and mobile device 2502. The merchant server may, for example, render GUI 2508 onto a display of mobile device 2502 so that a user of mobile device 2502 may directly interact with the merchant server.

[0251] GUI 2508 may be rendered onto a display of mobile device 2502 to allow a user to remotely interact with his or her bill. For example, a user's meal tab at a restaurant may be itemized by GUI 2508 and an alphanumeric entry box (e.g., box 2510) may allow the user to enter additional data (e.g., add a tip to the bill). A user may, for example, review a total to be charged, verify such a total, and then present payment card 2504 to mobile device 2502 to settle the total amount. In so doing, for example, contactless communication channel 2506 may receive payment information from payment card 2504 via any number of contactless communication mediums (e.g., RF, capacitive, audible, visible, electromagnetic, or magnetic communication mediums) and may communicate such payment information to a network entity (e.g., an

issuer of payment card 2504) to complete a purchase transaction for the total amount of the user's bill.

[0252] FIG. 26 shows flow charts for process sequences 2610-2650. Process sequence 2610 may, for example, execute a payment application on a mobile device (e.g., as in step 2611) to request a user of the mobile device to present a payment card to the mobile device. In step 2612, a user may present a payment card (e.g., tap a payment card onto a display of a mobile device) to begin a payment transaction. In step 2613, a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a payment card and a mobile device to communicate payment information from the payment card to the mobile device. In step 2614, a purchase may be completed by a mobile device by communicating received payment information to network entities to settle a payment transaction.

[0253] Process sequence 2620 may, for example, autonomously detect that a payment card is in a touching or a proximity relationship to a mobile device (e.g., as in step 2621). In step 2622, a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a payment card and a mobile device to communicate payment information from the payment card to the mobile device. In step 2623, a purchase may be completed by a mobile device by communicating received payment information to network entities to settle a payment transaction.

[0254] Step 2631 of sequence 2630 may include presenting a card to a mobile device. A card may, for

example, be a powered card or a non-powered card. In steps 2632 and 2633, a contactless communication channel may be established between a card and a mobile device and information may be exchanged between the card and the mobile device.

[0255] A card may, for example, include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. A card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device.

[0256] A card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a card as data communicated by a mobile device.

[0257] A card may, for example, include a light source (e.g., an LED) to form a contactless communication channel. Accordingly, for example, a card may emit varying light pulses from an LED that may

be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the card. A card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the card through a contactless communication channel. A mobile device may, for example, include sound emission capabilities that may be detected by a microphone of a card as data communicated by the mobile device through a contactless communication channel.

[0258] Step 2641 of sequence 2640 may include selecting items for purchase using a mobile device. A mobile device may, for example, include a scanning device (e.g., a camera) that may be used by a mobile device to capture images of barcodes that may be associated with items for purchase (e.g., grocery items in a grocery store). Accordingly, for example, a mobile device may collect images of barcodes and a processor of the mobile device may analyze the images to retrieve information (e.g., item description and cost) of each item scanned. Each item's description, cost and other information may, for example, be displayed on a GUI that may be generated by a processor and presented to a display of the mobile device as in step 2642. A payment card may, for example, be presented to the mobile device (e.g., as in step 2643) and payment information may be exchanged between the payment card and the mobile device (e.g., as in step 2644) via a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel). In step 2645, a mobile device may communicate received payment

information to network entities (e.g., a payment server and/or an issuer) to complete the transaction.

[0259] In step 2651 of sequence 2650, for example, a mobile device may remotely access an electronic bill. For example, a merchant (e.g., a restaurant) may provide access to a bill (e.g., a restaurant tab for food and beverages) to a patron of the merchant via that patron's mobile device. As per one example, a merchant may provide a link to a bill via a message (e.g., an email message or a text message) that may be sent by the merchant to the patron's mobile device or that may be sent by the patron's mobile device to the merchant. The patron may click on the link and may be taken to a website that may provide access to the patron's tab via a browser that may be executing on the patron's mobile device. As per another example, a data call between a patron's mobile device and a merchant may execute an application (e.g., locally on the patron's mobile device and/or remotely on a merchant's server) to allow a patron to review his or her bill.

[0260] Each item on the patron's bill may, for example, include a description, cost and other information and may be displayed on a GUI that may be generated by a processor and presented to a display of the mobile device as in step 2652. A payment card may, for example, be presented to the mobile device (e.g., as in step 2653) and payment information may be exchanged between the payment card and the mobile device (e.g., as in step 2654) via a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel). In step 2655, a mobile device may communicate received payment information to network

entities (e.g., a payment server and/or an issuer) to complete the transaction.

[0261] FIG. 27 shows mobile device 2700. Mobile device 2700 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, for example, mobile device 2700 may be operated in a mobile environment while a user of mobile device 2700 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 2700 may perform multiple functions simultaneously (e.g., a person may carry on a conversation while at the same time browsing and purchasing products on the internet).

[0262] Mobile device 2700 may include audio processing devices (e.g., microphone 2708 and speaker 2710). Accordingly, for example, mobile device 2700 may receive voice commands from a user via microphone 2708 and may process such commands to perform a function. For example, a user may place mobile device 2700 into a desired operational mode by speaking a command into microphone 2708 that is associated with the desired operational mode. In so doing, for example, mobile device 2700 may engage in hands-free operation by receiving voice commands via microphone 108 and performing functions associated with the received voice commands.

[0263] Mobile device 2700 may receive data input via microphone 2708. For example, a voice-band modem may generate signals in a voice-band frequency range that may be received by microphone 2708. A processor of mobile device 2700 may interpret the received audible

information as data signals and may process the data signals as, for example, data values and/or control data input.

[0264] Mobile device 2700 may include camera 2702. Camera 2702 may capture one or more frames of video data and store the video data within a memory of mobile device 2700. Accordingly, for example, a processor of mobile device 2700 may receive one or more frames of video information via camera 2702 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 2700 may receive optical information that is sensed by camera 2702 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 2700 as data values and/or control data.

[0265] Mobile device 2700 may include manual input interface 2712. Manual input interface 2712 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 2700 may enter information into mobile device 2700 via manual interface 2712 to cause a processor of mobile device 2700 to enter a particular mode of operation. Manual interface 2712 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile device 2700) during a particular mode of operation of mobile device 2700.

[0266] Mobile device 2700 may include display 2704. Display 2704 may provide visible information that may be utilized by a user during interaction with mobile device 2700. A portion or all of display 2704 may be touch sensitive such that objects making contact with display 2704 or objects coming within a proximity of display 2704 may be detected by a processor of mobile device 2700. Accordingly, for example, mobile wallet graphical user interface 2706 may be provided by display 2704 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, textual input boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 2700.

[0267] Display 2704 may, for example, display graphical objects that may interact with a user of mobile device 2700. Accordingly, for example, a virtual card (e.g., a virtual payment card) may be rendered onto display 2704 having interactive components associated with such a virtual payment card. In so doing, for example, a virtual payment card displayed by display 2704 may itself include a virtual user interface (e.g., one or more virtual buttons) that may be sensitive to touch or proximity. Such virtual buttons may be associated with a feature (e.g., one or more tracks of magnetic stripe information may be communicated by the mobile device when a button is activated). In so doing, for example, a feature activated on a virtual payment card displayed by display 2704 may cause mobile device 2700 to behave

like a payment card (e.g., one or more tracks of magnetic stripe information may be communicated by mobile device 2700 when a virtual button of a virtual payment card of display 2704 is activated).

[0268] FIG. 27 shows architecture 2750. User interface 2752 may, for example, be included within architecture 2750 to allow user interaction with architecture 2750. For example, a dedicated key pad or keyboard may be included within user interface 2752 to allow alphanumeric data entry into architecture 2750.

[0269] Architecture 2750 may include one or more displays 2754. Display 2754 may, for example, be touch-sensitive. Accordingly, for example, display 2754 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 2754. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of display 2754 may be detected by processor 2758 as alphanumeric data entry.

[0270] Alphanumeric entry boxes may, for example, be rendered onto display 2754. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 2752 and/or a virtual keypad rendered onto display 2754 to select alphanumeric characters to be placed within the alphanumeric entry box having a character position identified, for example, by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 2758 may receive alphanumeric characters as typed into a alphanumeric entry box of display 2754 and may use such alphanumeric characters as data input.

[0271] Display 2754 may, for example, render a virtual representation of a card (e.g., one or more virtual payment cards stored within memory 2760). Accordingly, for example, information (e.g., payment card number, cardholder name, bank logos and issuer identification) may be stored within memory 2760 and rendered onto display 2754 as a virtual representation of a card. In so doing, for example, virtual interactive objects (e.g., buttons, displays, light sources and light sensors) that may be associated with a virtual card on display 2754 may be utilized through interaction with display 2754 just as if the virtual card were physically present.

[0272] Display 2754 may, for example, provide data output from architecture 2750. For example, display 2754 may communicate data using a series of light pulses. Accordingly, for example, processor 2758 may cause one or more portions of display 2754 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 2754 via light pulses having varying characteristics. Display 2754 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0273] Architecture 2750 may include one or more transceivers 2756. Transceiver 2756 may communicate information to and/or may receive information from one or more devices. Transceiver 2756 may, for example, communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly,

for example, transceiver 2756 may allow a mobile device (e.g., mobile device 2700 of FIG. 27) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 2700 of FIG. 27) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 2756 may exchange information with one or more other mobile devices via one or more associated cellular stations.

[0274] Transceiver 2756 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 2756 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 2756 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 2700 of FIG. 27) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network.

[0275] Architecture 2750 may include contactless communication device 2762, which may communicate via

any one or more contactless communication methodologies, such as for example, near field communications (e.g., RFID), Bluetooth, touch simulation, light pulsing (e.g., via an LED), and electromagnetic data communication (e.g., via a dynamic magnetic stripe communications device). Accordingly, for example, contactless communication device 2762 may be compatible with any contactless device, such as for example, an RFID enabled payment card and a contactless reader (e.g., a magnetic stripe reader or an NFC reader).

[0276] A non-powered card may, for example, communicate with contactless communications device 2762. Contactless communication device 2762 may, for example, establish a carrier field (e.g., an RF field) that may be modulated by a device (e.g., an RFID tag) of a non-powered payment card. In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by contactless communications device 2762 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 2762 by modulating the RF field produced by contactless communications device 2762.

[0277] A powered card may, for example, communicate with contactless communication device 2762. A powered card may, for example, include a processor, a battery, a memory, wireless communications devices (e.g., a dynamic magnetic stripe communications device or RFID) and other electronics (e.g., buttons, displays, light sources and light sensors) that may allow a user to interact with the powered card to perform one or more functions. Accordingly, for example, a powered card

may be used to communicate specific information to contactless communication device 2762 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 2762 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications.

[0278] Contactless communication device 2762 may receive variable data sets from a powered card based upon, for example, manual input provided to a powered card. For example, a button associated with an on-line purchase may be pressed on the powered card that causes a variable data set (e.g., account number and expiration date) to be communicated from the powered card to contactless communication device 2762.

[0279] Discretionary data may, for example, be communicated by a powered card based upon which button was pressed on the powered card. In so doing, for example, a security code (e.g., "111") may be communicated within a discretionary data field when a button associated with a particular feature (e.g., pay with credit) is pressed on the powered card. As per another example, a different security code (e.g., "222") may be communicated within a discretionary data field when a button associated with a different feature (e.g., pay with debit) is pressed on the powered card. Accordingly, for example, processor 2758 may identify what type of device may be in communication with contactless communication device 2762 by analyzing the

data communicated to contactless communication device 2762.

[0280] Architecture 2750 may include memory 2760 and/or processor 2758 may include internal memory. Accordingly, for example, application code may be stored within memory 2760 and/or processor 2758 and executed by processor 2758 in support of functions performed by architecture 2750. For example, an application (e.g., a mobile wallet graphical user interface) may be executed by architecture 2750 and displayed onto display 2754, which may be used to interact with a user of a mobile device (e.g., mobile device 2700 of FIG. 27). Persons skilled in the art will appreciate that executable application code may be communicated to architecture 2750 via any one or more interfaces of architecture 2750 (e.g., user interface 2752, display 2754, transceiver 2756, and/or contactless communication device 2762).

[0281] Application data (e.g., virtual payment card data) may be stored within memory 2760 and accessed by processor 2758 during operation. For example, payment card data may be stored within memory 2760 and recalled by processor 2758 during a financial transaction being conducted by a mobile device (e.g., mobile device 2700 of FIG. 27). Once recalled, processor 2758 may communicate the payment card data via transceiver 2756 and/or contactless communication device 2762 to complete a financial transaction.

[0282] FIG. 28 shows network topology 2800 that may include, for example, mobile wallet 2802 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile wallet 2802 may, for example, include a contactless interface

that may initiate, sustain, and/or terminate a communication channel between a contactless device (e.g., an RFID enabled payment card) and mobile wallet 2802. A contactless device and mobile wallet 2802 may communicate using any number of contactless mediums, which may include for example, visible, audible, capacitive, electromagnetic, magnetic, and/or RF mediums.

[0283] Mobile wallet 2802 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 2812 and/or payment network 2814) and/or one or more wireless networks (e.g., mobile network 2810). Mobile wallet 2802 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile wallet 2802 to communicate information (e.g., voice and data) to cellular network access infrastructure 2806 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 2806 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0284] Mobile wallet 2802 may, for example, communicate with wireless access point 2808 over a wireless interface (e.g., a Bluetooth interface or a Wi-Fi interface). Accordingly, for example, mobile wallet 2802 may access one or more wired networks (e.g., IP network 2812 and/or payment network 2814) and/or one or more wireless networks (e.g., mobile

network 2810) without the need to first gain access to cellular network access infrastructure 2806.

[0285] Any contactless device (e.g., a powered payment card or a non-powered payment card) may, for example, communicate with mobile wallet 2802 via a contactless medium. Accordingly, for example, payment information (e.g., a payment account number and a card expiration date) may be communicated from a contactless device to mobile wallet 2802. In so doing, for example, items for purchase on IP network 2812 (e.g., the internet) may be accessed by a browser of mobile wallet 2802 via an access point (e.g., wireless access point 2808 or cellular network access infrastructure 2806). Mobile wallet 2802 may, for example, complete a purchase transaction by first obtaining required payment information from a contactless device, storing such payment information and communicating such payment information to network entities (e.g., payment server 2816 and/or issuer 2820).

[0286] Payment server 2816 may, for example, contact issuer 2820 via a network (e.g., payment network 2814) with payment information received from mobile wallet 2802 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile wallet 2802 via any one or more delivery options (e.g., via a short messaging service of mobile network 2810 or an email delivery service of IP network 2812). Mobile wallet 2802 may allow a user to associate purchase categories (e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile wallet so that the user may receive a more detailed accounting of his or her expenditures on his or her receipt. Accordingly,

for example, a user may enjoy a higher degree of integration such that a user may customize a level of detail provided on a receipt via mobile wallet 2802.

[0287] A payment receipt may, for example, be provided to mobile wallet 2802 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile wallet 2802 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0288] A mobile wallet (e.g., mobile wallet 2824) may, for example, include a contactless communication device (e.g., an RFID) that may initiate, sustain, and/or terminate contactless communication channel 228 with merchant terminal 2818. Accordingly, for example, mobile wallet 2824 may communicate payment information to merchant terminal 2818 to complete a financial transaction. In so doing, for example, mobile wallet 2824 may first receive payment information via a contactless communication channel from one or more contactless devices (e.g., a non-powered card), store the received payment information within a memory of mobile wallet 2824, and forward the payment information onto merchant terminal 2818 to complete a financial transaction. Accordingly, for example, payment information may be recalled from memory within mobile wallet 2824, optionally authenticated and authorized by a user of mobile wallet 2824 and communicated to merchant terminal 2818 via contactless communication channel 2828 to complete a financial transaction using merchant terminal 2818. An electronic receipt may, for example, be generated by merchant terminal 2818 and communicated to mobile wallet 2824 via contactless communication channel 2828.

[0289] FIG. 29 shows system 2900, which may include mobile wallet 2902 and payment card 2904. Mobile wallet 2902 may, for example, be a laptop computer, a PDA, a mobile telephonic device (e.g., a smartphone), an MP3 player, a GPS, or any other mobile device. Display 2908 may be a touch-sensitive display (e.g., sensitive to a change in capacitance). Payment card 2904 may, for example, be a powered payment card or a non-powered payment card.

[0290] Mobile wallet 2902 and payment card 2904 may each include a contactless communication device (e.g., RFID) that may communicate via a contactless communication channel that may be formed between mobile wallet 2902 and payment card 2904 after coming into proximity to one another. Payment card 2904 may, for example, be tapped onto display 2908 of mobile wallet 2902 to establish a proximity relationship that forms a communication channel between payment card 2904 and mobile wallet 2902. As per another example, payment card 2904 may be brought within a proximity distance (e.g., up to two inches) of mobile wallet 2902 to establish a contactless communication channel between mobile wallet 2902 and payment card 2904.

[0291] A processor of mobile wallet 2902 may, for example, execute application code that may generate a graphical user interface (GUI) onto display 2908 of mobile wallet 2902. Message 2906 of such a GUI may invite a user of mobile wallet 2902 to begin storage of card information (e.g., payment card information) by tapping one or more cards (e.g., one or more payment cards) against display 2908. As per another example, by tapping a card (e.g., payment card 2904) against mobile wallet 2902, a processor of mobile wallet 2902

may autonomously determine that card information associated with the tapped card is to be stored within a memory of mobile wallet 2902 and a processor of mobile wallet 2902 may then generate a mobile wallet GUI onto display 2908 to autonomously download the card information and engage a user of mobile wallet 2902 to administer any other activities that may be associated with such an information download.

[0292] A processor of mobile wallet 2902 may, for example, autonomously determine a type of card that may be tapped against it. For example, a processor of mobile wallet 2902 may receive payment card data that may be indicative of a non-powered payment card (e.g., payment card data received from a non-powered card may not provide a security code associated with the card). As per another example, a processor of mobile wallet 2902 may receive data that may be indicative of a powered card (e.g., payment card data received may contain a dynamically generated security code). Payment card data received from a powered card may, for example, include a dynamic security code that may change depending upon a type of transaction being conducted (e.g., debit or credit transaction).

[0293] As per another example, payment card 2904 may be a powered payment card that may include electronics to simulate a human touch (e.g., payment card 2904 may generate a change in capacitance that may be sensed by display 2908). Through a series of simulated touches, payment card 2904 may communicate a series of data bits to display 2908, which may then be processed by a processor of mobile wallet 2902. In so doing, for example, a contactless communication channel may be established where data is transferred from payment card

2904 to mobile wallet 2902 via a series of simulated touches.

[0294] Payment card 2904 may, for example, include a light sensor. Accordingly, for example, payment card 2904 may be sensitive to light pulses generated within a region of display 2908. The light sensor of payment card 2904 may receive a series of light pulses, which may be construed by a processor of payment card 2904 as data generated by mobile wallet 2902. In so doing, for example, payment card 2904 may receive an optical data stream represented by a series of light pulses generated by display 2908. As such, a two-way communication channel may be formed, where simulated touches may generate a data stream from payment card 2904 to mobile wallet 2902 and light pulses may generate a data stream from mobile device 2902 to payment card 2904.

[0295] FIG. 30 shows GUI 3000, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3000 may, for example, provide a summary information screen that provides virtual card 3002 and associated identifying information. Virtual card 3002, for example, may be a virtual representation of a physical card that may have been tapped against a display of a mobile device to form a contactless communication channel between the physical card and a mobile device.

[0296] Card (e.g., payment card) information (e.g., track 1 and track 2 magnetic stripe data) may be communicated to the mobile device via a contactless communication channel and such information may be displayed within virtual card 3002 as summary information that may be associated with the physical

payment card. A payment card number communicated to a mobile device within a magnetic stripe message may, for example, include issuer identification as well as an issuing network identifier. Accordingly, for example, a processor of a mobile device may analyze the payment card number received from a physical payment card and may render a portion or all of the identifying information associated with the payment card number onto virtual card 3002. In so doing, for example, issuer identification 3004 as well as a logo representative of an issuing network identifier may be rendered onto virtual card 3002. Additionally, a portion or all of payment card number 3006 as well as cardholder's information (e.g., cardholder's name 3008) may be rendered onto virtual card 3002.

[0297] A portion or all of the card information received from a physical card may be stored within a memory of a mobile device. Alternately, for example, a portion or all of the card information received from a physical card may be collected by a mobile device and communicated by the mobile device to a remote server for storage and/or validation purposes. In so doing, for example, instead of storing payment card information within a memory of a mobile device, card identification 3010 may, for example, be stored within a mobile device and used as an index identifier to look up payment information that may be stored within a remote server. A processor of a mobile device may generate card identification 3010 and may display card identification 3010 within an alphanumeric entry box. In so doing, for example, a user of a mobile device may either accept, or change, card identification 3010 to a value that may later be used to remind the user of

which physical payment card is associated with card identification 3010 and to recall payment information associated with card identification 3010 that may be remotely stored.

[0298] FIG. 31 shows GUI 3100, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3100 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. GUI 3100 may, for example, challenge a user of the mobile device to enter a PIN that may be associated with a payment card (e.g., VISA credit 3102) that was previously presented to the mobile device so that payment information may be uploaded from the payment card to the mobile device via a contactless communication channel generated between the payment card and the mobile device. GUI 3100 may, for example, generate virtual pin pad 3106 that may include touch-sensitive buttons having alphanumeric indicia associated with each button. A user may touch one or more buttons of pin pad 3106 that may correspond to respective characters of a PIN and an indication of the user's selection may appear within area 3104. Characters displayed within area 3104 may, for example, be hidden for security purposes.

[0299] Activation of virtual button 3108 may, for example, cause a processor of a mobile device to compare a PIN entered by a user of the mobile device to a PIN that may be associated with the payment card presented to the mobile device for storage. The PIN may, for example, be stored within protected memory of the mobile device, so that a processor of the mobile device may locally determine the validity of the PIN

entered. Alternately, for example, the mobile device may communicate the PIN to, for example, the issuing bank for a remote validation of the PIN entered. Persons skilled in the art will appreciate that a user interface (e.g., a keypad or keyboard) of a mobile device may be used instead of virtual pin pad 3106 to enter the one or more characters of a PIN.

[0300] Upon validation that the correct PIN was entered, virtual card 3110 may be displayed. In particular, for example, account number 3112 may be fully populated within virtual card 3110 to indicate to a user of the mobile device that the PIN was correctly entered and to allow the user to compare account number 3112 against an account number printed on the physical payment card of which virtual card 3110 is a representation. Persons skilled in the art will appreciate that virtual payment cards may be stored within a mobile wallet without first requiring a user to validate the payment card using a PIN entry. An alternate form of validation (e.g., a security code) may, for example, be required for validation. As per another example, no validation may be required to store a virtual payment card onto a mobile wallet.

[0301] FIG. 32 shows system 3200, which may include mobile wallet 3202 and card 3206. Card 3206 may, for example, be a powered card (e.g., a powered payment card). Accordingly, for example, card 3206 may include a processor, display 3212, a battery, manual input interfaces (e.g., buttons 3208 and 3210) and other electronic components (e.g., a light source, a light sensor and a touch simulator). A user of powered card 3206 may, for example, interact with card 3206 to

select the information that may be communicated to mobile wallet 3202 from card 3206.

[0302] A user may, for example, press button 3208 and then tap card 3206 against display 3204 of mobile wallet 3202 to generate a contactless communication channel (an RFID communication channel) between card 3206 and mobile wallet 3202. Accordingly, for example, card 3206 may communicate payment information (e.g., one, two and/or three tracks of magnetic stripe data) that may be associated with a feature selected by pressing button 3208. In so doing, for example, card 3206 may communicate information (e.g., within a discretionary data field) associated with a selected feature (e.g., a VISA debit payment feature).

[0303] FIG. 33 shows GUI 3300, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3300 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. GUI 3300 may, for example, render virtual card 3310 so that a user of the mobile device may compare information 3312 and 3314 to information that the user intended to communicate to the mobile device.

[0304] Accordingly, for example, a user may have pressed a button on a powered payment card associated with a debit pay feature and may have communicated the debit pay feature (e.g., within a discretionary data field of a magnetic stripe message) to a mobile device via a contactless communication channel that may have been created between the powered payment card and the mobile device. In so doing, for example, a processor of a mobile device may analyze the debit pay feature received from the powered payment card and may render

an indication (e.g., "Pay Now" identifier 3314) onto virtual card 3310 to indicate that virtual payment card 3310 has been stored within the mobile device such that when used by a user of the mobile device to complete a payment transaction, authorizes an immediate deduction of funds from the user's payment account. Alphanumeric entry box 3316 may, for example, allow the user to tag stored virtual card 3310 with a card identifier that reminds the user of the debit functionality associated with virtual card 3310.

[0305] FIG. 34 shows GUI 3400, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3400 may, for example, render virtual card 3410 to allow a user to verify information previously communicated to a mobile device via a contactless communication channel that may be generated between a powered payment card and the mobile device. A user of a mobile device may, for example, press a button on a powered payment card that may be associated with a credit pay feature and may communicate the credit pay feature along with other payment information (e.g., payment account number 3412 and expiration date) via a contactless communication channel to the mobile device.

[0306] A processor of a mobile device may, for example, analyze information received from a powered payment card (e.g., information received via a discretionary data field) and may determine that payment information received from the powered payment card may be associated with a credit feature (e.g., "Pay Later" feature 3414). Accordingly, for example, a processor of a mobile device may use identifier 3414 of

virtual card 3410 to signify such a credit payment feature.

[0307] Virtual card identifier 3416 may, for example, be an editable card identifier to allow a user of a mobile device to store and recall virtual card 3410 to/from a memory of a mobile device. Card identifier 3416 may, for example, be used by a mobile device to access virtual card 3410 from a remote location (e.g., a remote server) such that the mobile device need not store sensitive information that may be associated with virtual card 3410 within the mobile device.

[0308] GUI 3400 may, for example, allow an additional card to be associated with virtual card 3410. A rewards card may, for example, be associated with a credit account that may be associated with virtual card 3410. Accordingly, for example, rewards card information may be communicated to a mobile device by tapping the rewards card against portion 3418 to generate a contactless communication channel (e.g., an RFID communication channel) between the rewards card and the mobile device. As per another example, an identification card (e.g., a driver's license) may be associated with virtual card 3410. Accordingly, for example, identifying information (e.g., date of birth and a picture) associated with the holder of the identification card may be communicated to a mobile device and stored within the mobile device. In so doing, for example, stored identification information may be recalled from a memory of the mobile device to provide authentication information while completing a purchase transaction using the mobile device.

[0309] A user may, for example, select option 3420 to allow card information to be scanned into a mobile device using a scanning device (e.g., a camera) of the mobile device. Accordingly, for example, a card (e.g., a driver's license) may be scanned into a mobile device by selecting radio button 3420 and holding the driver's license in front of the mobile device while a snapshot of the driver's license is taken by a camera of the mobile device and stored in a memory location of the mobile device. A mobile device may alternately, for example, access identifying information (e.g., name, address, phone number, and picture) from a database (e.g., a motor vehicle database) that may be accessible from a network. Such information may be rendered onto a virtual identification card (e.g., a driver's license) that may be stored within a mobile device. In so doing, for example, user identification data may be recalled from a memory of a mobile device and rendered onto a display of the mobile device, so that a merchant may verify the validity of the user identification data when virtual card 3410 is used to complete a purchase transaction in the presence of the merchant.

[0310] Card information may be communicated via programming portion 3422. A powered card may, for example, provide touch simulation electronics and a light sensor such that when the powered card is placed against portion 3422, a two-way contactless communication channel may be created. Accordingly, for example, information may be communicated from the powered card to the mobile device through a series of touch simulations generated by the powered card and sensed by a portion within portion 3422 that is touch sensitive. In so doing, for example, a processor of a

mobile device may construe a series of touch simulations as a series of data bits communicated by a powered card that may be indicative of information associated with the powered card. GUI 3400 may, for example, provide a series of light pulses within portion 3422 that may be received by a light sensor of the powered card and construed by a processor of the powered card as data communicated by the mobile device.

[0311] FIG. 35 shows GUI 3500 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3500 may, for example, include upload area 3502 as generated by a processor of a mobile device. Upload area 3502 may, for example, include one or more data exchange areas (e.g., data exchange areas 3504 and 3506). Icon 3504 may, for example, be generated by GUI 3500 within an area of a display of a mobile device that may be sensitive to touch (e.g., an area that may be sensitive to a capacitance change). Area 3506 may, for example, be generated by GUI 3500 within an area of a display of a mobile device that may generate pulses of light.

[0312] Information associated with a powered payment card may be uploaded for use by a mobile device by exchanging data with the powered payment card via data exchange areas 3504 and 3506. For example, a powered payment card may be pressed against upload area 3502 so that a touch simulation device of the powered payment card aligns with data exchange area 3504 and a light sensing device of the powered payment card aligns with data exchange area 3506. Accordingly, for example, the powered payment card may communicate information to a processor of a mobile device by simulating a series of touches in data exchange area 3504 and data may be

communicated to the powered payment card by a processor of the mobile device by generating a series of light pulses in data exchange area 3506. In so doing, for example, a mobile device and a powered payment card may exchange information so that payment card information may be stored within the mobile device.

[0313] Once payment card information is uploaded into a mobile device, GUI 3500 of the mobile device may display a summary of the uploaded information in validation area 3510. Accordingly, for example, one, two or three tracks of magnetic stripe information may be uploaded from a payment card into a mobile device via data exchange area 3504 of upload area 3502. A portion or all of the uploaded data may, for example, be rendered within validation area 3510, so that a user of the mobile device may validate that the correct payment card information was uploaded and stored within the mobile device.

[0314] FIG. 36 shows GUI 3600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3600 may, for example, render virtual card 3610 and may display a portion of information that may be associated with virtual card 3610. Accordingly, for example, a payment card (e.g., a gift card) may be brought within a proximity or touch relationship with a mobile device such that a contactless communication channel may be generated between the payment card and the mobile device. In so doing, for example, payment account information may be communicated from the payment card to the mobile device and a portion or all of the payment card information may be rendered onto virtual card 3610.

[0315] A user of a mobile device may, for example, customize a visual appearance of virtual card 3610 by utilizing any number of graphical user interface objects (e.g., list 3604 and alphanumeric input box 3612) that may be rendered by GUI 3600. A user may, for example, drag-and-drop logos from list 3604 onto virtual card 3610 to more clearly identify virtual card 3610. Accordingly, for example, a user may identify virtual card 3610 as a gift card (e.g., a Walmart gift card), using drag-and-drop operation 3608, having a particular network brand (e.g., a VISA network brand), using drag-and-drop operation 3606. A user may, for example, annotate virtual card 3610 using alphanumeric input box 3612 with any identifying information that may be useful to the user (e.g., information that may be used to recall virtual card 3610 from a memory of a mobile device).

[0316] A mobile device may, for example, disallow certain customizations that may conflict with virtual card 3610. Accordingly, for example, a mobile device may prevent a user from applying a different network logo than was previously communicated by a physical card to the mobile device. In so doing, for example, a mobile device may prevent a user from customizing virtual card 3610 as, for example, a M/C network brand, when a payment card number previously communicated from a payment card to a mobile device indicated that the payment card was, for example, a payment card having a VISA network brand.

[0317] A credit balance, for example, may be communicated by a gift card to a mobile device via a contactless communication channel generated between the gift card and the mobile device and may be displayed as

account balance 3614 to represent an amount of credit that may be remaining on virtual card 3614. Virtual card 3610 may, for example, be used by a mobile device to complete a purchase transaction in which payment card information associated with virtual card 3610 may be communicated to a merchant terminal (e.g., communicated via an RFID communication channel) and an amount of the purchase may be communicated from the merchant terminal to the mobile device. Accordingly, for example, account balance 3614 may be updated (e.g., reduced) by the amount of the purchase and displayed so that a user of the mobile device may be updated as to an amount of credit remaining on virtual card 3610.

[0318] A user of a mobile device may, for example, purchase additional credit to be added to virtual card 3610. Accordingly, for example, account balance 3614 may be updated (e.g., increased) when an amount of credit is added to virtual card 3610. In so doing, for example, an amount of credit added to virtual card 3610 may be communicated (e.g., communicated via an RFID communication channel) to a mobile device by a merchant terminal and updated via account balance 3614 so that a user of the mobile device may receive up-to-date information relating to a credit balance that may be available on virtual card 3610. As per an example, a user may recall a virtual payment card from a memory of a mobile device, activate the payment card for use, and use the mobile device to purchase additional credit on virtual card 3610 using the activated payment card as the payment vehicle.

[0319] FIG. 37 shows GUI 3700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3700 may, for

example, provide a visual representation of all virtual cards that may be stored within a memory of a mobile device (or within a remote server) and may display each virtual card within one or more categories that may be associated with each virtual card. A processor of a mobile device may, for example, analyze information received from a physical card via a contactless communication channel (e.g., an RFID, electromagnetic, visible, audible, capacitive, or magnetic communication channel) to determine a card category that may be associated with the corresponding virtual card.

[0320] An account number may, for example, be communicated by a card to a processor of a mobile device that may identify the card as a particular card type (e.g., bank card, rewards card, identification card, healthcare card, travel card or airline card). Accordingly, for example, each virtual card stored within a memory of a mobile device may be assigned a category index by a processor of the mobile device and may then be rendered onto GUI 3700 in accordance with the category index assigned. As per another example, a user of a mobile device may assign a category index (e.g., card identification) to a virtual card after information associated with a corresponding physical card is communicated to the mobile device via a contactless communication channel.

[0321] One or more payment cards, for example, may be rendered onto GUI 3700 and each payment card may be aligned within category 3706. An ordering of each payment card in category 3706 may, for example, be established by a user of a mobile device via sort options 3702. A mobile device may, for example, maintain statistics (e.g., number of times each virtual

payment card is recalled from a memory of a mobile device and used to complete a purchase transaction via the mobile device). Accordingly, for example, upon selection of one of sort options 3702 (e.g., Most used), a processor of a mobile device may recall usage statistics that may be associated with each virtual payment card stored within a memory of a mobile device and may display each virtual payment card within category 3706 onto GUI 3700 in accordance with such usage statistics (e.g., the top virtual payment card displayed within category 3706 may have the most usages of all virtual payment cards stored within a memory of the mobile device).

[0322] A mobile device may, for example, maintain other information associated with virtual payment cards of category 3706. Accordingly, for example, a mobile device may access network devices (e.g., issuer servers) associated with each virtual payment card stored within the mobile device. In so doing, for example, a mobile device may collect information (e.g., credit limit and credit available) associated with each virtual payment card stored within a memory of the mobile device and may display each virtual payment card on GUI 3700 in accordance with sort options 3702 (e.g., the top card displayed within category 3706 may have the highest credit limit or may have the most credit available).

[0323] Category 3708 may, for example, be associated with all virtual gift cards that may be stored within a memory of a mobile device (or remote server). Information associated with each virtual gift card may, for example, include a merchant identifier, a merchant type identifier, and an amount of credit available.

Accordingly, for example, a user may select one of sort options 3704 (e.g., Most credit available) to display a list of virtual gift cards within category 3708 in a descending order, where the top virtual gift card of category 3708 may have the highest credit available.

[0324] A mobile device may, for example, be a locating device (e.g., a GPS) or may, for example, include location determination electronics. Accordingly, for example, a mobile device may determine its own location and may determine whether its location corresponds with a location of a merchant's place of business that may be associated with a virtual gift card of category 3708. In so doing, for example, a mobile device may determine that its location is within a Walmart store and if, for example, sort options 3704 is selected to "Location", then a processor of the mobile device may re-order the virtual gift cards of category 3706 such that a Walmart virtual gift card is displayed as the top card in the stack. Accordingly, for example, the Walmart virtual gift card may be conveniently located within GUI 3700 for selection by a user of a mobile device to use during a purchase transaction conducted between a contactless communication channel formed between the mobile device and a merchant terminal at the Walmart store.

[0325] Virtual cards may, for example, be autonomously sorted across categories depending upon a virtual card placement that may exist in a particular category. A virtual payment card may, for example, be selected to occupy a top card placement within category 3706. A virtual rewards card may, for example, be associated with the virtual payment card selected for top placement in category 3706. Accordingly, for

example, the associated virtual rewards card may be selected for top placement within category 3708 based upon its association with the virtual payment card selected for top placement within category 3706. As per another example, a virtual identification card (e.g., a virtual driver's license card) may be selected for top placement within category 3710 based upon its general association with any virtual payment card selected for top placement within category 3706 or its general association with any virtual gift card selected for top placement within category 3708.

[0326] FIG. 38 shows GUI 3800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3800 may, for example, provide a visual representation of all virtual cards that may be stored within a mobile device (or remote server) and may display each virtual card within one or more categories that may be associated with each virtual card. GUI 3800 may, for example, be rendered onto a touch-sensitive display of a mobile device, such that by touching a location of the display that corresponds to a location of a virtual card, that card may be selected for use. Accordingly, for example, a user may touch any area within virtual card 3804 to activate virtual card 3804 for use. In so doing, for example, indicia may be provided on GUI 3800 to indicate that virtual card 3804 has been selected for use (e.g., an outline of virtual card 3804 may be highlighted) and a copy of virtual card 3804 (e.g., virtual card 3802) may be rendered onto GUI 3800 to indicate to a user of the mobile device that virtual card 3802 has been selected for use.

[0327] FIG. 39 shows GUI 3900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3900 may, for example, allow a user of a mobile device to select (e.g., touch) one of the virtual cards rendered onto GUI 3900. Once selected, the virtual card may rise from its position (e.g., virtual card 3904 may be elevated above the neighboring virtual cards in category 3902) and may be highlighted to indicate the selection to a user. Once elevated, the selected virtual card (e.g., card 3904) may display relevant information associated with the virtual card (e.g., information displayed on a front surface of the virtual card such as account number and merchant affiliation) so that a user may verify that the selected virtual card is the virtual card that the user wishes to use. If the selected virtual card is not the virtual card that the user wishes to use, then the user may deselect (e.g., touch) the selected virtual card and the virtual card may fall back within the ranks of its neighboring virtual cards. If the selected virtual card is the virtual card that a user wishes to use, then the user may confirm (e.g., touch the selected virtual card twice) that the selected card is the desired virtual card for use.

[0328] FIG. 40 shows GUI 4000 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4000 may, for example, allow a user of a mobile device to use selected virtual card 4002 in some manner. A user may, for example, wish to complete a purchase transaction using the mobile device and selected virtual card 4004. Accordingly, for example, upon selection of option

4004, information associated with selected virtual card 4002 may be communicated from a mobile device to, for example, a merchant terminal to complete a purchase transaction. In so doing, for example, a contactless communication channel (e.g., an RFID communication channel) may be formed between the mobile device and the merchant terminal and payment information (e.g., payment account number and expiration date) may be communicated from the mobile device to the merchant terminal via the contactless communication channel. As per another example, other information (e.g., one, two, or three tracks of magnetic stripe information) that may be associated with virtual card 4002 may be communicated by the mobile device to the merchant terminal when the mobile device detects the presence of an RFID communication channel formed between the mobile device and the merchant terminal.

[0329] A mobile device may, for example, request electronic receipts to be delivered to the mobile device after purchase transactions are completed. Accordingly, for example, receipts may be delivered to the mobile device via an electronic delivery method (e.g., text messaging or email) and may be stored within a memory of the mobile device for future use. In so doing, for example, a user may select option 4006 to view a list of one or more receipts that may be associated with purchases conducted via the mobile device and virtual card 4002.

[0330] A mobile device may, for example, request electronic bank statements to be delivered to the mobile device at the end of each billing cycle of virtual card 4002. Alternately, for example, a mobile device may access a network entity (e.g., an issuer's

server) to retrieve bank statement information that may be associated with virtual card 4002. Accordingly, for example, a user of a mobile device may review any and all bank statements associated with virtual card 4002 that a user's mobile device may have collected via its network access capabilities (e.g., a wireless access point or cellular network access infrastructure).

[0331] A mobile device may, for example, allow virtual card 4002 to be associated with one or more virtual cards stored within a memory of the mobile device (or remote server). For example, virtual card 4002 may be associated with one or more cards (e.g., a rewards card and a driver's license) and a user of a mobile device may view such associations using a GUI of the mobile device.

[0332] A mobile device may, for example, allow virtual card 4002 to be associated with one or more virtual cards that may be stored within a memory of another mobile device and/or may allow virtual card 4002 to be associated with one or more physical cards not stored within any mobile device. Virtual card 4002 may, for example, be one of many (e.g., two) cards issued against the same general account (e.g., a husband and wife joint charge account). Accordingly, for example, a mobile device may recognize that virtual card 4002 is one of a pair of cards associated with such a joint account and may provide information to the user of the mobile device about such associations.

[0333] FIG. 41 shows system 4100, which may include a mobile device (e.g., mobile wallet 4102), merchant terminal 4106 and GUI 4108 that may be executed by a processor of mobile wallet 4102. A user of mobile wallet 4102 may recall a virtual card (e.g., a virtual

payment card) from a memory of mobile wallet 4102 (or from a remote server) and use mobile wallet 4102 to communicate payment information associated with the virtual payment card to a merchant terminal. Accordingly, for example, a user of mobile wallet 4102 may have selected a virtual payment account from within a memory of mobile wallet 4102 (or remote server) to complete a payment transaction.

[0334] Once mobile wallet 4102 is brought within a communication distance (e.g., within approximately 2 inches) of merchant terminal 4106, a contactless communication channel (e.g., RFID communication channel 4104) may be generated between mobile wallet 4102 and merchant terminal 4106. Payment information associated with a virtual payment card selected by a user of mobile wallet 4102 may, for example, be autonomously communicated by a processor of mobile wallet 4102 to merchant terminal 4106 via contactless communication channel 4104 once a presence of merchant terminal 4106 is detected by the processor of mobile wallet 4102.

[0335] Contactless communication channel 4104 may, for example, be a two-way communication channel. Accordingly, for example, merchant terminal 4106 may communicate information to mobile wallet 4102 via contactless communication channel 4104. In so doing, for example, merchant terminal 4106 may communicate a total sale amount to mobile wallet 4102 and may wait for a user of mobile wallet 4102 to acknowledge that the total sale amount is correct (e.g., a user of mobile wallet 4102 may press an acknowledgment key that causes mobile wallet 4102 to communicate a confirmation message to merchant terminal via contactless communication channel 4104). Further communication

from merchant terminal 4106 may query mobile wallet 4102 as to whether a user of mobile wallet 4102 requires cash back.

[0336] Once a purchase transaction is completed, a user of mobile wallet 4102 may request a receipt to be delivered to mobile wallet 4102 via any one of a number of mediums. A user may, for example, request that a receipt be delivered to mobile wallet 4102 at a later time (e.g., receipt queued for delivery at a later time via text messaging or email). A user may, for example, request that a receipt be delivered to mobile wallet 4102 immediately. Accordingly, for example, an electronic receipt may be generated by merchant terminal 4106 and communicated to mobile wallet 4102 via contactless communication channel 4104.

[0337] An application executing on a mobile device (e.g., a receipt handler application associated with GUI 4108) may have its own address. Accordingly, for example, the receipt handler's address may be well known within a network (e.g., a payment network), such that a server (e.g., an email server associated with a merchant's payment server) may email an electronic receipt directly to the receipt handler application that may be running on the mobile device. In so doing, for example, one or more applications running on a mobile device may have well known addresses (e.g., email addresses and multimedia message addresses) associated with them, so that the applications may directly communicate with network entities to autonomously provide a user of the mobile device with up-to-date and valuable information.

[0338] FIG. 42 shows system 4200, which may include a mobile device (e.g., mobile wallet 4202), merchant

terminal 4212 and GUI 4204 that may be executed by a processor of mobile wallet 4202. Mobile wallet 4202 may, for example, complete a purchase transaction with merchant terminal 4212 by exchanging payment information with merchant terminal 4212 via a contactless communication channel (e.g., RFID communication channel 4214). Merchant terminal 4212 may, for example, communicate electronic receipt 4206 to mobile wallet 4202 after a purchase transaction completes. Electronic receipt 4206 may, for example, be displayed by a processor of mobile wallet 4202 onto GUI 4204 so that a user of mobile wallet 4202 may view electronic receipt 4206 and may execute certain options that may be associated with electronic receipt 4206.

[0339] Mobile wallet 4202 may, for example, allow a user of mobile wallet 4202 to annotate electronic receipt 4206 with a note that may be entered into alphanumeric entry box 4208. Mobile wallet 4202 may, for example, allow electronic receipt 4206 to be associated with a virtual card (e.g., virtual payment card VISA 3456 that was used to complete the purchase transaction) stored within a memory of mobile wallet 1602.

[0340] FIG. 43 shows GUI 4300 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4300 may, for example, allow a user of a mobile device to view receipts that may be associated with a selected virtual card. Accordingly, for example, a user of a mobile device may select a virtual card (e.g., virtual payment card 4302) and may view a summary of receipts that may be associated with virtual payment card 4302. In so doing, for example, a user may select summary receipt

4304 (e.g., by touching portion 4304 on GUI 4300) and a processor of the mobile device may retrieve details of summary receipt 4304 from a memory of the mobile device and display them in receipt detail area 4306.

[0341] FIG. 44 shows GUI 4400 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4400 may, for example, allow a user of a mobile device to view virtual cards stored within a memory of the mobile device (or remote server) that may be associated with a selected virtual card. Accordingly, for example, selected virtual card 4402 may have an association with virtual rewards card 4404 and selected virtual card 4402 may have an association with virtual identification card 4406.

[0342] A mobile device may, for example, access a user's rewards account by accessing a network entity (e.g., an issuer's server) to determine information associated with the rewards account (e.g., number of rewards points earned). A mobile device may, for example, access the network entity on a regularly scheduled basis and store the retrieved rewards account information within a memory location of the mobile device. A mobile device may, for example, access the network entity only upon demand to retrieve rewards account information and may only display the retrieved rewards account information without storing the retrieved rewards account information.

[0343] GUI 4400 may, for example, allow a user to obtain further information that may be associated with virtual cards 4404 and/or 4406. A user may, for example, touch a display of a mobile device in the vicinity of virtual card 4404 to obtain other

information (e.g., a rewards point balance) associated with virtual card 4404. Accordingly, for example, a user may obtain a rewards points total that may be associated with virtual card 4404 and may touch virtual card 4404 again to conduct a purchase transaction with rewards points that may be associated with virtual card 4404. In so doing, for example, a mobile device may, for example, establish a contactless communication channel (e.g., an RFID communication channel) with a merchant terminal and may communicate points information that may be associated with virtual card 4404 so that a purchase transaction may be completed using rewards points that may be associated with virtual card 4404.

[0344] GUI 4400 may, for example, provide other information to a user concerning virtual card 4406. For example, a processor of a mobile device may detect that an expiration date of virtual card 4406 is approaching. Accordingly, for example, a user may touch a display in the vicinity of virtual card 4406 to automatically renew the driver's license using the mobile device. In so doing, for example, a mobile device may contact a network entity (e.g., a driver's license renewal server) to order a renewal driver's license. The renewal driver's license may, for example, be delivered to the user as a physical card, in which case the user may upload information associated with the physical driver's license into the mobile device via a contactless communication channel formed between the physical driver's license and the mobile device. Alternately, for example, a mobile device may receive an electronic copy of a virtual driver's license and replace information associated

with virtual card 4406 with the updated information received from a driver's license renewal server.

[0345] FIG. 45 shows system 4500, which may include mobile wallet 4502 and a powered card (e.g., powered payment card 4506). Powered card 4506 may, for example, include a contactless communication device (e.g., an RFID) that may communicate with a contactless communication device (e.g., an RFID) of mobile wallet 4502. A GUI executed by a processor of mobile wallet 4502 may invite a user of powered card 4506 to tap powered card 4506 against display 4504 of mobile wallet 4502. Such contact with, or proximity to, mobile wallet 4502 may generate a contactless communication channel within which information may be exchanged between powered card 4506 and mobile wallet 4502.

[0346] As per another example, powered card 4506 may include circuitry that may simulate a touch. Display 4504 may be touch-sensitive. Accordingly, for example, powered card 4506 may communicate data to mobile wallet 4502 by simulating a series of touches that may be sensed by display 4504 and processed by a processor of mobile wallet 4502 as data received from powered card 4506. Powered card 4506 may include light sensor 4510. Accordingly, for example, a processor of mobile wallet 4502 may generate a series of light pulses on a portion of display 4504 that may be detected by light sensor 4510 of powered card 4506 and processed by a processor of powered card 4506 as data communicated by mobile wallet 4502. In so doing, for example, data may be communicated by powered card 4506 via a series of simulated touches and data may be communicated by mobile wallet 4502 via a series of light pulses.

[0347] Information communicated by powered card 4506 to mobile wallet 4502 may, for example, include payment information (e.g., payment account number, expiration date, and cardholder name). Information communicated by powered card 4506 to mobile wallet 4502 may, for example, include other information relating to a configuration of powered card 4506 including, for example, whether or not a display exists and if so, at what location; whether or not a manual input interface (e.g., one or more buttons) exists and if so, at what location; and whether or not a light sensor exists and if so, at what location. Accordingly, for example, configuration information relating to powered card 4506 may be communicated to mobile wallet 4502, so that when a virtual card relating to powered card 4506 is generated and stored within mobile wallet 4502, the virtual card may employ all of the features that may be employed by its physical counterpart.

[0348] Information communicated by powered card 4506 may, for example, be encrypted. Decryption may, for example, be executed within mobile wallet 4502 so that information communicated by powered card 4506 may be stored within a memory of mobile wallet 4502 in a decrypted format. Alternately, for example, information communicated by powered card 4506 may be stored within a memory of mobile wallet 4502 in an encrypted format. Mobile wallet 4502 may, for example, authenticate itself to a network entity (e.g., an issuer server) such that each time encrypted information is recalled from a memory of mobile wallet 4502, a decryption key may be communicated by the network entity to mobile wallet 4502 for decryption purposes.

[0349] FIG. 46 shows GUI 4600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4600 may, for example, display virtual card 4602 that may employ all of the features of its physical counterpart. Accordingly, for example, manual input interfaces (e.g., virtual buttons 4606 through 4614) may have the same functionality on virtual card 4602 as they do on the physical counterpart to virtual card 4602. In so doing, for example, virtual buttons 4606 through 4614 may be displayed on portions of GUI 4600 that may be touch-sensitive, such that when virtual buttons 4606 through 4614 are touched, a processor of the mobile device may impart a functionality to the mobile device just as if the mobile device itself was the physical card (e.g., a PIN may be entered into virtual card 4602 via one or more buttons 4606-4614 to unlock virtual dynamic portion 4618 of virtual payment card number 4616).

[0350] A mobile device may, for example, provide a light-sensitive display, such that when virtual card 4602 is rendered onto the light-sensitive display, light sensor 4604 may exhibit the same functionality as its physical counterpart. Accordingly, for example, virtual card 4602 may be rendered so that light sensor 4604 exists on a light-sensitive portion of a display of a mobile device. A processor of the mobile device may, for example, detect light pulses sensed at light sensor 4604 as data communicated to virtual card 4602. In so doing, for example, virtual card 4602 may receive information that changes the functionality of virtual card 4602 (e.g., an expiration date of virtual payment card 4602 may be updated via light sensor 4604).

[0351] A mobile device may, for example, provide a display that may simulate touch. Accordingly, for example, virtual card 4602 may be rendered onto a display of a mobile device so that touch-simulating portion 4620 aligns with a portion of the display that may be capable of simulating touch. In so doing, for example, virtual card 4602 may communicate information to another device (e.g., another mobile device) when touch-simulating portion 4620 of GUI 4600 is pressed against another device (e.g., a touch-sensitive display of another mobile device) and simulates a series of touches that may be construed by a processor of the other device as data communicated to the other device.

[0352] Virtual display 4618 may, for example, display a dynamic portion of payment card number 4616 just as it would be displayed on the physical counterpart to virtual card 4602. For example, virtual card 4602 may be disabled for use when virtual display 4618 does not display a valid portion of virtual card number 4616. Upon entry of a password (e.g., a PIN may be entered by touching one or more buttons 4606-4614 that corresponds to the PIN), virtual card 4602 may be activated for use. Accordingly, for example, once a valid PIN is entered, virtual display 4618 may be populated with a remaining portion of virtual payment card number 4616 thereby activating virtual card 4602 for use. In so doing, for example, a mobile device that displays activated virtual card 4602 via GUI 4600 may communicate payment information (e.g., virtual payment card number 4616 and expiration date) to a device (e.g., a merchant terminal) via a contactless communication channel (e.g., an RFID communication channel) so that a purchase transaction may be

completed between the mobile device and the merchant terminal.

[0353] FIG. 47 shows GUI 4700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4700 may, for example, display virtual card 4702 that may employ all of the features of its physical counterpart. For example, a powered card (e.g., a powered payment card) may establish a contactless communication channel (e.g., an RFID communication channel) with a mobile device and communicate configuration and payment information that may be associated with the powered card. Accordingly, for example, a powered card may provide a manual interface (e.g., buttons) to allow a user to select a method of payment (e.g., credit, debit, or points) at the point of sale and may communicate such methods of payment to a mobile device. In so doing, for example, a mobile device may render virtual payment card 4702 having a virtual manual interface (e.g., virtual buttons 4704 through 4708), which a user may select (e.g., touch) in order to select a method of payment to be used by the mobile device when the mobile device communicates payment information to complete a purchase transaction.

[0354] A mobile device may, for example, establish a contactless communication channel (e.g., an RFID communication channel) with a merchant terminal to communicate payment information to the merchant terminal to complete a purchase transaction. Accordingly, for example, a user may touch one of virtual buttons 4704-4708 just prior to placing the mobile device within a proximity to the merchant terminal. In so doing, for example, the mobile device

may communicate one, two, and/or three tracks of magnetic stripe data to the merchant terminal and may include additional information (e.g., within a discretionary data field) to communicate a method of payment (e.g., credit, debit, or points) to the merchant terminal. Persons skilled in the art will appreciate that payment information may be communicated by a mobile device to a network entity (e.g., a payment server) via a wireless interface (e.g., a cellular interface) such that a method of payment (e.g., credit, debit, or points) may be communicated by the mobile device to the payment server to complete a remote purchase transaction.

[0355] FIG. 48 shows GUI 4800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4800 may, for example, allow a user of a mobile device to break a payment up into multiple payment methods for a single purchase. For example, a user of a mobile device may have provided a mobile device within a proximity to a merchant terminal, such that the mobile device may have communicated a method of payment (e.g., credit) to the merchant terminal based upon a user selection made via a GUI displayed by the mobile device. A processor of the mobile device may, for example, recognize that a virtual card selected by the user for payment may offer additional payment methods (e.g., debit and points). Accordingly, for example, GUI 4800 may be rendered by a processor of the mobile device to allow the user of the mobile device the option to spread the payment across several accounts by entering amounts into alphanumeric entry boxes 4804-4808. In so doing, for example, a user may spread a purchase across multiple payment

methods by entering an amount desired to be charged to each payment method (e.g., $5 credit, $5 debit, and 1500 points for a $25 total purchase). The mobile device may, for example, settle the transaction as three separate financial transactions by communicating payment information to one or more network entities (e.g., a payment server) that corresponds to each of the three financial transactions.

[0356] FIG. 49 shows GUI 4900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4900 may, for example, communicate a credit offer to a user of a mobile device that may have been communicated to the mobile device via any one of a number of electronic means (e.g., text messaging, email, or internet browser pop-up). A credit offer may, for example, be extended to a user of a mobile device to add a payment card to the user's mobile device. A credit offer (e.g., credit offer 4906) may, for example, be extended to a user of a mobile device to replace a virtual card (e.g., virtual payment card 4904) that already exists within the user's mobile device. Accordingly, for example, network entities may examine virtual cards and related information that may be stored within a memory of a mobile device and attempt to sway the user of the mobile device to opt into another virtual card offer that may be better for the user (e.g., the new virtual card may offer a lower interest rate than a user's current virtual payment card).

[0357] GUI 4900 may, for example, provide credit offer options 4908 to a user of a mobile device. Accordingly, for example, a user may elect to accept a new credit offer and cancel a current virtual payment

card with the same option. In so doing, for example, a mobile device may communicate with a network entity (e.g., an issuer of virtual payment card 4904) to cancel virtual payment card 4904 and may communicate with a network entity (e.g., an issuer for payment card offer 4906) to open the new payment account being offered.

[0358] Other options may be provided by GUI 4900. For example, a user may opt to accept the new credit offer, but keep virtual payment card 4904 as well. As per another example, a user may opt to accept the new credit offer, keep virtual payment card 4904, and transfer any balance that may be owing on virtual payment card 4904 to the new payment account now being offered.

[0359] FIG. 50 shows mobile application 5000 that may be executed by a processor of a mobile device and provided onto a display of the mobile device. Application 5000 may, for example, be any executable application that may reside within a memory of a mobile device. For example, application 5000 may be an internet browsing application that may allow a user of a mobile device to browse online for goods and/or services and may allow the user to purchase such goods and/or services from application 5000. As per another example, mobile application 5000 may be a gaming activity that may require a purchase transaction to continue on to a next level of play or to obtain gaming features for purchase.

[0360] Application 5000 may, for example, provide access to mobile wallet 5002 which may be another application running on a mobile device. Accordingly, for example, when application 5000 requires payment for

a particular function performed by application 5000 (e.g., a user wishes to purchase goods from an Amazon website), application 5000 may launch mobile wallet 5002 to allow a user to select a method of payment from mobile wallet 5002. A user may browse through each virtual card of mobile wallet 5002 by touching a virtual card to display the virtual card. Once a user has verified that a particular virtual card is the virtual card to be used to complete a purchase transaction, the user may touch the virtual card twice again to authorize a mobile device to complete a purchase transaction using payment information associated with the selected virtual card.

[0361] As per another example, a user may preselect payment options, such that mobile application 5000 need not launch mobile wallet 5002 to obtain a payment authorization. Instead, for example, a user may pre-authorize one virtual payment card within mobile wallet 5002 to be used by any other application running on a mobile device for purchase transactions. In so doing, for example, a user may pre-authorize payment information to be autonomously retrieved from mobile wallet 5002 without involving user interaction to authorize application 5000 for the purchase transaction.

[0362] FIG. 51 shows flow charts for process sequences 5110-5150. Process sequence 5110 may, for example, execute a mobile wallet application on a mobile device (e.g., as in step 5111) to request a user of the mobile device to present a card to the mobile device. In step 5112, a user may present a card to a mobile device (e.g., tap a card onto a display of a mobile device). In step 5113, a contactless

communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a card and a mobile device to communicate card information from the payment card to the mobile device. In step 5114, information may be stored within the mobile device or remote server (e.g., virtual cards may be generated, stored, and displayed by a GUI of the mobile device) for future use.

[0363] Process sequence 5120 may, for example, autonomously detect that a card is in a touching or a proximity relationship to a mobile device (e.g., as in step 5121). In step 5122, a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a card and a mobile device to communicate information from the card to the mobile device. In step 5123, information associated with each physical card presented to the mobile device may be stored within the mobile device for future use.

[0364] Step 5131 of sequence 5130 may include presenting a card to a mobile device. A card may, for example, be a powered card or a non-powered card. In steps 5132 and 5133, a contactless communication channel may be established between a card and a mobile device and information may be exchanged between the card and the mobile device.

[0365] A card may, for example, include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. A card may, for example, include circuitry to simulate touch (e.g.,

a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device.

[0366] A card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a card as data communicated by a mobile device.

[0367] A card may, for example, include a light source (e.g., an LED) to form a contactless communication channel. Accordingly, for example, a card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the card. A card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the card through a contactless communication channel. A mobile device may, for example, include sound emission capabilities that may be detected by a microphone of a card as data communicated by the mobile device through a contactless communication channel.

[0368] Step 5141 of sequence 5140 may include arranging information contained within a memory of a mobile device and/or a remote server and rendering the information on a display of a mobile device. The rendered information may, for example, be virtual cards that are representative of physical card counterparts previously presented to the mobile device for upload.

[0369] The virtual cards may, for example, be arranged according to category (e.g., payment cards, gift cards and identification cards). Within each category, virtual cards may be sorted according to any sort preference. For example, payment cards may be sorted in an order of most frequently used to least frequently used, in order of most available credit to least available credit, or in order of highest credit limit to lowest credit limit. Other cards (e.g., merchant gift cards) may be sorted in accordance with a user's location. For example, a mobile device may determine a location of its user and may sort virtual cards in response to the determined location (e.g., a virtual Walmart gift card may be displayed at the top of a gift card list based upon a user's location within a Walmart store).

[0370] Virtual cards displayed by a GUI of a mobile device may, for example, be selected for use (e.g., as in step 5142). A user may, for example, touch a virtual card among several virtual cards displayed by a mobile device to view information related to the touched virtual card. If desired for use, the touched virtual card may be touched twice again and activated for use (e.g., as in step 5143). An activated virtual card may, for example, be used to complete a purchase transaction via the mobile device. An activated

virtual card may, for example, be deleted from a memory of the mobile device. Documents associated with an activated virtual card, such as purchase transaction receipts and bank statements, may be viewed from a display of a mobile device. Virtual cards that may be associated with an activated virtual card may be viewed from a display of a mobile device and activated themselves to perform other functions (e.g., an activated virtual payment card may be associated with a virtual rewards card, where the virtual rewards card may be activated to obtain and view the total number of rewards points that may be associated with the virtual rewards card).

[0371] Step 5151 of sequence 5150 may include running an application on a mobile device. Such an application may be any executable application that may require purchase transactions to be completed while the application executes. As per one example, a user booking airline tickets using his or her mobile device may select their itinerary and may book their itinerary through a purchase transaction conducted by the mobile device. Accordingly, for example, the mobile application may request access to a mobile wallet application also running on the mobile device (e.g., as in step 5152), a user may grant access to the mobile wallet application (e.g., as in step 5153) by selecting a virtual payment card from within the mobile wallet and may authorize a purchase transaction to be conducted by the mobile application using the authorized virtual payment card. As per another example, a mobile application may autonomously request access to a mobile wallet application (e.g., as in step 5152) that has been pre-authorized by a user of the

mobile device (e.g., as in step 5153) such that the mobile application may autonomously conduct the purchase transaction without any further involvement with the user.

[0372] FIG. 52 shows mobile device 5200. Mobile device 5200 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, mobile device 5200 may be operated in a mobile environment while a user of mobile device 5200 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 5200 may perform multiple functions simultaneously (e.g., a person may carry on a conversation while at the same time browsing and authorizing purchases on the internet).

[0373] Mobile device 5200 may include audio processing devices (e.g., microphone 5208 and speaker 5210). Accordingly, for example, mobile device 5200 may receive voice commands from a user via microphone 5208 and may process such commands to perform a function. For example, a user may place mobile device 5200 into a desired operational mode by speaking a command into microphone 5208 that is associated with the desired operational mode. In so doing, for example, mobile device 5200 may engage in hands-free operation by receiving voice commands via microphone 5208 and performing functions associated with the received voice commands.

[0374] Mobile device 5200 may receive data input via microphone 5208. For example, a voice-band modem may generate signals in a voice-band frequency range that

may be received by microphone 5208. A processor of mobile device 5200 may interpret the received audible information as data signals and may process the data signals as, for example, data values and/or control data input.

[0375] Mobile device 5200 may include camera 5202. Camera 5202 may capture one or more frames of video data and store the video data within a memory of mobile device 5202. Accordingly, for example, a processor of mobile device 5200 may receive one or more frames of video information via camera 5202 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 5200 may receive optical information that may be sensed by camera 5202 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 5200 as data values and/or control data.

[0376] Mobile device 5200 may include manual input interface 5212. Manual input interface 5212 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 5200 may enter information into mobile device 5200 via manual interface 5212 to cause a processor of mobile device 5200 to enter a particular mode of operation. Manual interface 5212 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile

device 5200) during a particular mode of operation of mobile device 5200.

[0377] Mobile device 5200 may include display 5204. Display 5204 may provide visible information that may be utilized by a user during interaction with mobile device 5200. A portion or all of display 5204 may be touch sensitive such that objects making contact with display 5204 or objects coming within a proximity of display 5204 may be detected by a processor of mobile device 5200. Accordingly, for example, mobile authorization graphical user interface 5206 may be provided by display 5204 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, alphanumeric input boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 5200.

[0378] FIG. 52 shows architecture 5250. User interface 5252 may, for example, be included within architecture 5250 to allow user interaction with architecture 5250. For example, a dedicated key pad or keyboard may be included within user interface 5252 to allow alphanumeric data entry into architecture 5250.

[0379] Architecture 5250 may include one or more displays 5254. Display 5254 may, for example, be touch-sensitive. Accordingly, for example, display 5254 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 5254. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of

display 5254 may be detected by processor 5258 as alphanumeric data entry.

[0380] Alphanumeric entry boxes may, for example, be rendered onto display 5254. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 5252 and/or a virtual keypad rendered onto display 5254 to select alphanumeric characters to be placed within the alphanumeric entry box in accordance with a character position identified by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 5258 may receive alphanumeric characters as typed into a alphanumeric entry box of display 5254 and may use such alphanumeric characters as data input.

[0381] Display 5254 may, for example, provide data output from architecture 5250. For example, display 5254 may communicate data using a series of light pulses. Accordingly, for example, processor 5258 may cause one or more portions of display 5254 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 5254 via light pulses having varying characteristics. Display 5254 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0382] Architecture 5250 may include one or more transceivers 5256. Transceiver 5256 may communicate information to and/or may receive information from one or more devices. Transceiver 5256 may, for example,

communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly, for example, transceiver 5256 may allow a mobile device (e.g., mobile device 5200 of FIG. 52) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 5200 of FIG. 52) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 156 may exchange information with one or more other mobile devices via one or more associated cellular stations.

[0383] Transceiver 5256 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 5256 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 5256 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 5200 of FIG. 52) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network.

[0384] Architecture 5250 may include contactless communication device 5262, which may communicate via any one or more contactless communication methodologies, such as for example, near field communications (e.g., RFID), Bluetooth, touch simulation, light pulsing (e.g., via an LED), and electromagnetic data communication (e.g., via a dynamic magnetic stripe communications device). Accordingly, for example, contactless communication device 5262 may be compatible with any contactless device, such as for example, an RFID enabled payment card and a contactless reader (e.g., a magnetic stripe reader or an NFC reader).

[0385] A non-powered card may, for example, communicate with contactless communications device 5262. Contactless communication device 5262 may, for example, establish a carrier field (e.g., an RF field) that may be modulated by a device (e.g., an RFID tag) of a non-powered payment card. In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by contactless communications device 5262 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 5262 by modulating the RF field produced by contactless communications device 5262.

[0386] A powered card may, for example, communicate with contactless communication device 5262. A powered card may, for example, include a processor, a battery, a memory, wireless communication devices (e.g., a dynamic magnetic stripe communications device or RFID) and other electronics (e.g., buttons) that may allow a user to interact with the powered card to perform one

or more functions. Accordingly, for example, a powered card may be used to communicate specific information to contactless communication device 5262 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 5262 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications.

[0387] Contactless communication device 5262 may receive variable data sets from a powered card based upon, for example, manual input provided to a powered card. For example, a button associated with an on-line purchase may be pressed on the powered card that causes a variable data set (e.g., account number and expiration date) to be communicated from the powered card to contactless communication device 5262.

[0388] Discretionary data may, for example, be communicated by a powered card based upon which button was pressed on the powered card. In so doing, for example, a security code (e.g., "111") may be communicated within a discretionary data field when a button associated with a particular feature (e.g., pay with credit) is pressed on the powered card. As per another example, a different security code (e.g., "222") may be communicated within a discretionary data field when a button associated with a different feature (e.g., pay with debit) is pressed on the powered card. A powered card may, for example, communicate a different security code no matter what feature may be selected on the powered card. Accordingly, for

example, processor 5258 may identify what type of device may be in communication with contactless communication device 5262 by analyzing the data communicated to contactless communication device 5262.

[0389] Any device having contactless communication capability may communicate with contactless communication device 5262 to authorize functions that may be performed by a mobile device. An RFID enabled device (e.g., an RFID equipped automobile key) may, for example, communicate with contactless communication device 5262 to authorize functions that may be performed by a mobile device (e.g., mobile device 5200 of FIG. 52) on a device that may be controlled by the RFID enabled device (e.g., an automobile that corresponds to the RFID equipped automobile key). For example, processor 5258 may execute an automobile application that may wirelessly communicate with an automobile to perform remote functions (e.g., start an engine of the automobile or unlock the driver's door). Through use of an RFID equipped key, for example, such functions may be authorized to be performed by a mobile device (e.g., mobile device 5200 of FIG. 52) once the RFID equipped key has communicated the necessary security credentials (e.g., a key code) to an application running on a processor of the mobile device to establish that a one-to-one correspondence exists between the automobile and the RFID equipped key.

[0390] Architecture 5250 may include memory 5260 and/or processor 5258 may include internal memory. Accordingly, for example, application code may be stored within memory 5260 and/or processor 5258 and executed by processor 5258 in support of functions performed by architecture 5250. For example, an

application (e.g., a graphical user interface) may be executed by processor 5258 and displayed onto display 5254, which may be used to interact with a user of a mobile device (e.g., mobile device 5200 of FIG. 52). Persons skilled in the art will appreciate that executable application code may be communicated to architecture 5250 via any one or more interfaces of architecture 5250 (e.g., user interface 5252, display 5254, transceiver 5256, and/or contactless communication device 5262).

[0391] Application data (e.g., security credentials) may be stored within memory 5260 and accessed by processor 5258 during operation. For example, security credentials may be stored within memory 5260 and recalled by processor 5258 to authorize a function that may be performed by processor 5258 of a mobile device (e.g., mobile device 5200 of FIG. 52). Accordingly, for example, processor 5258 of a mobile device may challenge a user of the mobile device to produce security credentials to authorize any function that may be performed by the mobile device. A processor of the mobile device may, for example, validate the security credentials locally within the mobile device itself. Alternately, for example, security credentials may be forwarded to a network entity (e.g., an authorization server) for remote validation.

[0392] FIG. 53 shows network topology 5300 that may include, for example, mobile device 5302 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile device 5302 may, for example, include a contactless interface that may initiate, sustain, and/or terminate communication channel 5326 between contactless device

5304 and mobile device 5302. Contactless device 5304 and mobile device 5302 may communicate via channel 5326 using any number of contactless mediums, which may include for example, visible, audible, capacitive, electromagnetic, magnetic, and/or RF mediums.

[0393] Mobile device 5302 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 5312 and/or payment network 5314) and/or one or more wireless networks (e.g., mobile network 5310). Mobile device 5302 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile device 5302 to communicate information (e.g., voice and data) to cellular network access infrastructure 5306 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 5306 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0394] Mobile device 5302 may, for example, communicate with wireless access point 5308 over a wireless interface (e.g., a Bluetooth interface or a Wi-Fi interface). Accordingly, for example, mobile device 5302 may access one or more wired networks (e.g., IP network 5312 and/or payment network 5314) and/or one or more wireless networks (e.g., mobile network 5310) without the need to first gain access to cellular network access infrastructure 5306.

[0395] Contactless device 5304 may, for example, be a powered card, a non-powered card (e.g., a powered

payment card or a non-powered payment card) or any contactless enabled device (e.g., an RFID enabled device). Accordingly, for example, security credentials may be communicated via a contactless communication channel from contactless device 5304 to mobile device 5302 to authenticate a purchase transaction that may be performed by mobile device 5302. In so doing, for example, items for purchase on IP network 5312 (e.g., the internet) may be accessed by a browser of mobile device 5302 via an access point (e.g., wireless access point 5308 or cellular network access infrastructure 5306), payment information may be retrieved from a memory of mobile device 5302, a user of mobile device 5302 may be challenged for security credentials (e.g., at least a portion of a payment account number and a card expiration date communicated to mobile device 5302 from a payment card corresponding to the payment information retrieved from a memory of mobile device 5302), such payment information may be authenticated by such security credentials, and such payment information may be communicated to network entities (e.g., issuer 5320) to complete the purchase transaction.

[0396] Issuer 5320 may, for example, contact authorization server 5316 via a network (e.g., payment network 5314) with payment information and security credentials received from mobile device 5302 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile device 5302 via any one or more delivery options (e.g., via a short messaging service of mobile network 5310 or an email delivery service of IP network 5312). Mobile device 5302 may

allow a user to associate purchase categories (e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile device so that the user may receive a more detailed accounting of his or her expenditures on his or her receipt. Accordingly, for example, a user may enjoy a higher degree of integration such that a user may customize a level of detail provided on a receipt via mobile device 5302.

[0397] A payment receipt may, for example, be provided to mobile device 5302 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile device 5302 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0398] A processor of mobile device 5302 may, for example, authorize wireless device 5334 to perform functions that may be authenticated by contactless device 5304 (e.g., via security credentials communicated by contactless device 5304 to a processor of mobile device 5302). Accordingly, for example, a processor of mobile device 5302 may require security credentials to be communicated by contactless device 5304 via contactless communication channel 5326 and based upon a validity of the security credentials communicated, the processor may communicate instructions to wireless device 5334 via contactless communication channel 5336 to perform some function. As per another example, a processor of mobile device 5302 may communicate instructions (e.g., via wireless access point 5308 or cellular network access infrastructure 5306) to wireless device 5334 (e.g., a car or a home) to perform a function (e.g., start the

engine of the car) based upon a validity of security credentials communicated by contactless device 5304.

[0399] A processor of mobile device 5302 may, for example, locally validate security credentials communicated by contactless device 5304. Alternately, for example, mobile device 5302 may forward security credentials communicated by contactless device 5304 to a network entity (e.g., authorization server 5332) for remote validation.

[0400] A mobile device (e.g., mobile device 5324) may, for example, include a contactless communication device (e.g., an RFID device) that may initiate, sustain, and/or terminate contactless communication channel 5328 with merchant terminal 5318. Accordingly, for example, a processor of mobile device 5324 may communicate payment information to merchant terminal 5318 to complete a financial transaction. In so doing, for example, a processor of mobile device 5324 may receive payment information via contactless communication channel 5330 from contactless device 5322 (e.g., a powered or a non-powered card) and store the received payment information within a memory of mobile device 5324. To complete a purchase transaction, contactless device 5322 may, for example, be presented to mobile device 5324 and may communicate security credentials (e.g., at least a portion of a payment card number and a cardholder's name) via contactless communication channel 5330. A processor of mobile device 5324 may validate the security credentials and may forward the payment information onto merchant terminal 5318 to complete the purchase transaction.

[0401] FIG. 54 shows system 5400, which may include mobile device 5402 and contactless devices 5408-5414.

Mobile device 5402 may, for example, be a laptop computer, a PDA, a mobile telephonic device (e.g., a smartphone), an MP3 player, a GPS, or any other mobile device. Display 5404 may be a touch-sensitive display (e.g., sensitive to a change in capacitance). Contactless devices may, for example, include non-powered payment card 5408, identification card (e.g., driver's license 5410), powered payment card 5412, key 5414, and any other device capable of communicating security credentials to mobile device 5402 via a contactless communication channel that may be formed with mobile device 5402.

[0402] Mobile device 5402 and contactless devices 5408-5414 may each include a contactless communication device (e.g., an RFID device) that may communicate via a contactless communication channel that may be formed between mobile device 302 and contactless devices 5408-5414 after coming into proximity to one another. Contactless devices 5408-5414 may, for example, be tapped onto display 5404 of mobile device 5402 to establish a proximity relationship that forms a communication channel with mobile device 5402. As per another example, contactless devices 5408-5414 may be brought within a proximity distance (e.g., up to two inches) of mobile device 5402 to establish a contactless communication channel with mobile device 5402.

[0403] A processor of mobile device 5402 may, for example, execute application code that may generate a graphical user interface (GUI) onto display 5404 of mobile device 5402. Message 5406 of a GUI may invite a user of mobile device 5402 to begin a mobile authorization by tapping a contactless device against

display 5404. As per another example, by tapping a contactless device against mobile device 5402, a processor of mobile device 5402 may autonomously determine that a mobile authorization is desired and may then generate a mobile authorization GUI onto display 5404.

[0404] Mobile device 5402 may, for example, autonomously determine a type of contactless device that may be tapped against it. For example, a processor of mobile device 5402 may receive security credentials that may be indicative of a non-powered payment card (e.g., security credentials received from non-powered payment card 5408 may include at least a portion of a payment card number and a cardholder's name). As per another example, a processor of mobile device 5402 may receive security credentials that may be indicative of a powered card (e.g., security credentials received from powered card 5412 may contain a dynamically generated security code). Security credentials received from powered card 5412 may, for example, include a dynamic security code that may change for each function authorized by powered card 5412.

[0405] A contactless device (e.g., key 5414) may, for example, be a key that may start the ignition of a car, open a door to a home, or open a safe deposit box. Key 5414 may, for example, include a contactless communication device (e.g., an RFID device) that may communicate security credentials to a processor of mobile device 5402. Once security credentials received from key 5414 are validated, a processor of mobile device 5402 may effect an operation that may eliminate the need to physically use key 5414 to perform the

operation (e.g., a user of mobile device 5402 may remotely start the engine of the user's car by running an application on a processor of mobile device 5402 to validate security credentials received from key 5414 and wirelessly communicate with a wireless device of the user's car to start its ignition). As per an example, the user's physical key 5414 may, for example, be locked inside the user's car, in which case the user may select another contactless device (e.g., identification card 5410) to present to mobile device 5402. Identification card 5410 may, for example, communicate security credentials to a processor of mobile device 5402 and once the processor authorizes the identify of the user of mobile device 5402, mobile device 5402 may, for example, wirelessly communicate with the user's car to unlock its doors so that the user may retrieve key 5414 that may have been previously locked within the user's car.

[0406] Powered payment card 5412 may, for example, include electronics to simulate a human touch (e.g., powered payment card 5412 may generate a change in capacitance that may be sensed by display 5404). Through a series of simulated touches, powered payment card 5412 may communicate a series of data bits to display 5404, which may then be processed by a processor of mobile device 5402 as security credentials. In so doing, for example, a contactless communication channel may be established where data is transferred from powered payment card 5412 to a processor of mobile device 5402 via a series of simulated touches to authorize a function to be performed (or commanded to be performed) by a processor of mobile device 5402.

[0407] Powered payment card 5412 may, for example, include a light sensor. Accordingly, for example, powered payment card 5412 may be sensitive to light pulses generated within a region of display 5404. The light sensor of powered payment card 5412 may receive a series of light pulses, which may be construed by a processor of powered payment card 5412 as data generated by a processor of mobile device 5402. In so doing, for example, powered payment card 5412 may receive an optical data stream represented by a series of light pulses generated by display 5404. As such, a two-way communication channel may be formed, where simulated touches may generate a data stream from powered payment card 5412 to mobile device 5402 and light pulses may generate a data stream from mobile device 5402 to powered payment card 5412.

[0408] Mobile device 5402 may, for example, include a motion-capture device (e.g., a camera). Identification card (e.g., driver's license 5410) may, for example, include a barcode. Accordingly, for example, a contactless communication channel may be formed between identification card 5410 and mobile device 5402 where a camera of mobile device 5402 may capture an image of the barcode of identification card 5410. In so doing, for example, a processor of mobile device 5402 may analyze the barcode image and extract information from the barcode image that may be construed by the processor as security credentials that when validated, may authorize a processor of mobile device 5402 to perform (or cause to perform) any function.

[0409] As per another example, a user's photograph may appear on identification card 5410. Accordingly,

for example, a camera of mobile device 5402 may capture an image of the picture and a processor of mobile device 5402 may construe the captured image as a security credential. In so doing, for example, a processor of mobile device 5402 may compare a scanned image of a user's picture to an image contained within a memory of mobile device 5402 (or contained within a memory of a remote authorization server) for authorization. As per yet another example, a user may snap a picture of himself or herself with a camera of mobile device 5402 so that a processor of mobile device 5402 may scan the snapped picture for authorization purposes.

[0410] Mobile device 5402 may, for example, require authorization before being activated for use. Accordingly, for example, a processor of mobile device 5402 may require a password to be entered and verified before a processor of mobile device 5402 may unlock functions available to be performed by mobile device 5402. In so doing, for example, one or more contactless devices 5408-5414 may be presented to mobile device 5402 and security credentials may be communicated by the one or more contactless devices 5408-5414 in lieu of providing a password to mobile device 5402. Upon validation of the security credentials, a processor of mobile device 5402 may unlock those functions that may be available to be executed by the processor of mobile device 5402.

[0411] FIG. 55 shows GUI 5500, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 5500 may, for example, provide a summary of each card that may be available for use within a memory of the mobile device

(e.g., each card may be displayed as virtual cards having visible and functional features that are substantially the same as their physical counterparts).

[0412] Physical card (e.g., payment card) information (e.g., track 1, track 2, and/or track 3 magnetic stripe data) may be communicated by the physical card to the mobile device via a contactless communication channel and such information may be displayed within a virtual card (e.g., virtual payment card 5502) as summary information that may be associated with the physical payment card. A payment card number communicated to a processor of a mobile device may, for example, include issuer identification as well as an issuing network identifier. Accordingly, for example, a processor of a mobile device may analyze the payment card number received from a physical payment card and may render a portion or all of the identifying information associated with the payment card number onto virtual payment card 5502. In so doing, for example, issuer identification as well as a logo representative of an issuing network identifier may be rendered onto virtual payment card 5502. Other virtual payment cards may, for example, be sorted behind virtual payment card 5502 in virtually any order (e.g., most popular to least popular, highest credit limit to lowest credit limit, or highest credit available to lowest credit available). Other virtual cards (e.g., virtual gift card 404 and virtual driver's license 5506) may be stored within a memory of a mobile device as well.

[0413] FIG. 56 shows GUI 5600, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 5600 may, for

example, allow a selection of a virtual card contained within a memory of a mobile device to be authorized for use by its physical counterpart. Accordingly, for example, a user may touch anywhere within the vicinity of virtual card 5604 as it is being displayed by GUI 5600. Such a selection may be verified by highlighting attributes of a selected card (e.g., highlighting an outline of virtual card 5604) and by displaying the selected virtual card within verification region 502. In so doing, for example, a user of a mobile device may view a virtual card that is selected for authorization (e.g., as viewed within region 5602) so that the user may retrieve the physical card that corresponds to the virtual card that is to be authorized.

[0414] Once retrieved, a user may tap the physical card against region 5602. Accordingly, for example, a contactless communication channel (e.g., an RFID communication channel) may be formed between the physical card and the mobile device, such that security credentials may be communicated from the physical card to the mobile device via the contactless communication channel to authorize virtual payment card 5602 for use. In so doing, for example, a physical card may communicate security credentials (e.g., at least a portion of a payment card number of the physical card and/or a cardholder's name) to a processor of the mobile device and the processor may compare the received security credentials to security credentials stored within a memory of the mobile device that may be associated with virtual payment card 5602. If the processor of the mobile device determines that the received security credentials match at least a portion of the security credentials associated with virtual

payment card 5602, then virtual card 5602 may be authorized for use.

[0415] FIG. 57 shows GUI 5700, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 5700 may, for example, allow the authorization of a virtual card via an alternate contactless communication channel. For example, GUI 5700 may display a virtual payment card (e.g., virtual payment card 5702) in a region within GUI 5700 that may provide a touch-sensitive area 5704 and area 5706 that may be capable of producing light pulses having varying characteristics (e.g., intensity, pulse width, and/or color).

[0416] A user's physical card that corresponds to virtual payment card 5702 may, for example, be a powered card having touch-simulation electronics and a light sensor. Accordingly, for example, the user's physical card may be pressed against region 5702, such that the touch simulation electronics of the physical card aligns with touch-sensitive portion 5704 and the light sensor of the physical card aligns with portion 5706. In so doing, for example, a contactless communication channel may be formed between the user's physical card and the mobile device, such that data may be communicated from the user's physical card to the mobile device through a series of simulated touches generated by the physical card and sensed at portion 5704 by a processor of the mobile device. Such communicated data may be construed by a processor of the mobile device as security credentials communicated by the user's physical card.

[0417] Security credentials that may be communicated (e.g., via a capacitive, visible, audible,

electromagnetic, magnetic, or RFID-based contactless communication channel) to a mobile device by a powered payment card may, for example, include a dynamic security code that may change with each use. Accordingly, for example, a network entity (e.g., an authorization server) may be synchronized with the user's powered payment card, such that when a dynamic security code of the powered payment card changes, so does the corresponding dynamic security code of the authorization server. In so doing, for example, a dynamic security code received by a mobile device from a powered payment card during authorization of virtual payment card 5702 may be communicated by a processor of the mobile device to an authorization server for verification that the dynamic security code matches the dynamic security code maintained by the authorization server. If so, virtual payment card 5702 may be authorized for use by the mobile device (e.g., payment information associated with virtual payment card 5702 may be communicated by the mobile device to complete a purchase transaction).

[0418] FIG. 58 shows system 5800 that may include mobile terminal 5802, payment card 5808, network 5814 and authorization server 5810. A processor of mobile device 5802 may, for example, execute an application (e.g., GUI 5804) that allows a user of mobile device 5802 to perform any financial account management function (e.g., change from paper statements to e-statements, transfer money from one account to another or open a checking account).

[0419] Prior to authorizing the financial account management function, GUI 5804 may challenge a user of mobile device 5802 to tap a card against mobile device

5802 that may be associated with the transaction. Accordingly, for example, a payment card (e.g., payment card 5808) that may be associated with the financial accounts used for the financial account management function may be used as a security credential to authorize the transaction. In so doing, for example, security credentials communicated by payment card 5808 to mobile device 5802 via contactless communication channel 5806 (e.g., an RFID communication channel) may be relayed by mobile device 5802 to authorization server 5810 via communication channel 5812 for authorization of the financial account management function. Once authorized, a processor of mobile device 5802 may receive the authorization from authorization server 5810 and may contact other network entities (e.g., a payment server of network 5814) to complete the financial account management function.

[0420] Payment card 5808 need not be directly related to the financial accounts involved with a financial account management function. Instead, authorization server 5810 may, for example, maintain links between various financial accounts that may be owned by a user of a mobile device. Accordingly, for example, while payment card 5808 may not be used as the source account from which money is to be transferred to an auto loan account, payment card 5808 may nevertheless be linked with the source account (e.g., M/C 1234). In so doing, for example, authorization server 5810 may recognize the link between payment card 5808 and the source account (e.g., M/C 1234) and may authorize the money transfer due to the recognized link.

[0421] Payment card 5808 may, for example, be a powered payment card. Accordingly, for example, a dynamic security code may be communicated from payment card 5808 to a processor of mobile device 5802 (e.g., via a discretionary data field of a magnetic stripe message communicated by payment card 5808) along with other identifying information (e.g., at least a portion of a dynamic payment card number or a cardholder's name). In so doing, for example, the dynamic security code and/or other optional identifying information may serve as the security credential that authorizes mobile device 5802 to perform the requested function. The dynamic security code and/or other optional identifying information may, for example, be relayed to authorization server 5810. Accordingly, for example, authorization server 5810 may analyze the security code and any other optional identifying information to determine whether the requested function is to be authorized. If so, the authorization may be communicated by authorization server 5810 to a processor of mobile device 5802 via communication channel 5812 so that the function may be completed.

[0422] FIG. 59 shows system 5900 that may include mobile terminal 5902, key 5908, network 5912 and car 5914. A processor of mobile device 5902 may, for example, execute an automobile application (e.g., GUI 5904) that may allow a user of mobile device 5902 to establish wireless link 5910 between car 5914 and mobile device 5902. Accordingly, for example, a user of mobile device 5902 may communicate wireless commands to car 5914 via wireless communication channel 5910.

[0423] A user may, for example, start his or her car from the convenience and warmth of the user's office at

work when temperatures outside may warrant a time period within which car 5914 may need to warm up. Accordingly, for example, a user may start his or her car via commands communicated by a processor of mobile device 5902 to car 5914 prior to leaving the office for the day. In so doing, for example, a processor of mobile device 5902 may require authorization to issue the command, in which case the user may be challenged to present key 5908 within a communication distance from mobile device 5902 to form contactless communication channel 5906. Security credentials may, for example, be communicated from key 5908 to a processor of mobile device 5902 via contactless communication channel 5906 and the processor may compare the received security credentials to security credentials stored within a memory of mobile device 5902 (or a remote authorization server). If a match is found, for example, a processor of mobile device 5902 may be authorized to issue one or more commands 5916 to car 5914.

[0424] A wireless device of car 5914 may, for example, communicate to a processor of mobile device 5902 via communication channel 5910. Accordingly, for example, once a command is authorized and sent to a wireless device of car 5914 by a processor of mobile device 5902, the wireless device of car 5914 may respond with an acknowledgment that the command (e.g., "Start car") was executed. A wireless device of car 5914 may, for example, provide status to a display of mobile device 5902. Accordingly, for example, a wireless device of car 5914 may report a gasoline level status to mobile device 5902 via communication channel 5910 so that the user of mobile device 5902 may know

that leaving car 5914 running for a length of time may deplete the car's gas reserves.

[0425] FIG. 60 shows GUI 6000, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 6000 may, for example, allow a user of a mobile device to determine how certain functions that may be performed by the mobile device may be authorized. GUI 6000 may, for example, provide authorization options 6002 to determine how the mobile device itself may be authorized for use. A PIN, for example, may be required to be entered in order to activate the mobile device for use. As per another example, a memory of the mobile device may contain information associated with any physical card. Accordingly, for example, authorization to activate the mobile device may require that a user produce a physical card (e.g., a driver's license) that may correspond to a virtual card (e.g., a virtual driver's license) that may be stored within a memory of the mobile device. Alternately, for example, a physical card that corresponds to any virtual card or any virtual bank card stored within a memory of the mobile device may be used to authorize the mobile device for use.

[0426] Banking functions performed by a mobile device may, for example, be authorized as defined by options 6004. A mobile device may, for example, be equipped with scanning capability, such that biometrics (e.g., fingerprints) may be taken from the user of the mobile device and verified before banking functions may be authorized. As per another example, a dynamic security code communicated to a processor of a mobile device by a powered payment card via a contactless

communication channel may authorize banking functions to be performed by the mobile device.

[0427] Functions associated with remote operation of a car may, for example, be authorized as defined by options 6006. A mobile device may, for example, be equipped with a camera, such that only when a picture of an authorized user is taken with the camera and verified by a processor of the mobile device will that user be able to issue remote commands (e.g., unlock driver's door) to the user's car.

[0428] Other functions, such as remote house functions, may be authorized as defined by options 6008. For example, a garage door of a user's house may be commanded to be opened by the user's mobile device, but only if a house key communicates security credentials (e.g., a key code) to a processor of the user's mobile device via a contactless communication channel. Alternately, for example, a user may disable any house functions to be conducted by the user's mobile device.

[0429] FIG. 61 shows flow charts for process sequences 6110-6140. Process sequence 6110 may, for example, execute an authorization setup application (e.g., a GUI) on a mobile device that allows a user of the mobile device to select authorization options (e.g., as in steps 6111-6112) to be enforced by a processor of the mobile device (e.g., as in step 6113). For example, banking functions that may be performed by a mobile device may first require that a physical bank card be placed in proximity to the mobile device so that the physical bank card may communicate security credentials to a processor of the mobile device via a contactless communication channel that may be formed

between the physical banking card and the mobile device. In so doing, for example, a processor of the mobile device may compare the security credentials received from the physical card to security credentials stored within a memory of the mobile device (or remote authorization server). Upon a successful comparison, a processor of a mobile device may authorize banking functions to be performed by the mobile device.

[0430] A memory of a mobile device may, for example, contain a number of virtual cards that may correspond to information communicated to a processor of the mobile device via physical card counterparts to the virtual cards. Such virtual cards may, for example, be selected (e.g., as in step 6121 of sequence 6120) to perform a function in conjunction with the mobile device (e.g., payment information associated with a virtual payment card may be selected to complete a purchase transaction using the mobile device). In step 6122, a user of a mobile device may be required to produce a physical card that corresponds to the selected virtual card. A contactless communication channel (e.g., an RFID communication channel) may be formed between the physical card and the mobile device so that security credentials may be communicated from the physical card to a processor of the mobile device via the contactless communication channel (e.g., as in step 6123). In step 6124, a processor of a mobile device may compare the security credentials to security credentials stored within a memory of the mobile device (or remote authorization server) that corresponds to a physical card. Upon a favorable comparison, a processor of a mobile device may authorize the selected virtual card for use.

[0431] Any function (e.g., non-purchase transactions) that may be performed by a mobile device may be requested (e.g., as in step 6131 of sequence 6130) and challenged (e.g., as in step 6132 of sequence 6130). For example, a processor of a mobile device may be requested to perform any function (e.g., remotely start the engine of a user's car) and a processor of the mobile device may first require security credentials to be presented before the function may be performed. Security credentials may, for example, be any information that may be communicated to a mobile device by a contactless device (e.g., an RFID enabled ignition key) via a contactless communication channel. A processor of the mobile device may authorize the requested function if the security credentials are verified (e.g., as in step 6133) and may deny the requested function if the security credentials are not verified (e.g., as in step 6134).

[0432] In step 6141 of sequence 6140, a user of a mobile device may request a function to be performed by a mobile device. Upon receipt of security credentials communicated by a contactless communication device to a processor of the mobile device (e.g., as in step 6142), the security credentials may be forwarded (e.g., as in step 6143) to a remote authorization server for verification. In step 6144, the remote authorization server may communicate a message to a processor of the mobile device to either grant or deny authorization for the mobile device to perform the requested function.

[0433] FIG. 62 shows card 6200 that may include, for example, a dynamic number that may be entirely, or partially, displayed using a display (e.g., display 6206). A dynamic number may include a permanent

portion such as, for example, permanent portion 6204 and a dynamic portion such as, for example, dynamic portion 6206. Card 6200 may include a dynamic number having permanent portion 6204 and permanent portion 6204 may be incorporated on card 6200 so as to be visible to an observer of card 6200. For example, labeling techniques, such as printing, embossing, laser etching, etc., may be utilized to visibly implement permanent portion 6204.

[0434] Card 6200 may include a second dynamic number that may be entirely, or partially, displayed via a second display (e.g., display 6208). Display 6208 may be utilized, for example, to display a dynamic code such as a dynamic security code. Card 6200 may also include third display 6222 that may be used to display graphical information, such as logos and barcodes. Third display 6222 may also be utilized to display multiple rows and/or columns of textual and/or graphical information.

[0435] Persons skilled in the art will appreciate that any one or more of displays 6206, 6208, and/or 6222 may be implemented as a bi-stable display. For example, information provided on displays 6206, 6208, and/or 6222 may be stable in at least two different states (e.g., a powered-on state and a powered-off state). Any one or more of displays 6206, 6208, and/or 6222 may be implemented as a non-bi-stable display. For example, the display is stable in response to operational power that is applied to the non-bi-stable display. Other display types, such as LCD or electro-chromic, may be provided as well.

[0436] Other permanent information, such as permanent information 6220, may be included within card

6200, which may include user specific information, such as the cardholder's name or username. Permanent information 6220 may, for example, include information that is specific to card 6200 (e.g., a card issue date and/or a card expiration date). Information 6220 may represent, for example, information that includes information that is both specific to the cardholder as well as information that is specific to card 6200.

[0437] Card 6200 may accept user input data via any one or more data input devices, such as buttons 6210-6218. Buttons 6210-6218 may be included to accept data entry through mechanical distortion, contact, or proximity. Buttons 6210-6218 may be responsive to, for example, induced changes and/or deviations in light intensity, pressure magnitude, or electric and/or magnetic field strength. Such information exchange may then be determined and processed by a processor of card 6200 as data input. An RFID chip may, for example, include memory that may be populated with data to be communicated via RFID antenna 6224 when one or more buttons 6210-6218 are pressed. Accordingly, for example, once a button is pressed, RFID data may be loaded into an RFID chip memory and once an RFID communication channel is formed (e.g., once card 6200 is brought within an RFID communication distance of an RFID enabled device) the data in RFID chip memory may be communicated via an RFID communication channel using RFID antenna 6224. Once RFID data is communicated, or after a configurable delay period, the RFID chip memory may be erased.

[0438] FIG. 62 shows architecture 6250, which may include one or more processors 6254. One or more processors 6254 may be configured to utilize external

memory 6252, internal memory of processor 6254, internal memory of RFID chip 6262, or a combination of external memory 6252, internal memory of RFID chip 6262, and internal memory of processor 6254 for dynamically storing information, such as executable machine language, related dynamic machine data, RFID data and user input data values.

[0439] One or more of the components shown in architecture 6250 may be configured to transmit information to processor 6254 and/or may be configured to receive information as transmitted by processor 6254. For example, one or more displays 6256 may be coupled to receive data from processor 6254. The data received from processor 6254 may include, for example, at least a portion of dynamic numbers and/or dynamic codes. The data to be displayed on the display may be displayed on one or more displays 6256.

[0440] One or more displays 6256 may be, for example, touch sensitive and/or proximity sensitive. For example, objects such as fingers, pointing devices, etc., may be brought into contact with displays 6256, or in proximity to displays 6256. Detection of object proximity or object contact with displays 6256 may be effective to perform any type of function (e.g., transmit data to processor 6254). Displays 6256 may have multiple locations that are able to be determined as being touched, or determined as being in proximity to an object.

[0441] Persons skilled in the art will appreciate that a card (e.g., card 6200 of FIG. 62) may, for example, be a self-contained device that derives its own operational power from one or more batteries 6258. Furthermore, one or more batteries 6258 may be

included, for example, to provide operational power for a period of time (e.g., approximately 2-4 years). One or more batteries 6258 may be included, for example, as rechargeable batteries.

[0442] Input and/or output devices may be implemented on architecture 6250. For example, integrated circuit (IC) chip 6260 (e.g., an EMV chip) may be included on architecture 150 to communicate information to a chip reader (e.g., an EMV chip reader) via contacts that may be formed on a surface of a card (e.g., card 6200 of FIG. 62). Other input and/or output devices may be included on architecture 6250, for example, to provide any number of input and/or output capabilities within architecture 6250. For example, other input and/or output devices may include an audio device capable of receiving and/or transmitting audible information. Other input and/or output devices may include a device that exchanges analog and/or digital data using a visible data carrier. Alternately, for example, other input and/or output devices may include a device that is sensitive to a non-visible data carrier, such as an infrared data carrier or electromagnetic data carrier.

[0443] A dynamic magnetic stripe communications device may be included within architecture 6250 to communicate information to, for example, a read-head of a magnetic stripe reader via, for example, electromagnetic signals. For example, electromagnetic field generators 6270-6274 may be included to communicate one or more tracks of electromagnetic data to read-heads of a magnetic stripe reader. Electromagnetic field generators 6270-6274 may include, for example, a series of electromagnetic elements,

where each electromagnetic element may be implemented as a coil wrapped around one or more materials (e.g., a magnetic material and/or a non-magnetic material). Additional materials may be placed outside the coil (e.g., a magnetic material and/or a non-magnetic material).

[0444] Electrical excitation by processor 6254 of one or more coils of one or more electromagnetic elements via, for example, driving circuitry 6264 may be effective to generate electromagnetic fields from one or more electromagnetic elements. One or more electromagnetic field generators 6270-6274 may be utilized to communicate electromagnetic information to, for example, one or more read-heads of a magnetic stripe reader.

[0445] Timing aspects of information exchange between architecture 6250 and the various I/O devices implemented on architecture 6250 may be determined by processor 6254. Detector 6266 may be utilized, for example, to sense the proximity and/or actual contact, of an external device, which in turn, may trigger the initiation of a communication sequence. The sensed presence and/or touch of the external device may then be communicated to a controller (e.g., processor 6254), which in turn may direct the exchange of information with the external device. The sensed presence and/or touch of the external device may be effective to, for example, determine the type of device or object detected.

[0446] For example, the detection may include the detection of, for example, a read-head of a magnetic stripe reader. In response, processor 6254 may activate one or more electromagnetic field generators

6270-6274 to initiate a communications sequence with, for example, one or more read-heads of a magnetic stripe reader. The timing relationships associated with communications between one or more electromagnetic field generators 6270-6274 and one or more read-heads of a magnetic stripe reader may be provided through use of the detection of the magnetic stripe reader.

[0447] Persons skilled in the art will appreciate that processor 6254 may provide user-specific and/or card-specific information through utilization of any one or more of buttons 6210-6218, RFID chip 6262, RFID antenna 6268, IC chip 6260, electromagnetic field generators 6270-6274, and any other input and/or output device. RFID antenna 6268 may, for example, be brought within a communication distance of an RFID enabled device which may be generating a carrier field (e.g., an RF field). In so doing, RFID antenna 6268 may collect energy from the RF field which may then be detected by RFID chip 6262. RFID chip 6262 may, for example, communicate a presence of an RFID communication device to processor 6252. Processor 6252 may, in turn, populate a memory of RFID chip 6262 with user-specific and/or card-specific information (e.g., a payment account number, cardholder name, and a dynamic security code) that may then be communicated to the RFID enabled device via RFID antenna 168.

[0448] RFID antenna 6268 may be configured to receive data from an RFID device (e.g., an RFID tag). Accordingly, for example, RFID chip 6262 may interrogate the capabilities of an RFID device and may receive data from the RFID device upon a determination that the RFID device may communicate data. RFID antenna 6268 may, for example, be provided as two or

more RFID antennas that may be used to enhance RFID data communication and/or reception with an RFID enabled device.

[0449] FIG. 63 shows network topology 6300 that may include, for example, mobile device 6302 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile device 6302 may, for example, include a contactless interface that may initiate, sustain, and/or terminate communication channel 6326 between card 6304 and mobile device 6302. Card 6304 and mobile device 6302 may communicate via channel 6326 via a contactless communication medium (e.g., an RF medium).

[0450] Mobile device 6302 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 6312 and/or payment network 6314) and/or one or more wireless networks (e.g., mobile network 6310). Mobile device 6302 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile device 6302 to communicate information (e.g., voice and data) to cellular network access infrastructure 6306 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 6306 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0451] Mobile device 6302 may, for example, communicate with wireless access point 6308 over a wireless interface (e.g., a Bluetooth interface or a

Wi-Fi interface). Accordingly, for example, mobile device 6302 may access one or more wired networks (e.g., IP network 6312 and/or payment network 6314) and/or one or more wireless networks (e.g., mobile network 6310) without the need to first gain access to cellular network access infrastructure 6306.

[0452] Card 6304 may, for example, be a powered card or a non-powered card (e.g., a powered payment card or a non-powered payment card). Accordingly, for example, payment information (e.g., a payment account number and a card expiration date) may be communicated from card 6304 to mobile device 6302 in support of a financial transaction being conducted by mobile device 6302. In so doing, for example, items for purchase on IP network 6312 (e.g., the internet) may be accessed by a browser of mobile device 6302 via an access point (e.g., wireless access point 6308 or cellular network access infrastructure 6306). Mobile device 6302 may, for example, complete a purchase transaction by first obtaining required payment information from card 6304 and then communicating such payment information to network entities (e.g., payment server 6316 and/or issuer 6320).

[0453] Payment server 6316 may, for example, contact issuer 6320 via a network (e.g., payment network 6314) with payment information received from mobile device 6302 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile device 6302 via any one or more delivery options (e.g., via a short messaging service of mobile network 6310 or an email delivery service of IP network 6312). Mobile device 6302 may allow a user to associate purchase categories

(e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile device so that the user may receive a more detailed accounting of his or her expenditures on his or her receipt. Accordingly, for example, a user may enjoy a higher degree of integration such that a user may customize a level of detail provided on a receipt via mobile device 6302. A payment receipt may, for example, be provided to mobile device 6302 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile device 6302 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0454] A device (e.g., mobile device 6328 and/or card 6322) may, for example, include a contactless communication device (e.g., an RFID device) that may initiate, sustain, and/or terminate a contactless communication channel (e.g., an RFID communications channel) with merchant terminal 6318. Accordingly, for example, card 6322 and/or mobile device 6328 may communicate payment information to merchant terminal 6318 to complete a financial transaction. In so doing, for example, mobile device 6328 and/or card 6322 may first receive a request from a user to communicate payment information to merchant terminal 6318.

[0455] As per an example, a user of card 6322 may press a button on card 6322 that may cause payment information to be transferred to a memory of a processor (e.g., an RFID chip). An associated RFID antenna may, for example, sense the presence of merchant terminal 6318 by detecting an RF carrier field that may be generated by an RFID device of merchant terminal 6318. Once the presence of merchant terminal

6318 is sensed, payment information may be transferred from an RFID chip of card 6322 to an RFID antenna of card 6322 to communicate the payment information via an RFID communication channel to merchant terminal 6318 to complete a financial transaction.

[0456] As per another example, card 6322 may be a non-powered card (e.g., a non-powered payment card). Accordingly, for example, card 6322 may include an RFID chip and associated RFID antenna that may be brought within proximity to merchant terminal 6318. An RFID antenna of card 6322 may sense an RF carrier field generated by merchant terminal 6318 and may derive operational power from the RF carrier field. The operational power may, for example, be collected by an RFID antenna of card 6322 and provided to an associated RFID chip of card 6322 in order to energize the RFID chip of card 6322. Once energized, an RFID chip of card 6322 may modulate an RF carrier field generated by merchant terminal 6318 to, for example, communicate payment information from card 6322 to merchant terminal 218 to complete a purchase transaction.

[0457] Any computing device (e.g., desktop computer 6330) may, for example, provide contactless communication electronics (e.g., an RFID reader) that may communicate with a contactless communication device (e.g., card 6332 and/or mobile device 6334). Accordingly, for example, any information that may be communicated by card 6332 (e.g., payment information) may be received by computing device 6330 (e.g., received via an RFID communication channel established between card 6332 and computing device 6330) and forwarded onto a network entity (e.g., issuer 6320 and/or payment server 6316) to complete a purchase

transaction. Persons skilled in the art will appreciate that any RFID information may be exchanged between computing device 6330 and an RFID enabled device (e.g., card 6332 and/or mobile device 6334).

[0458] FIG. 64 shows mobile device 6400. Mobile device 6400 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, mobile device 6400 may be operated in a mobile environment while a user of mobile device 6400 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 6400 may perform multiple functions simultaneously (e.g., a person may carry on a conversation while at the same time browsing and purchasing products on the internet).

[0459] Mobile device 6400 may include audio processing devices (e.g., microphone 6408 and speaker 6410). Accordingly, for example, mobile device 6400 may receive voice commands from a user via microphone 6408 and may process such commands to perform a function. For example, a user may place mobile device 6400 into a desired operational mode by speaking a command into microphone 6408 that is associated with the desired operational mode. In so doing, for example, mobile device 6400 may engage in hands-free operation by receiving voice commands via microphone 6408 and performing functions associated with the received voice commands.

[0460] Mobile device 6400 may receive data input via microphone 6408. For example, a voice-band modem may generate signals in a voice-band frequency range that

may be received by microphone 6408. A processor of mobile device 6400 may interpret the received audible information as data signals and may process the data signals as, for example, data values and/or control data input.

[0461] Mobile device 6400 may include camera 6402. Camera 6402 may capture one or more frames of video data and store the video data within a memory of mobile device 6400. Accordingly, for example, a processor of mobile device 6400 may receive one or more frames of video information via camera 6402 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 6400 may receive optical information that is sensed by camera 6402 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 6400 as data values and/or control data.

[0462] Mobile device 6400 may include manual input interface 6412. Manual input interface 6412 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 6400 may enter information into mobile device 6400 via manual interface 6412 to cause a processor of mobile device 6400 to enter a particular mode of operation. Manual interface 6412 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile

device 6400) during a particular mode of operation of mobile device 6400.

[0463] Mobile device 6400 may include display 6404. Display 6404 may provide visible information that may be utilized by a user during interaction with mobile device 6400. A portion or all of display 6404 may be touch sensitive such that objects making contact with display 6404 or objects coming within a proximity of display 6404 may be detected by a processor of mobile device 6400. Accordingly, for example, RFID operations graphical user interface 6406 may be provided by display 6404 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, textual input boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 6400.

[0464] FIG. 64 shows architecture 6450. User interface 6452 may, for example, be included within architecture 6450 to allow user interaction with architecture 6450. For example, a dedicated key pad or keyboard may be included within user interface 6452 to allow alphanumeric data entry into architecture 6450.

[0465] Architecture 6450 may include one or more displays 6454. Display 6454 may, for example, be touch-sensitive. Accordingly, for example, display 6454 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 6454. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of

display 6454 may be detected by processor 6458 as alphanumeric data entry.

[0466] Alphanumeric entry boxes may, for example, be rendered onto display 6454. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 6452 and/or a virtual keypad rendered onto display 6454 to select alphanumeric characters to be placed within the alphanumeric entry box in accordance with a character position identified by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 6458 may receive alphanumeric characters as typed into a alphanumeric entry box of display 6454 and may use such alphanumeric characters as data input.

[0467] Display 6454 may, for example, provide data output from architecture 6450. For example, display 6454 may communicate data using a series of light pulses. Accordingly, for example, processor 6458 may cause one or more portions of display 6454 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 6454 via light pulses having varying characteristics. Display 6454 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0468] Architecture 6450 may include one or more transceivers 6456. Transceiver 6456 may communicate information to and/or may receive information from one or more devices. Transceiver 6456 may, for example,

communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly, for example, transceiver 6456 may allow a mobile device (e.g., mobile device 6400 of FIG. 64) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 6400 of FIG. 64) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 356 may exchange information with one or more other mobile devices via one or more associated cellular stations.

[0469] Transceiver 6456 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 6456 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 6456 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 6400 of FIG. 64) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network.

[0470] Architecture 6450 may include RFID chip 6464, RFID antenna 6462, and optional RFID antenna 6466 which may combine to communicate with an RFID enabled device via an RFID communication channel. Accordingly, for example, architecture 6450 may be compatible with any RFID device, such as for example, an RFID enabled card, an RFID reader, and an RFID enabled computing device (e.g., an RFID enabled desktop computer). RFID antenna 6466 may, for example, be provided to enhance RFID data communication and/or reception.

[0471] RFID antenna 6462 and/or RFID antenna 6466 may, for example, establish an RF carrier field that may be modulated by an RFID device (e.g., an RFID tag of a non-powered payment card). In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by RFID antenna 6462 and/or RFID antenna 6466 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to RFID antenna 6462 and/or RFID antenna 6466 by modulating the RF field produced by RFID antenna 6462 and/or RFID antenna 6466.

[0472] A powered card may, for example, communicate with RFID antenna 6462 and/or RFID antenna 6466. A powered card may, for example, include a processor, a battery, a memory, a wireless communications device (e.g., a powered RFID device) and other electronics (e.g., buttons) that may allow a user to interact with the powered card to perform one or more functions. Accordingly, for example, a powered card may be used to communicate specific information to RFID antenna 6462 and/or RFID antenna 6466 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively

communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to RFID antenna 6462 and/or RFID antenna 6466 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications.

[0473] RFID chip 6464 may, for example, receive RFID data from processor 6458 and may store such RFID data temporarily. Accordingly, for example, once an RFID communication channel is formed with an RFID enabled device, RFID data contained within RFID chip 6464 may be communicated to the RFID enabled device via RFID antenna 6462 and/or RFID antenna 6466. RFID antennas 6462 and 6466 may, for example, communicate the same RFID data to an RFID enabled device. RFID antennas 6462 and 6466 may, for example, communicate different RFID data sets to an RFID enabled device and the differences between the RFID data sets communicated may provide multiple other channels of data that may be communicated (e.g., an amplitude difference between RFID data sets may be an RFID data channel and a phase difference between RFID data sets may be an additional RFID data channel).

[0474] Architecture 6450 may include memory 6460 and/or processor 6458 may include internal memory. Accordingly, for example, application code may be stored within memory 6460 and/or processor 6458 and executed by processor 6458 in support of functions performed by architecture 6450. For example, an application (e.g., a graphical user interface) may be executed by processor 6458 and displayed onto display 6454, which may be used to interact with a user of a mobile device (e.g., mobile device 6400 of FIG. 64).

Persons skilled in the art will appreciate that executable application code may be communicated to architecture 6450 via any one or more interfaces of architecture 6450 (e.g., user interface 6452, display 6454, transceiver 6456, and/or RFID antennas 6462 and/or 6466).

[0475] Application data (e.g., payment data) may be temporarily stored within RFID chip 6464 and communicated by RFID antenna 6462 and/or RFID antenna 6466 during operation. For example, payment data may be temporarily communicated to RFID chip 6464 by processor 6458 during a financial transaction being conducted via an RFID communication channel between a mobile device (e.g., mobile device 6400 of FIG. 64) and another RFID device (e.g., a merchant terminal). Once RFID data is communicated (or after a configurable delay period has expired), processor 6458 may cause the payment data stored within RFID chip 6464 to be erased so as to reduce an ability of an RFID skimmer to access data from RFID chip 6464.

[0476] FIG. 65 shows card 6500, which may be a powered card and may include, for example, board 6502, board 6504, dynamic magnetic communications device 6506, RFID chip 6518, board 6508, battery 6514, conductive leads 6520-6526 and RFID antenna 6516. Additional circuitry may be provided on board 6502, which may include, for example, processor 6530, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6506, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons).

[0477] All boards, circuitry, and other components of card 6500 may be laminated to form card assembly 6510. Such a lamination may, for example, be implemented using a series of lamination process steps, such that an electronics package containing boards 6502, 6504, and/or 6508 and associated electronics may be encapsulated by an injection molding process (e.g., a reaction injection molding process), whereby a silicon-based material or a polyurethane-based material may be injected and cured (e.g., using temperature and/or chemical reaction) to form the electronics package. The electronics package may then be sandwiched between layers of laminate (e.g., layers of polymer laminate). Accordingly, for example, both surfaces of card assembly 6510 may be formed by a layer of laminate such that no electrical contacts exist on either surface of card assembly 6510. Alternately, for example, a surface of card assembly 6510 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6510 to provide connectivity from a surface of card assembly 6510 to a processor (e.g., an EMV chip) of card 6500.

[0478] RFID antenna 6516 may, for example, be formed using an additive technique, whereby patterns of a conductive element (e.g., copper) may be applied to a PCB substrate (e.g., applied to either side of board 6508) according to a patterning mask definition layer. RFID antenna 6516 may, for example, be formed using a subtractive technique whereby patterns of a conductive element (e.g., copper) may be removed from a pre-plated PCB substrate (e.g., removed from either side of board 6508) according to an etching mask definition layer. Other non-PCB fabrication techniques may be used to

implement RFID antenna 6516 as may be required by a particular application.

[0479] Conductive leads 6520 and 6522 may, for example, provide electrical conductivity between board 6508 and board 6502. Accordingly, for example, RFID data signals received by RFID antenna 6516 may be communicated to RFID chip 6518 via conductive leads 6520 and 6522. RFID data signals to be communicated by RFID antenna 6516 (e.g., RFID data signals provided to RFID chip 6518 via processor 6530) may, for example, be received from RFID chip 6518 via conductive leads 6520 and 6522. Conductive leads 6524 and 6526 may, for example, provide electrical conductivity between board 6508 and board 6502 so that operational power may be provided to the active electrical components that may exist on board 6502 from battery 6514. Conductive leads 6520-6526, for example, may use conductive adhesive, soldering paste, or any other type of conductive applications to provide electrical conductivity between boards 6508 and 6502.

[0480] FIG. 66 shows card 6600, which may be a powered card and may include, for example, board 6602, board 6604, dynamic magnetic communications device 6606, RFID chip 6618, board 6608, battery 6614, conductive leads 6620-6626 and RFID antenna 6616. Additional circuitry may be provided on board 6602, which may include, for example, processor 6630, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6606, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons). All boards, circuitry, and other components of card 6600

may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6610 having no exposed contacts. Alternately, for example, a surface of card assembly 6610 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6610 to provide connectivity from a surface of card assembly 6610 to a processor (e.g., an EMV chip) of card 6600.

[0481] RFID antenna 6616 may, for example, be formed using additive and/or subtractive techniques to define patterns of a conductive element (e.g., copper) to form RFID antenna 6616 (e.g., on either side of board 6604). Conductive leads 6620 and 6622 may, for example, provide electrical conductivity between board 6604 and board 6602. Accordingly, for example, RFID data signals received by RFID antenna 6616 may be communicated to RFID chip 6618 via conductive leads 6620 and 6622. RFID data signals to be communicated by RFID antenna 6616 (e.g., as may be provided to RFID chip 6618 by processor 6630) may be received from RFID chip 6618 via conductive leads 6620 and 6622. Conductive leads 6624 and 6626 may, for example, provide electrical conductivity between board 6608 and board 6602 so that operational power may be provided to the active electrical components that may exist on board 6602 from battery 6614.

[0482] FIG. 67 shows card 6700, which may be a powered card and may include, for example, board 6702, board 6704, dynamic magnetic communications device 6706, RFID chip 6718, board 6708, battery 6714, conductive leads 6722-6726 and RFID antenna 6716. Additional circuitry may be provided on board 6702,

which may include, for example, processor 6730, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6706, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons). All boards, circuitry, and other components of card 6700 may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6710 having no exposed contacts. Alternately, for example, a surface of card assembly 6710 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6710 to provide connectivity from a surface of card assembly 6710 to a processor (e.g., an EMV chip) of card 6700.

[0483] RFID antenna 6716 may, for example, be formed using additive and/or subtractive techniques to define patterns of a conductive element (e.g., copper) to form RFID antenna 6716 (e.g., on either side of board 6704). One or more conductive leads 6722 may, for example, provide electrical conductivity between RFID chip 6718 of board 6704 and processor 6730 of board 6702. Accordingly, for example, while data exchanged between RFID chip 6718 and RFID antenna 6716 may remain on board 6704, one or more conduction paths 6722 may be provided so that data that is to be communicated by RFID antenna 6716 may first be communicated to RFID chip 6718 by processor 6730 that may exist, for example, on board 6702. Conductive leads 6724 and 6726 may, for example, provide electrical conductivity between board 6708 and board 6702 so that operational power may be provided to the active electrical

components that may exist on boards 6702 and 6704 from battery 6714.

[0484] FIG. 68 shows card 6800, which may be a powered card and may include, for example, board 6802, board 6804, dynamic magnetic communications device 6806, RFID chip 6818, board 6808, battery 6814, conductive leads 6824-6826 and RFID antenna 6816. Additional circuitry may be provided on board 6802, which may include, for example, processor 6830, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6806, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons). All boards, circuitry, and other components of card 6800 may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6810 having no exposed contacts. Alternately, for example, a surface of card assembly 6810 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6810 to provide connectivity from a surface of card assembly 6810 to a processor (e.g., an EMV chip) of card 6800.

[0485] RFID antenna 6816 may, for example, be formed using additive and/or subtractive techniques to define patterns of a conductive element (e.g., copper) to form RFID antenna 6816 (e.g., on a top side of board 6802). Accordingly, for example, RFID antenna 6816 may be applied to board 6802 at a location proximate to a location of board 6804. In so doing, for example, RFID antenna 6816 may be applied to board 6802 below a location where board 6804 attaches to board 6802 and

conduction paths may be extended to RFID chip 6818 from RFID antenna 6816 (e.g., via conductive traces on board 6802). Conductive leads 6824 and 6826 may, for example, provide electrical conductivity between board 6808 and board 6802 so that operational power may be provided to the active electrical components that may exist on board 6802 from battery 6814. Persons skilled in the art will appreciate that RFID antenna 6816 may be placed anywhere on any board (e.g., around a perimeter of board 6802) so as to maximize an effectiveness of RFID antenna 6816.

[0486] Persons skilled in the art will further appreciate that any combination of processors, EMV chips, display drivers, dynamic magnetic stripe communications device drivers, RFID chips, and associated circuitry may be combined into one or more application specific integrated circuits (ASIC). Accordingly, for example, a core processor may interoperate with an ASIC that combines the functionalities of an RFID chip, a dynamic magnetic stripe communications device driver, and a display driver. Alternately, for example, a core processor, RFID chip, a dynamic magnetic stripe communications device driver, a display driver and associated electronics may be consolidated into a single ASIC. As per another example, a core processor and an RFID chip may be provided as discrete components that may interoperate with an ASIC that may be dedicated to dynamic magnetic stripe communications device driver functions and another ASIC that may be dedicated to display driver functions.

[0487] FIG. 69 shows card 6900, which may include multiple RFID antennas (e.g., RFID antennas 6902-6904)

and associated RFID chips (e.g., RFID chips 6906-6908). Additional circuitry may be provided on card 6900, which may include, for example, a processor, an EMV chip, a display, a display driver, driver circuitry for a dynamic magnetic stripe communications device, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons). All boards, circuitry, and other components of card 6900 may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6912 having no exposed contacts. Alternately, for example, a surface of card assembly 6912 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6912 to provide connectivity from a surface of card assembly 6912 to a processor (e.g., an EMV chip) of card 6900.

[0488] Processor 6910 may, for example, provide data to RFID chips 6906 and/or 6908 that may be communicated by RFID antenna 6902 and/or RFID antenna 6904, respectively. Processor 6910 may, for example, receive data from RFID chips 6906 and/or 6908 that may be received by RFID antenna 6902 and/or RFID antenna 6904, respectively.

[0489] Card 6900 may, for example, be placed within a communication distance of one or more RFID devices (e.g., one or more RFID enabled merchant terminals) in order to conduct a purchase transaction. Accordingly, for example, processor 6910 may communicate track 1 and track 2 magnetic stripe data to the RFID enabled merchant terminal via RFID chip 6906 and associated RFID antenna 6902. Alternately, for example, processor

6910 may communicate track 1 and track 2 magnetic stripe data to the RFID enabled merchant terminal via RFID chip 6908 and associated RFID antenna 6904.

[0490] As per another example, processor 6910 may utilize both RFID antennas 6902 and 6904 and associated RFID chips 6906 and 6908, respectively, to increase communication efficiency. Accordingly, for example, processor 6910 may communicate track 1 magnetic stripe data to RFID chip 6906 and track 2 magnetic stripe data to RFID chip 6908, so that track 1 magnetic stripe data may be communicated to an RFID enabled merchant terminal via RFID antenna 6902 and track 2 magnetic stripe data may be communicated to an RFID enabled merchant terminal via RFID antenna 6904. In so doing, for example, two tracks of magnetic stripe data may be communicated in half the time.

[0491] As per yet another example, RFID data communicated to RFID chips 6906 and 6908 by processor 6910 may be communicated in a fashion such that multiple channels of information may be communicated in addition to the first and second channels of information communicated by RFID chips 6906 and 6908. For example, phase, frequency, and/or amplitude differences between data communicated by RFID chip 6906/RFID antenna 6902 and data communicated by RFID chip 6908/RFID antenna 6904 may be used to communicate multiple channels of information. Accordingly, for example, a first set of information may be communicated by RFID chip 6906/RFID antenna 6902, a second set of information may be communicated by RFID chip 6908/RFID antenna 6904, and a third set of information may be communicated as an amplitude difference between each data element of the first and second information sets.

A fourth set of information may be communicated, for example, as a phase difference between each data element of the first and second data sets. A fifth set of information may be communicated, for example, as a rate of change of the phase difference (e.g., frequency difference) between each data element of the first and second information sets. Persons skilled in the art will appreciate that any number of channels of information may be communicated by a pair of RFID communicators when differences between RFID data sets communicated by each RFID communicator are exploited as data channels.

[0492] A pair of RFID communicators may, for example, be used to increase accuracy of RFID data communicated. For example, the same RFID data may be communicated by RFID chip 6906/RFID antenna 6902 as is communicated by RFID chip 6908/RFID antenna 6904 so as to increase a probability that an RFID reader may receive RFID data that was intended to be communicated. Accordingly, for example, an RFID reader that may be spatially oriented such that data reception quality from a first RFID communicator is diminished in relation to a data reception quality from a second RFID communicator, may nevertheless receive a complete set of RFID data due to the redundant RFID communication configuration.

[0493] An RFID reader may, for example, employ collision avoidance algorithms, so that communications received from a first RFID communicator do not trump communications received from a second RFID communicator. Accordingly, for example, processor 6910 of card 6900 may communicate to such an RFID reader that dual RFID communicators may be present within card

6900. In so doing, for example, the RFID reader may activate its collision avoidance algorithm to accept RFID communications from both RFID communicators (e.g., RFID chip 6906/RFID antenna 6902 and RFID chip 6908/RFID antenna 6904) simultaneously.

[0494] RFID data may, for example, be received by RFID chip 6906/RFID antenna 6902 and RFID chip 6908/RFID antenna 6904. Accordingly, for example, card 6900 may be an RFID reader that may utilize a pair of RFID readers (e.g., a first RFID reader is provided by RFID chip 6906/RFID antenna 6902 and a second RFID reader is provided by RFID chip 6908/RFID antenna 6904). In so doing, for example, processor 6910 may impose an RFID communication protocol that accepts RFID data form each RFID reader simultaneously.

[0495] FIG. 70 shows card 7000 that may include, for example, configuration 7002. Configuration 7002 may include, for example, button 7004, button 7008, display 7006 and display 7010. Button 7004 may be associated with display 7006. Button 7004 may be pressed to utilize the option described by display 7006. Button 7008 may be associated with display 7010. Button 7008 may be pressed to utilize the option described by display 7010. A card may include additional buttons or displays or may not include the number of buttons or displays of card 7000. For example, a card may include only a single button (e.g., button 7004).

[0496] A user of card 7000 may, for example, select options 7006 or 7010 when card 7000 is to be used (e.g., when card 7000 is to be utilized at a point-of-sale terminal to complete a purchase transaction). Accordingly, for example, a user of card 7000 may press button 7004 to select option 7006 if the user wishes to

exchange RFID data between card 7000 and an RFID device. Alternately, for example, a user of card 7000 may press button 7008 to select option 7010 if the user wishes to communication information to a magnetic stripe reader.

[0497] A user may, for example, press button 7008 to prepare card 7000 for communications with a magnetic stripe reader. Accordingly, for example, a processor of card 7000 may initiate a mode of operation upon activation of option 7010, whereby the processor searches for the presence of a read-head housing of a magnetic stripe reader. Once option 7010 is activated, a user may bring card 7000 within a communication distance of a magnetic stripe reader (e.g., the user may swipe card 7000 through a magnetic stripe reader). Upon the detection of the read-head housing of the magnetic stripe reader, the processor may communicate one, two, and/or three tracks of magnetic stripe data to a read-head of the detected magnetic stripe reader via dynamic magnetic stripe communications device 7014.

[0498] Alternately, for example, a user may press button 7004 to prepare card 7000 for communication with an RFID device. Accordingly, for example, a processor of card 7000 may initiate a mode of operation upon activation of option 7006, whereby a processor of card 7000 provides magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to an RFID chip of card 7000. Once option 7006 is activated, a user may bring card 7000 within a communication distance of an RFID reader (e.g., the user may wave card 7000 within an RFID communication distance of an RFID reader) and an RFID communication sequence between card 7000 and an RFID reader may be completed where

RFID data may be provided to RFID antenna 7012 from an RFID chip on card 7000 and communicated from RFID antenna 7012 to the RFID reader.

[0499] Upon activation of option 7006, a processor of card 7000 may activate passive RFID communications or active RFID communications using RFID antenna 7012 and an associated RFID chip. Passive RFID communications, for example, may require little or no energy to be expended by card 7000. Instead, RFID antenna 7012 may collect energy from an RFID reader when a user of card 7000 brings card 7000 within a communication distance of the RFID reader. The energy collected by RFID antenna 7012 may, for example, provide power to an RFID chip of card 7000. In so doing, for example, an RFID chip of card 7000 may communicate with a processor of card 7000, so that the processor may populate a memory of the RFID chip with information (e.g., payment information) that may be needed to complete a transaction (e.g., a purchase transaction). Once populated with information, the RFID chip of card 7000 may communicate the information to RFID antenna 7012, which may then communicate the information to the RFID reader.

[0500] Active RFID communications from card 7000 may, for example, utilize battery power from within card 7000. Accordingly, for example, once card 7000 is brought within a communication distance of an RFID reader, RFID antenna 7012 may detect the RFID reader and may wake an RFID chip from a low-power state. In so doing, for example, an RFID antenna 7012 may detect energy from an RFID reader and an RFID chip of card 7000 may utilize battery power of card 7000 to receive information from a processor of card 7000 and to

provide the received information to RFID antenna 7012 for subsequent communication to an RFID reader.

[0501] Card 7000 may, for example, operate as an RFID reader, such that when brought within a communication distance of another RFID device, an RFID chip of card 7000 may interrogate the RFID device to determine whether the RFID device is to receive information from card 7000 (e.g., the RFID device is operating as an RFID reader) or whether the RFID device is to communicate information to card 7000 (e.g., the RFID device is operating as an RFID tag). Accordingly, for example, an RFID chip of card 7000 may interrogate the RFID device to determine that the RFID device is an RFID tag an that RFID data may be communicated from the RFID device to an RFID chip of card 7000. In so doing, for example, an RFID chip of card 7000 may receive information, such as executable machine code, payment information, or any other type of information that may be required by card 7000 to operate as intended and may forward such information to a processor of card 7000 to be stored within a memory of card 7000. As per one example, an RFID chip of card 7000 may receive personalization information (e.g., cardholder information and cardholder account information) to prepare card 7000 for use as a payment card.

[0502] FIG. 71 shows system 7100, which may include card 7102 and one or more RFID devices (e.g., mobile devices 7104 and 7106). Card 7102 may, for example, communicate with multiple RFID devices simultaneously. A user of card 7102 may, for example, enable RFID communications with card 7102 by pressing one of buttons 7112 or 7114. Accordingly, for example, payment information (e.g., payment account number and

cardholder name) may be communicated from a core processor within card 7102 and stored within one or more RFID chips of card 7102. Data indicative of which button was pushed (e.g., discretionary data indicative of either credit button 7112 or debit button 7114) may also be communicated and stored within the one or more RFID chips of card 7102.

[0503] As per one example, card 7102 may provide two RFID communication devices that may detect an RF carrier field that may be generated by each of mobile devices 7104 and 7106. Users of mobile devices 7104 and 7106 may, for example, be husband and wife who may wish to store payment information associated with card 7102 on respective memory locations of mobile devices 7104 and 7104 so that such payment information may be used to complete purchase transactions using mobile devices 7104 and 7106.

[0504] A first RFID communication device of card 7102 may establish RFID communication channel 7110 with an RFID reader of mobile device 7104 and a second RFID communication device of card 7102 may establish communication channel 7108 with an RFID reader of mobile device 7106. Accordingly, for example, the first and second RFID communication devices of card 7102 may communicate payment information temporarily stored within an RFID chip of each respective RFID communication device of card 7102. In so doing, for example, mobile devices 7104 and 7106 may store payment information communicated via RFID communication channels 7110 and 7108, respectively, within respective memory locations of mobile devices 7104 and 7106. Mobile devices 7104 and 7106 may later recall such payment information from their respective memory

locations, communicate the stored payment information via channels 7116 and 7118, respectively, of payment network 7120, and complete payment transactions with network entity 7122 using payment information received from card 7102.

[0505] FIG. 72 shows system 7200, which may include mobile device 7202, a stationary device (e.g., desktop computer 7204), payment network 7206, and network entity 7208. An application (e.g., RFID operations GUI 7212) may be executed by a processor of mobile device 7202 and may, for example, report a detection of an RFID device to a display of mobile device 7202. Such an RF device may, for example, include any device (e.g., desktop computer 7204) that may be RFID equipped. An RFID antenna and associated RFID chip may, for example, exist within desktop computer 7204 such that when mobile device 7202 is brought within an RFID communication distance of desktop computer 7204, an RFID antenna of mobile device 7202 may detect its presence, report the same to an RFID chip within mobile device 7202, which may then be reported to a processor of mobile device 7202 and reported to a user of mobile device 7202 via GUI 7212.

[0506] GUI 7212 may, for example, ask the user of mobile device 7202 whether he or she wishes to allow an RFID connection between mobile device 7202 and desktop computer 7204. The user may indicate his or her wish via radio buttons 7214 and may also indicate whether information (e.g., payment information) stored within a memory of mobile device 7202 is to be communicated to desktop computer 7204 via an RFID communication channel previously authorized by the user of mobile device 7202 (e.g., by selecting one of radio buttons 7216). If so,

then such information may be communicated to desktop computer 7204 by mobile device 7202 and stored within a memory of desktop computer 7204. In so doing, for example, payment information communicated by mobile device 7202 to desktop computer 7204 may subsequently be communicated by desktop computer 7204 via communication channel 7210 of payment network 7206 to complete a purchase transaction (e.g., an online purchase of items contained within a shopping cart generated by an internet browser of desktop computer 7204) via network entity 7208.

[0507] A flow diagram of communication sequences is shown in FIG. 73. Step 7311 of sequence 7310 may, for example, include activating an RFID search within a card. Accordingly, for example, a user interface (e.g., one or more buttons) of a card may be associated with a communication feature on the card, whereby pressing one of the buttons may activate an RFID communication device on the card. In step 7312, an RFID device may be detected by the card and an RFID connection may be established between the card and the RFID device. RFID data may, for example, be transferred to an RFID chip on the card (e.g., as in step 7313) and the RFID data contained within an RFID chip on the card may, for example, be communicated via an RFID antenna on the card to the RFID device (e.g., as in step 7314). Once RFID data is communicated, RFID data contained within an RFID chip on the card may be erased so as to reduce a likelihood of skimming RFID data from the RFID chip on the card.

[0508] Step 7321 of sequence 7320 may, for example, include activating an RFID search within a mobile device. Accordingly, for example, a user interface

(e.g., a GUI executing on a processor of the mobile device) may be associated with a communication feature on the mobile device, whereby interfacing with the GUI may activate an RFID communication channel between a detected RFID device and the mobile device (e.g., as in step 7322). In step 7323, RFID data may, for example, be transferred to an RFID chip on the mobile device and the RFID data contained within an RFID chip on the mobile device may, for example, be communicated via an RFID antenna on the mobile device to the RFID device (e.g., as in step 7324). Once RFID data is communicated, RFID data contained within an RFID chip on the mobile device may be erased so as to reduce a likelihood of skimming RFID data from the RFID chip on the mobile device.

[0509] Step 7331 of sequence 7330 may, for example, include transferring RFID data from a core processor to an RFID chip on a card or a mobile device in preparation for communicating the RFID data via an RFID antenna on the card or the mobile device. If a timeout period that may be set in step 7332 expires before the RFID data is communicated by the card or mobile device (e.g., as in step 7333), then RFID data previously transferred to the RFID chip may be erased from the RFID chip by the core processor.

[0510] Step 7341 of sequence 7340 may, for example, include transferring RFID data from a core processor to an RFID chip on a card or a mobile device in preparation for communicating the RFID data via two RFID antennas on the card or the mobile device. In step 7342, the same data may be transferred to both RFID antennas. Alternately, for example, different data may be transferred each RFID antenna. In step

7343, both RFID antennas may communicate data to an RFID reader. As per one example, the same data may be communicated by both RFID antennas so as to increase a reliability of data communication. As per another example, different data may be communicated by each RFID antenna in order to increase an efficiency of data communication. As per yet another example, different data may be communicated by each RFID antenna, where differences (e.g., phase, frequency, and/or amplitude) may be used to communicate multiple other data channels.

[0511] Persons skilled in the art will appreciate that the present invention is not limited to only the embodiments described. Instead, the present invention more generally involves mobile information and the exchange thereof. Persons skilled in the art will also appreciate that the apparatus of the present invention may be implemented in other ways than those described herein. All such modifications are within the scope of the present invention, which is limited only by the claims that follow.

What is claimed is:

1. A method, comprising:

accessing a network using a mobile device;

selecting an object for purchase from said network using said mobile device;

communicating payment information from a payment card to said mobile device using a contactless communication channel; and

communicating said payment information from said mobile device to said network to complete a purchase transaction for said object.

2. A method, comprising:

communicating source account information to a first mobile device using a first contactless communication channel;

communicating target account information to a second mobile device using a second contactless communication channel;

communicating said target account information from said second mobile device to said first mobile device; and

coordinating a money transfer from said source account into said target account using said first mobile device.

3. The method of claim 1, wherein said mobile device is a laptop computer.

4. The method of claim 1, wherein said mobile device is a PDA.

5. The method of claim 1, wherein said mobile device is a phone.

6. The method of claim 1, wherein said contactless communication channel is an RFID communication channel.

7. The method of claim 1, wherein said mobile device and said payment card are brought within a proximity distance of up to two inches to establish said contactless communication channel.

8. The method of claim 1, wherein said payment card is a powered card.

9. The method of claim 1, wherein said payment card is a non-powered card.

10. The method of claim 1, wherein said payment card simulates a series of touches to a display of said mobile device to establish at least a portion of said contactless communication channel.

11. The method of claim 1, wherein said mobile device communicates an optical data stream to said payment card to establish at least a portion of said contactless communication channel.

12. The method of claim 2, wherein a powered card communicates said target account information.

13. The method of claim 2, wherein a non-powered card communicates said target account information.

14. The method of claim 2, wherein a powered card communicates said source account information.

15. The method of claim 2, wherein a non-powered card communicates said source account information.

16. The method of claim 2, wherein said first mobile device is a laptop computer.

17. The method of claim 2, wherein said first mobile device is a PDA.

18. The method of claim 2, wherein said first mobile device is a phone.

19. The method of claim 2, wherein said second mobile device is a laptop computer.

20. The method of claim 2, wherein said second mobile device is a PDA.

21. The method of claim 2, wherein said second mobile device is a phone.

22. A method, comprising:

establishing a contactless communication channel between one or more physical cards and a mobile device;

communicating information from said physical card to said mobile device using said contactless communication channel;

creating a mobile wallet of virtual cards within a memory of said mobile device from said communicated information; and

selecting one of said virtual cards to complete a purchase transaction using said mobile device.

23. The method of claim 22, wherein said mobile device is a laptop.

24. The method of claim 22, wherein said mobile device is a PDA.

25. The method of claim 22, wherein said mobile device is a phone.

26. The method of claim 22, wherein said mobile device is an MP3 device.

27. The method of claim 22, wherein said mobile device is a GPS device.

28. The method of claim 22, wherein said physical card is a non-powered card.

29. The method of claim 22, wherein said physical card is a powered card.

30. The method of claim 22, wherein said contactless communication channel is an RFID communication channel.

31. The method of claim 22, wherein said mobile device and said physical card are brought within a proximity distance of up to two inches to establish said contactless communication channel.

32. The method of claim 22, wherein said physical card simulates a series of touches to a display of said mobile device to establish at least a portion of said contactless communication channel.

33. The method of claim 22, wherein said mobile device communicates an optical data stream to said physical card to establish at least a portion of said contactless communication channel.

34. The method of claim 22, wherein establishing said contactless communication channel comprises entering a PIN associated with said physical card to authorize said communicated information.

35. The method of claim 22, wherein said communicated information is selected based on manual input entered into said physical card.

36. The method of claim 22, wherein said communicated information includes payment information associated with a first payment account selected by pressing a first button of said physical card.

37. The method of claim 22, wherein said virtual cards include gift cards.

38. The method of claim 22, wherein said mobile device includes a graphical user interface to modify a visual appearance of said virtual cards as displayed by said mobile device.

39. The method of claim 22, wherein said communicated information is used to create a visual appearance of said virtual cards as displayed by said mobile device.

40. The method of claim 22, wherein said virtual cards are sorted onto a display of said mobile device based on manual input selection received by a graphical user interface of said mobile device.

41. The method of claim 22, wherein completing said purchase transaction includes establishing a second contactless communication channel between said mobile device and a merchant terminal and communicating payment information associated with said selected virtual card to said merchant terminal via said second contactless communication channel.

42. A method, comprising:

executing an application on a processor of a mobile device to perform a function;

communicating information to said mobile device from a contactless device using a contactless communication channel;

confirming said communicated information matches at least a portion of predetermined information; and

executing said function from said mobile device based on said confirmation.

43. The method of claim 42, wherein said mobile device is a laptop.

44. The method of claim 42, wherein said mobile device is a PDA.

45. The method of claim 42, wherein said mobile device is a phone.

46. The method of claim 42, wherein said mobile device is an MP3 device.

47. The method of claim 42, wherein said mobile device is a GPS device.

48. The method of claim 42, wherein said contactless device is a non-powered card.

49. The method of claim 42, wherein said contactless device is a powered card.

50. The method of claim 42, wherein said contactless device is an automobile key.

51. The method of claim 42, wherein said contactless device is a home door key.

52. The method of claim 42, wherein said contactless device is a key to a safe deposit box.

53. The method of claim 42, wherein said contactless communication channel is an RFID communication channel.

54. The method of claim 42, wherein a camera of said mobile device establishes said contactless communication channel.

55. The method of claim 42, wherein said contactless device is a powered card, said mobile device and said powered card being brought within a proximity distance of up to two inches to establish said contactless communication channel.

56. The method of claim 42, wherein said contactless device is a powered card, said powered card simulating a series of touches to a display of said mobile device to establish at least a portion of said contactless communication channel.

57. The method of claim 42, wherein said contactless device is a powered card, said mobile device communicating an optical data stream to said powered card to establish at least a portion of said contactless communication channel.

58. The method of claim 42, wherein said predetermined information exists on a memory of said mobile device.

59. The method of claim 42, wherein said predetermined information exists on a memory of a remote authorization server.

60. The method of claim 42, wherein said contactless device is a non-powered card, said non-powered card providing said communicated information to authorize a purchase transaction based on payment account information associated with said non-powered card.

61. The method of claim 42, wherein said function is executed by a device external to said mobile device.

62. A card, comprising:

a first board including a first RFID chip and a first RFID antenna; and

a second board including a processor, wherein first data is transferred from said processor to said first RFID chip via conductive terminals between said first and second boards and wherein said first data is communicated from said first RFID chip to a first RFID communication channel via said first RFID antenna.

63. A card, comprising:

a first board including a first RFID antenna; and

a second board including a first RFID chip and a processor, wherein first data is transferred from said processor to said RFID chip and wherein said first data is communicated from said first RFID chip to a first RFID communication channel via said first RFID antenna.

64. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, said first and second data being the same.

65. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel

via said second RFID antenna, said first and second data being different.

66. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a difference between said first and second data forms information for a third RFID communication channel.

67. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a first difference between said first and second data forms information for a third RFID communication channel and a second difference between said first and second data forms information for a fourth RFID communication channel.

68. The card of claim 62, wherein said first data is erased from said first RFID chip after said first data is communicated from said first RFID chip to said first RFID communication channel.

8. The card of claim 1, wherein said first data is erased from said first RFID chip after a delay period has expired.

69. The card of claim 62, wherein said first and second boards are encapsulated, said encapsulation being laminated between first and second lamination layers.

70. The card of claim 62, further comprising a dynamic magnetic stripe communications device.

71. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, said first and second data being the same.

72. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, said first and second data being different.

73. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a first difference between said first and second data forms information for a third RFID communication channel.

74. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a first difference between said first and second data forms information for a third RFID communication channel and a second difference between said first and second data forms information for a fourth RFID communication channel.

75. The card of claim 63, wherein said first data is erased from said first RFID chip after said first data is communicated from said first RFID chip to said first RFID communication channel.

76. The card of claim 63, wherein said first data is erased from said first RFID chip after a delay period has expired.

77. The card of claim 63, wherein said first and second boards are encapsulated, said encapsulation being laminated between first and second lamination layers.

78. The card of claim 63, further comprising a dynamic magnetic stripe communications device.

79. A method comprising:

communicating first data from a device to a reader via a first RFID communication channel;

communicating second data from said device to said reader via a second RFID communication channel;

receiving said first and second data via said reader; and

avoiding collisions between said first and second data within said reader.

80. The method of claim 79, wherein said first and second data are different.

81. A system, comprising:

means for accessing a network;

means for selecting an object for purchase from said network;

means for communicating payment information from a payment card to a mobile device; and

means for communicating said payment information from said mobile device to a network to complete a purchase transaction for said object.

82. A system, comprising:

means for communicating source account information to a first mobile device;

means for communicating target account information to a second mobile device;

means for communicating said target account information from said second mobile device to said first mobile device; and

means for coordinating a money transfer from said source account into said target account.

83. A system, comprising:

means for establishing a contactless communication channel between one or more physical cards and a mobile device;

means for communicating information from said physical card to said mobile device using said contactless communication channel;

means for creating a mobile wallet of virtual cards within a memory of said mobile device from said communicated information; and

means for selecting one of said virtual cards to complete a purchase transaction using said mobile device.

84. A system, comprising:

means for executing an application on a mobile device to perform a function;

means for communicating information to said mobile device from a contactless device;

means for confirming said communicated information matches at least a portion of predetermined information; and

means for executing said function from said mobile device based on said confirmation.

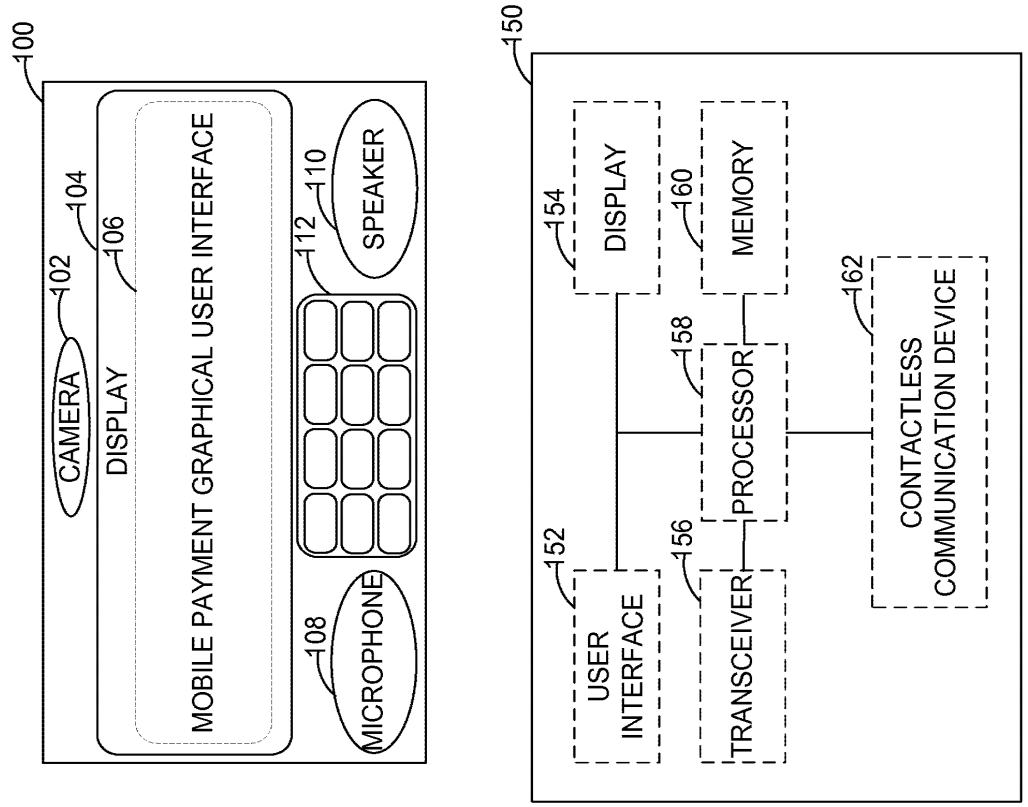

100
CAMERA
102
104
DISPLAY
106
MOBILE PAYMENT GRAPHICAL USER INTERFACE
112
110
SPEAKER
MICROPHONE
108
150
154
DISPLAY
160
MEMORY
158
PROCESSOR
162
CONTACTLESS COMMUNICATION DEVICE
152
USER INTERFACE
156
TRANSCEIVER

FIG. 1

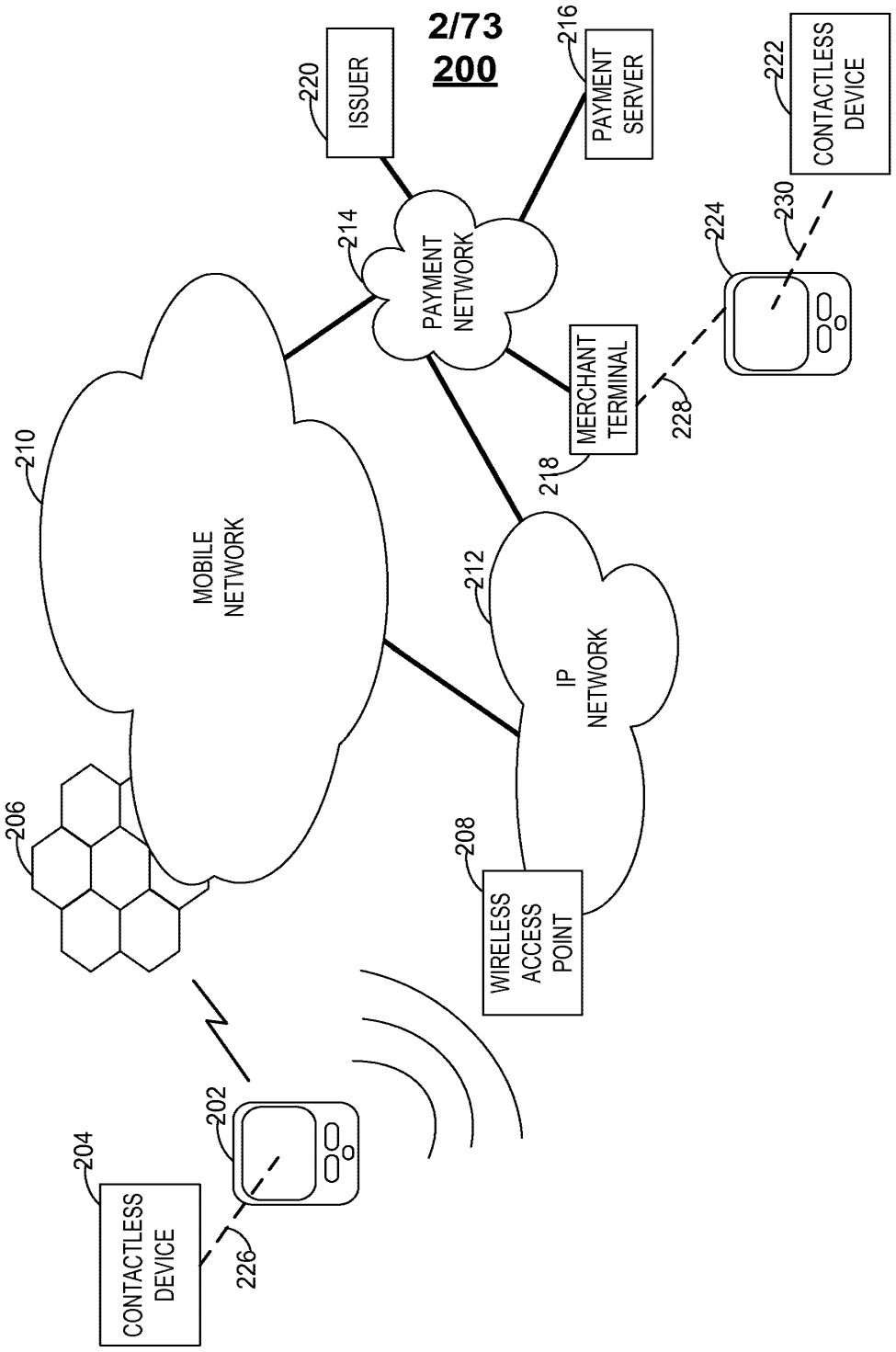

2/73
200
ISSUER
220
PAYMENT SERVER
216
CONTACTLESS DEVICE
222
PAYMENT NETWORK
214
MOBILE NETWORK
210
MERCHANT TERMINAL
218
224
230
228
IP NETWORK
212
206
208
WIRELESS ACCESS POINT
202
204
CONTACTLESS DEVICE
226

FIG. 2

300

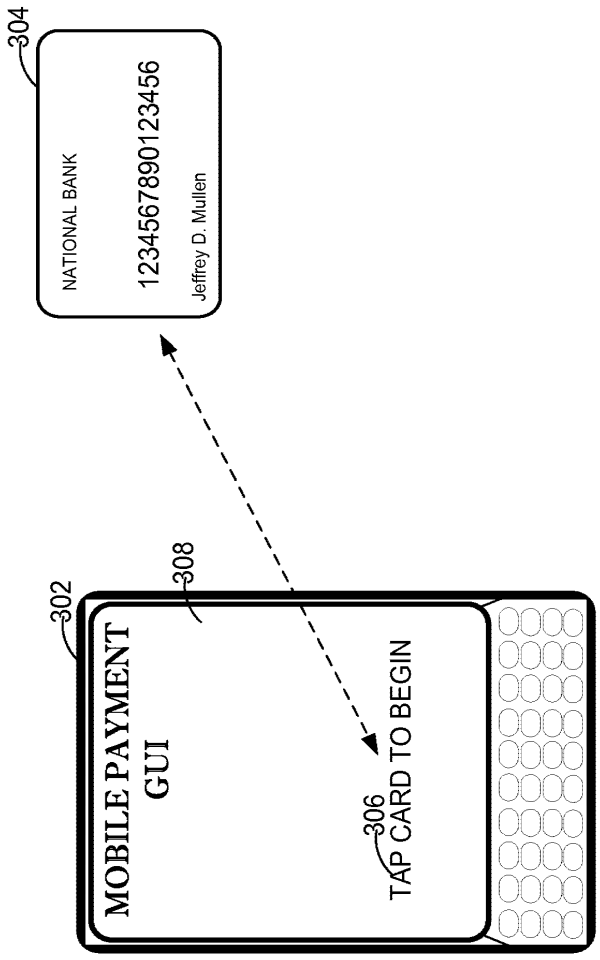

304
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
308
302
MOBILE PAYMENT
GUI
306
TAP CARD TO BEGIN

FIG. 3

400

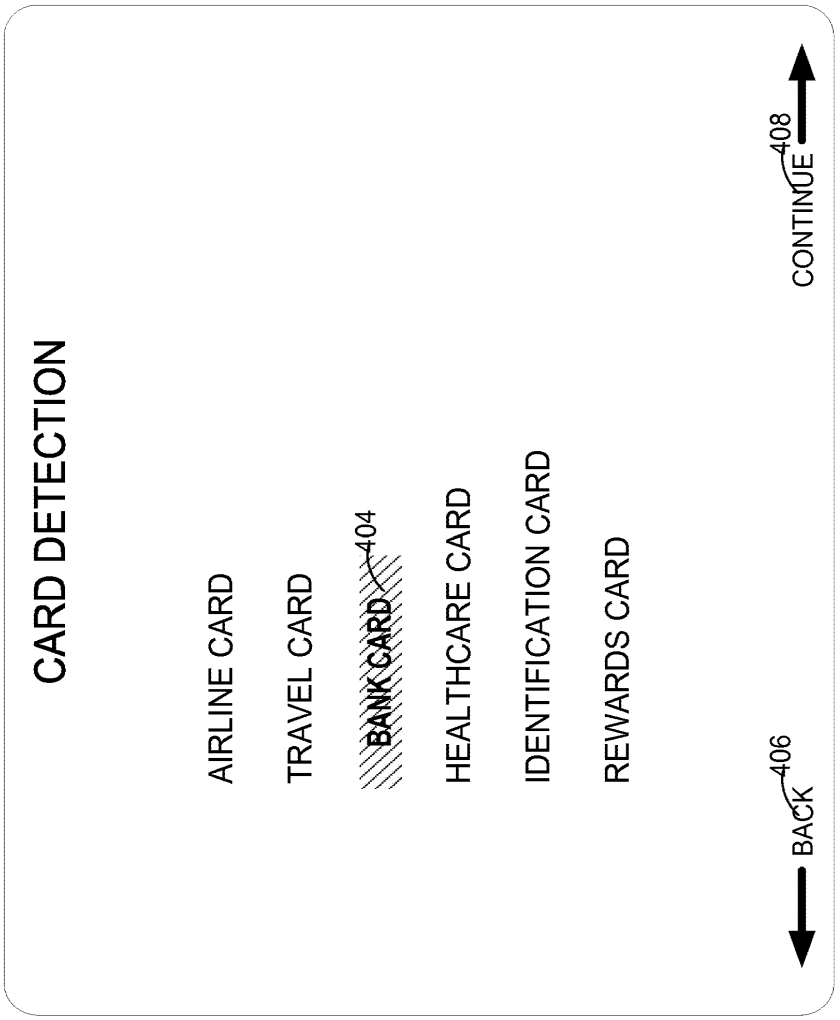

CARD DETECTION
AIRLINE CARD
TRAVEL CARD
BANK CARD
404
HEALTHCARE CARD
IDENTIFICATION CARD
REWARDS CARD
BACK
406
CONTINUE
408

FIG. 4

500

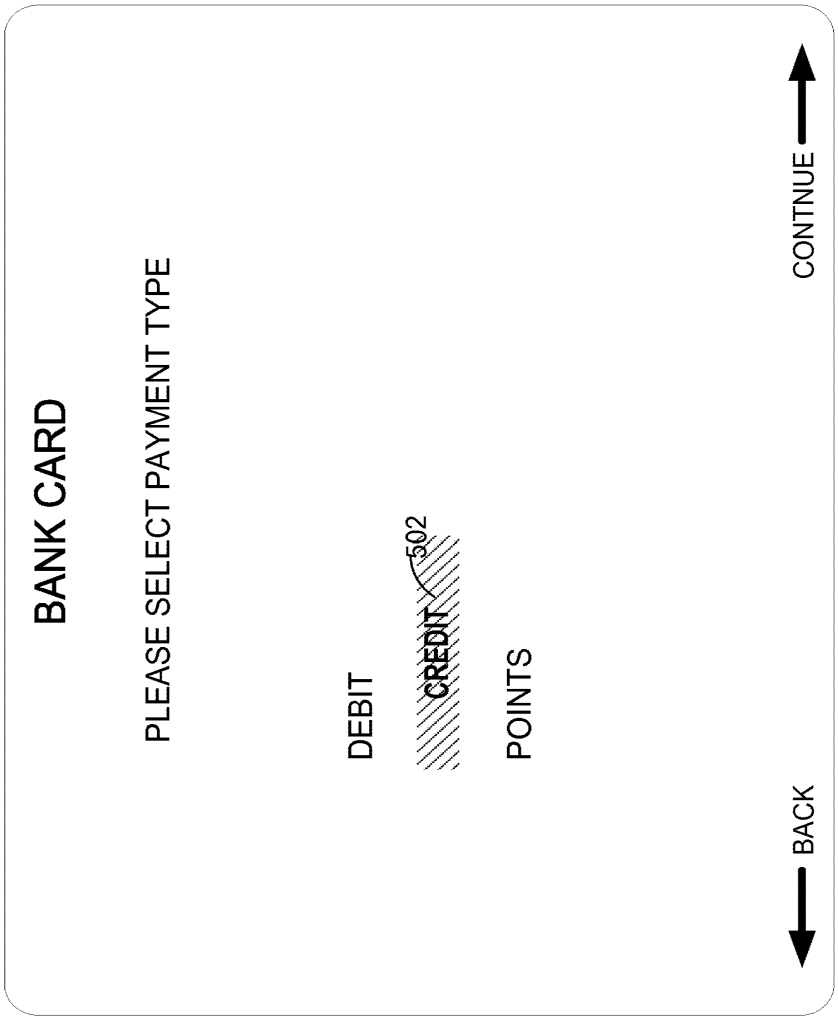

BANK CARD
PLEASE SELECT PAYMENT TYPE
DEBIT
CREDIT
502
POINTS
CONTNUE
BACK

FIG. 5

600

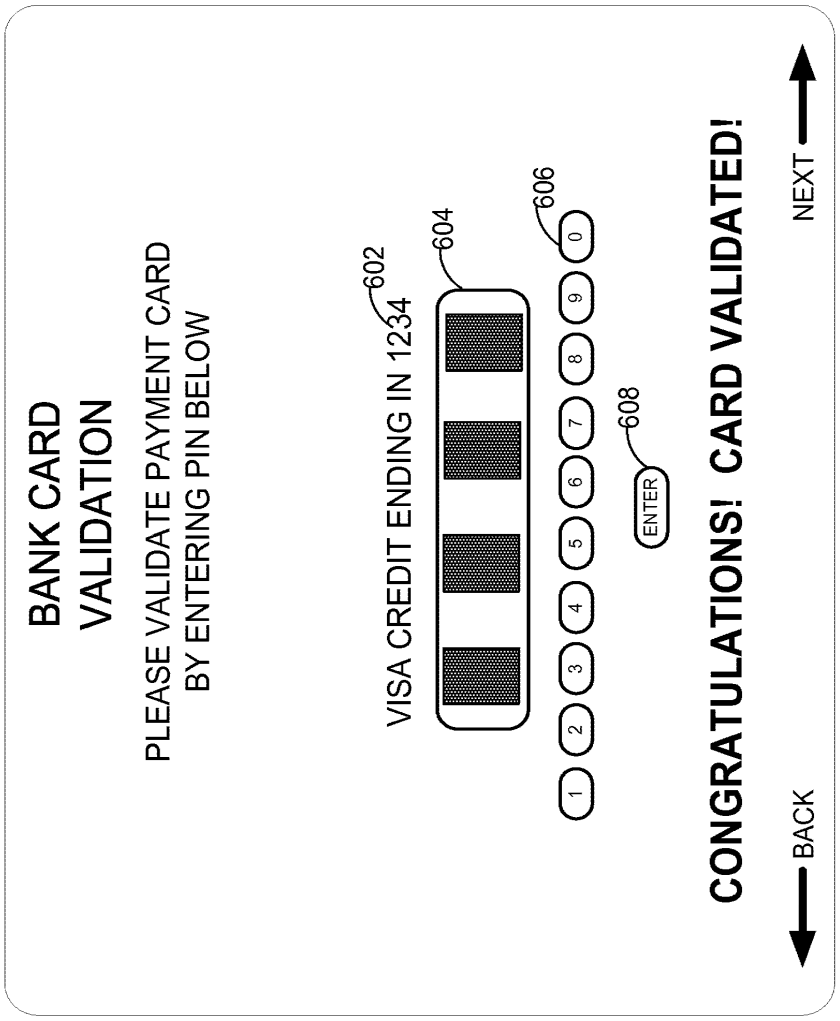

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING PIN BELOW
VISA CREDIT ENDING IN 1234
602
604
606
1
2
3
4
5
6
7
8
9
0
ENTER
608
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 6

700

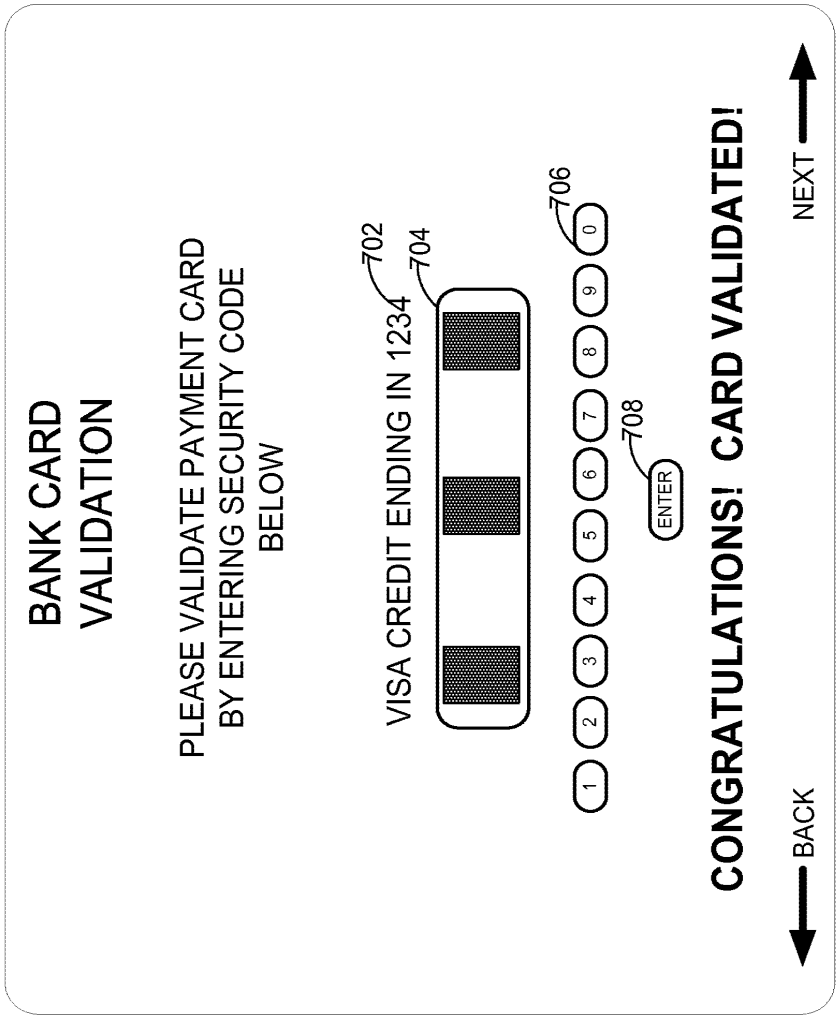

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING SECURITY CODE
BELOW
VISA CREDIT ENDING IN 1234
702
704
706
708
1
2
3
4
5
6
7
8
9
0
ENTER
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 7

800

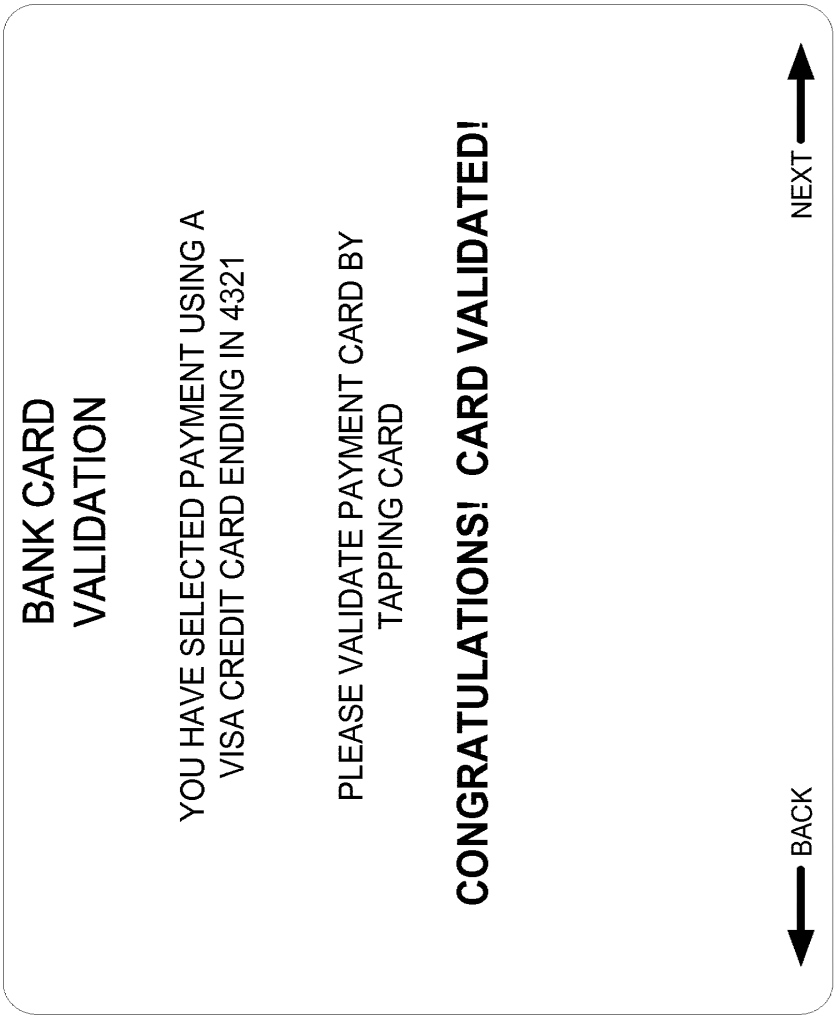

BANK CARD
VALIDATION
YOU HAVE SELECTED PAYMENT USING A
VISA CREDIT CARD ENDING IN 4321
PLEASE VALIDATE PAYMENT CARD BY
TAPPING CARD
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 8

900

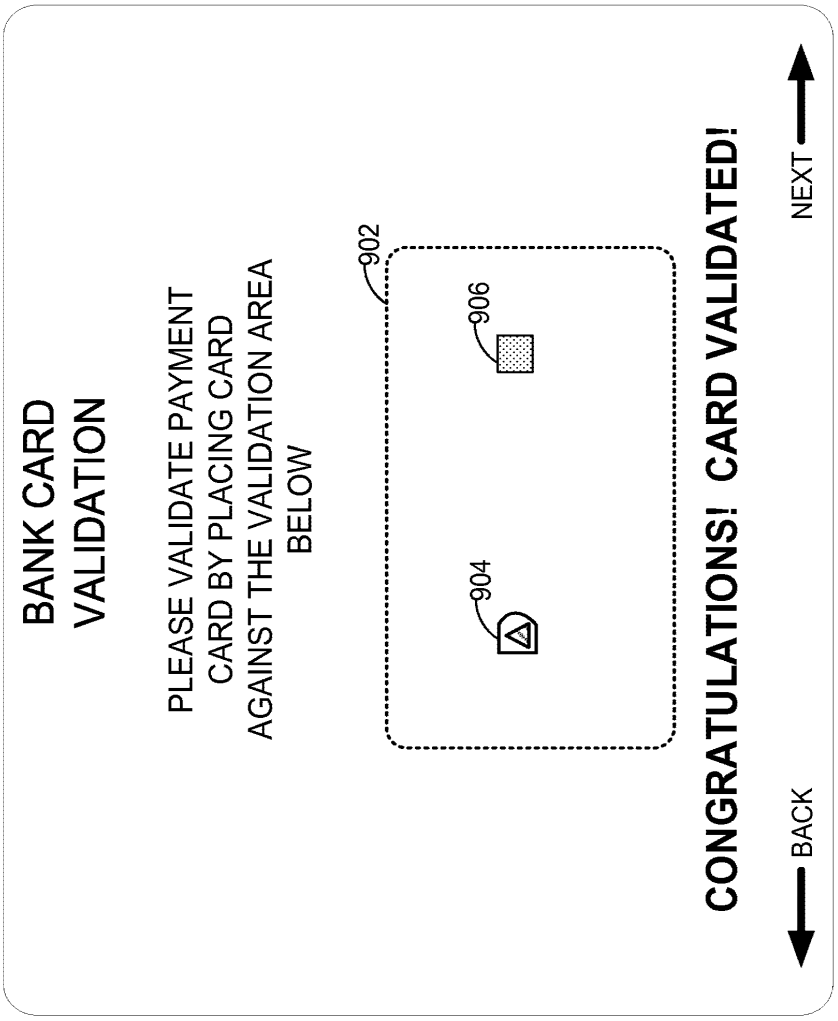

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT
CARD BY PLACING CARD
AGAINST THE VALIDATION AREA
BELOW
902
906
904
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 9

1000

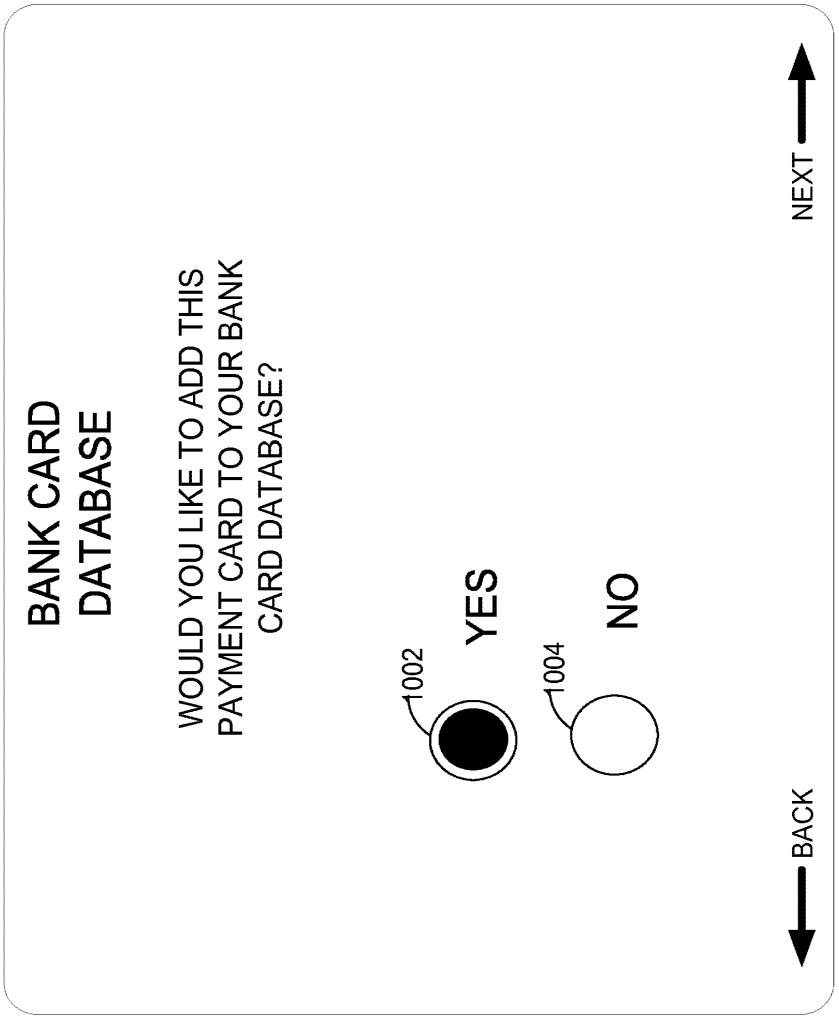

BANK CARD DATABASE
WOULD YOU LIKE TO ADD THIS PAYMENT CARD TO YOUR BANK CARD DATABASE?
1002
YES
1004
NO
NEXT
BACK

FIG. 10

1100

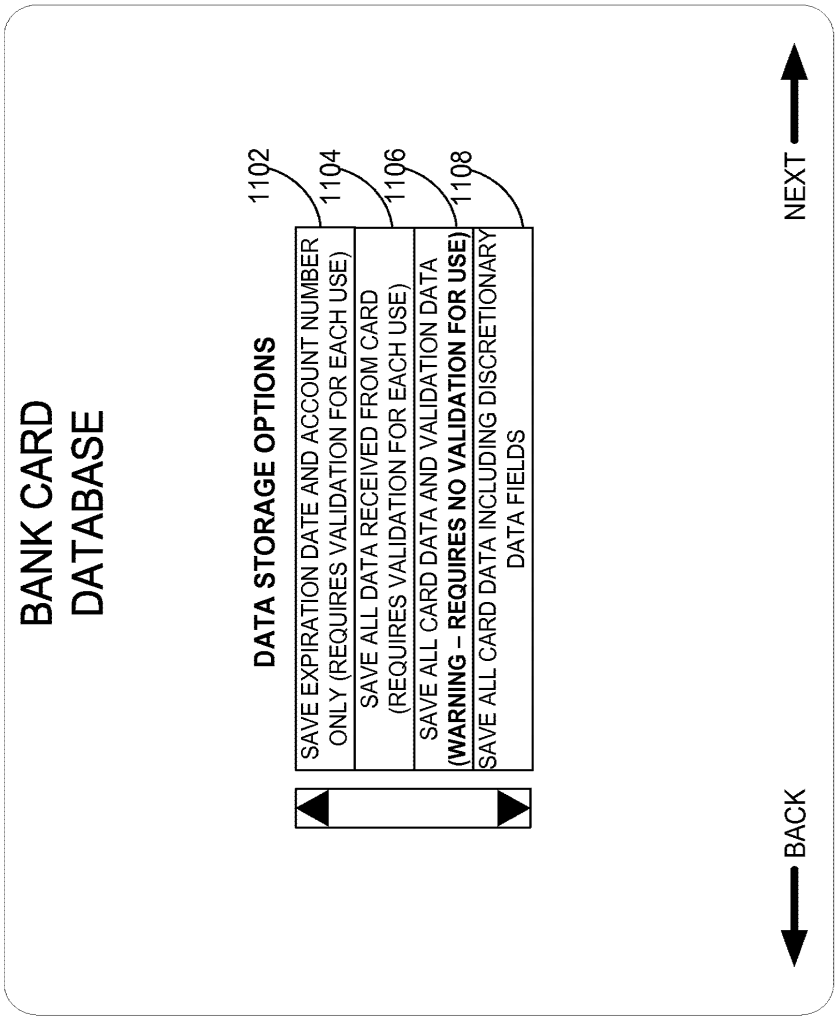

BANK CARD DATABASE
DATA STORAGE OPTIONS
1102
1104
1106
1108
SAVE EXPIRATION DATE AND ACCOUNT NUMBER ONLY (REQUIRES VALIDATION FOR EACH USE)
SAVE ALL DATA RECEIVED FROM CARD (REQUIRES VALIDATION FOR EACH USE)
SAVE ALL CARD DATA AND VALIDATION DATA (WARNING – REQUIRES NO VALIDATION FOR USE)
SAVE ALL CARD DATA INCLUDING DISCRETIONARY DATA FIELDS
NEXT
BACK

FIG. 11

1200

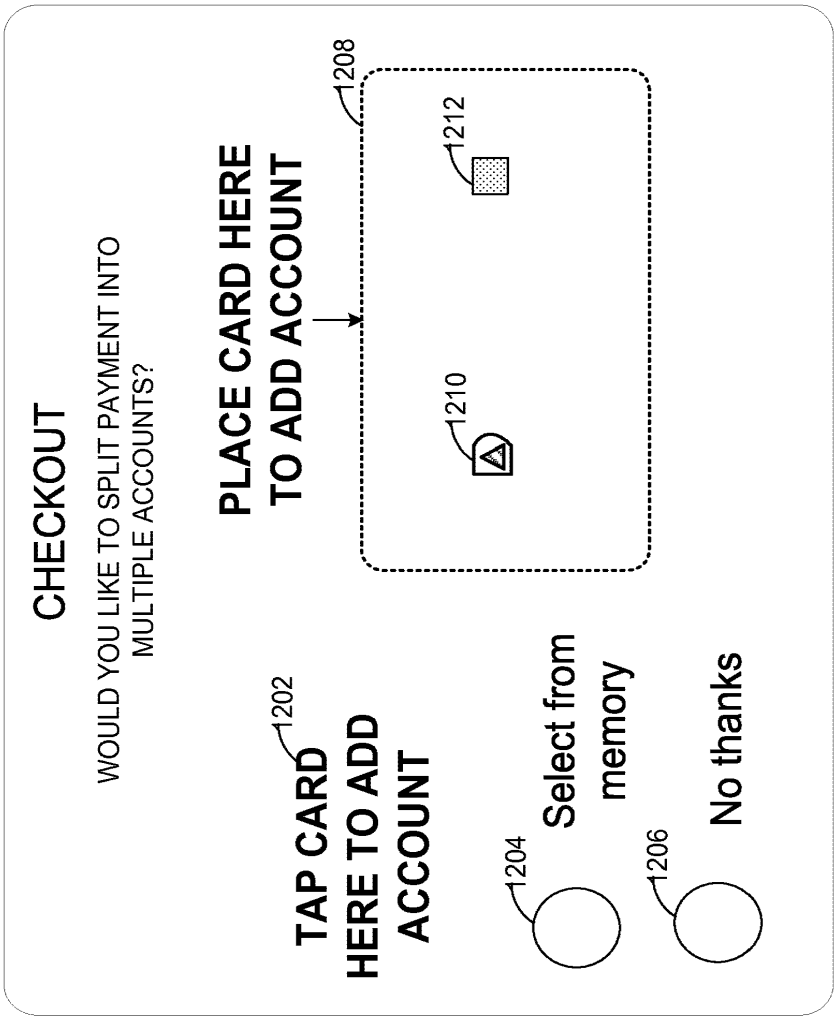

CHECKOUT
WOULD YOU LIKE TO SPLIT PAYMENT INTO MULTIPLE ACCOUNTS?
PLACE CARD HERE TO ADD ACCOUNT
208
212
210
TAP CARD HERE TO ADD ACCOUNT
202
Select from memory
204
No thanks
206

FIG. 12

1300

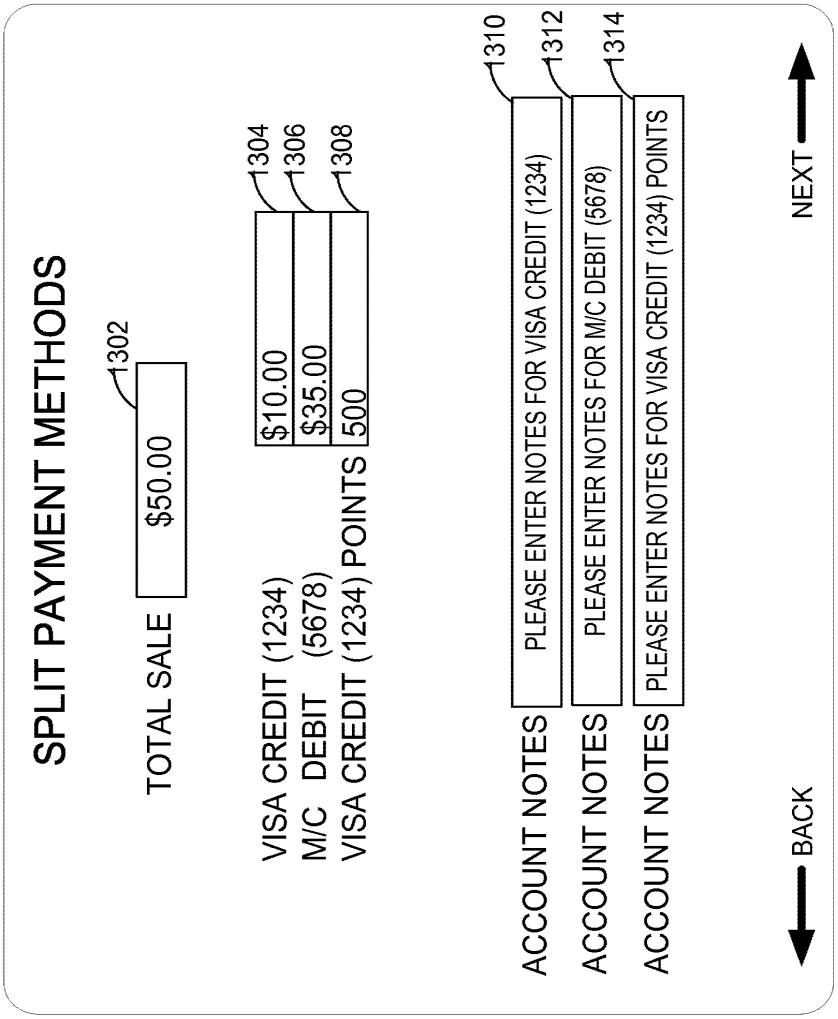

SPLIT PAYMENT METHODS
TOTAL SALE
$50.00
1302
VISA CREDIT (1234)
M/C DEBIT (5678)
VISA CREDIT (1234) POINTS
$10.00
$35.00
500
1304
1306
1308
ACCOUNT NOTES
ACCOUNT NOTES
ACCOUNT NOTES
PLEASE ENTER NOTES FOR VISA CREDIT (1234)
PLEASE ENTER NOTES FOR M/C DEBIT (5678)
PLEASE ENTER NOTES FOR VISA CREDIT (1234) POINTS
1310
1312
1314
BACK
NEXT

FIG. 13

14/73
1400

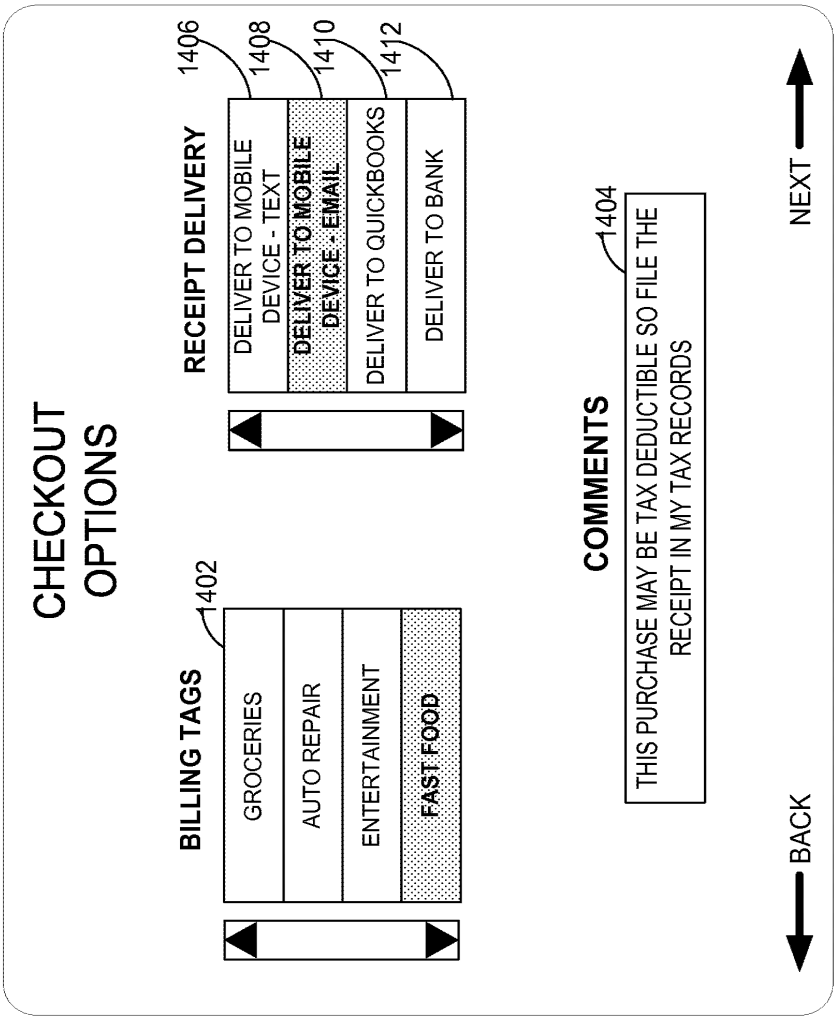


FIG. 14

15/73

1500

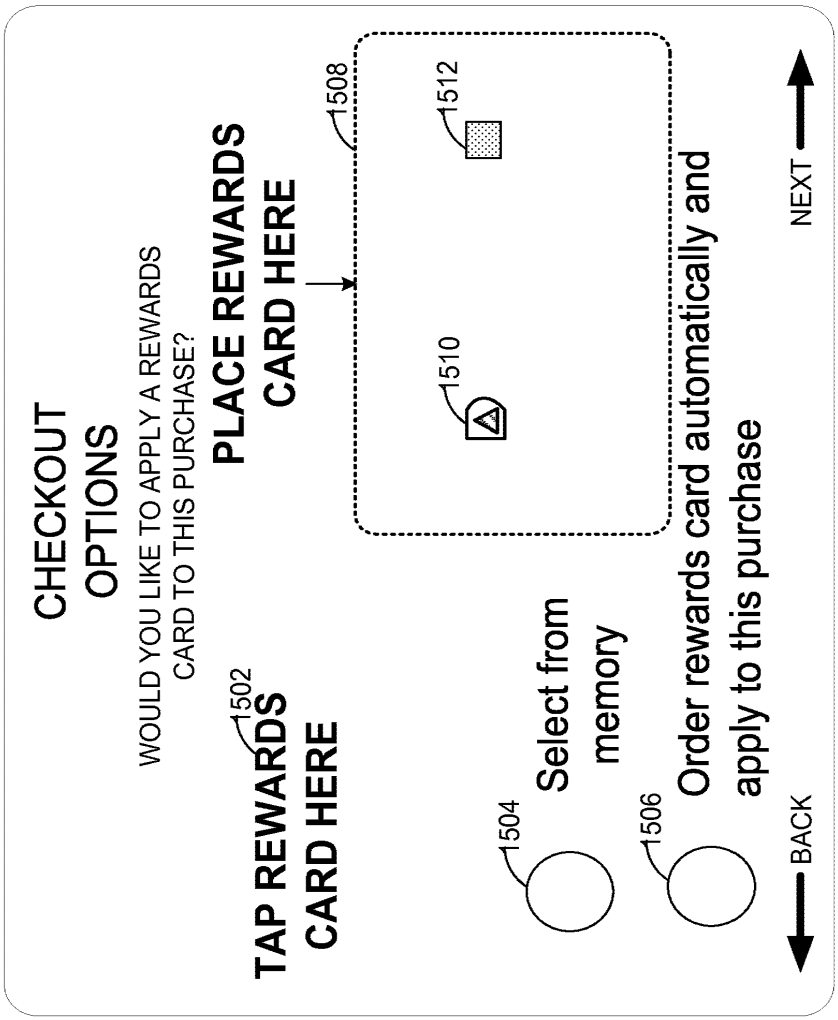


FIG. 15

1600

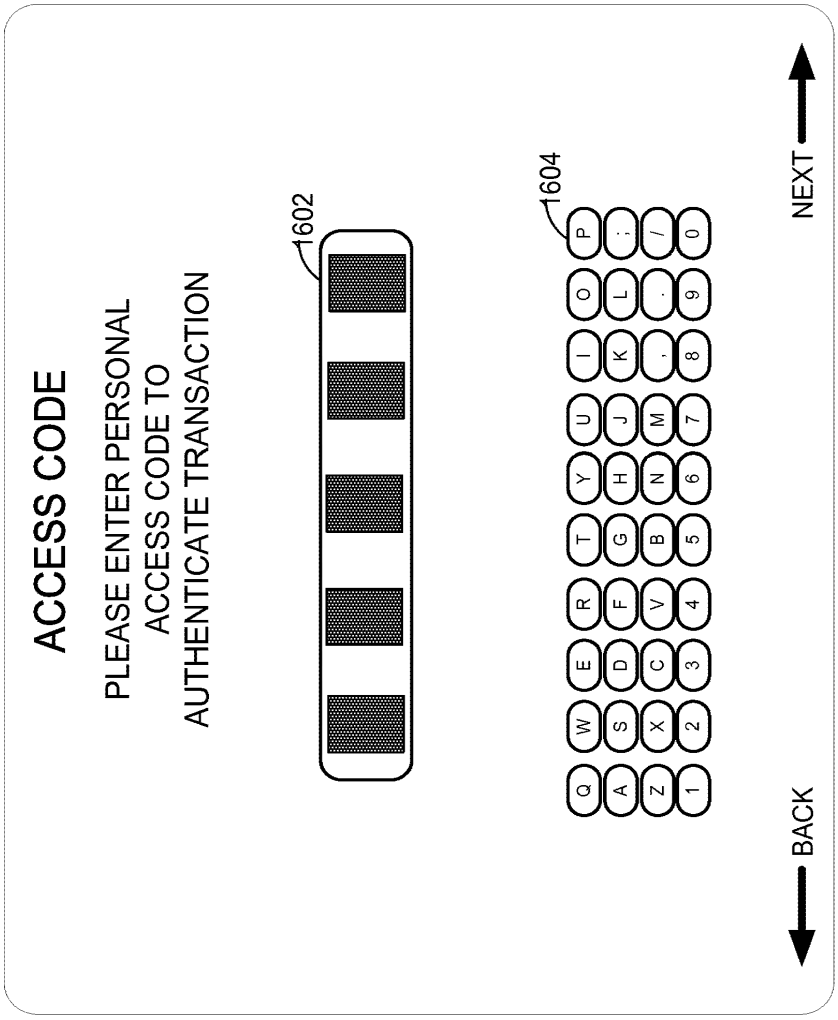

ACCESS CODE
PLEASE ENTER PERSONAL ACCESS CODE TO AUTHENTICATE TRANSACTION
1602
1604
NEXT
BACK
Q A Z 1
W S X 2
E D C 3
R F V 4
T G B 5
Y H N 6
U J M 7
I K , 8
O L . 9
P ; / 0

FIG. 16

1700

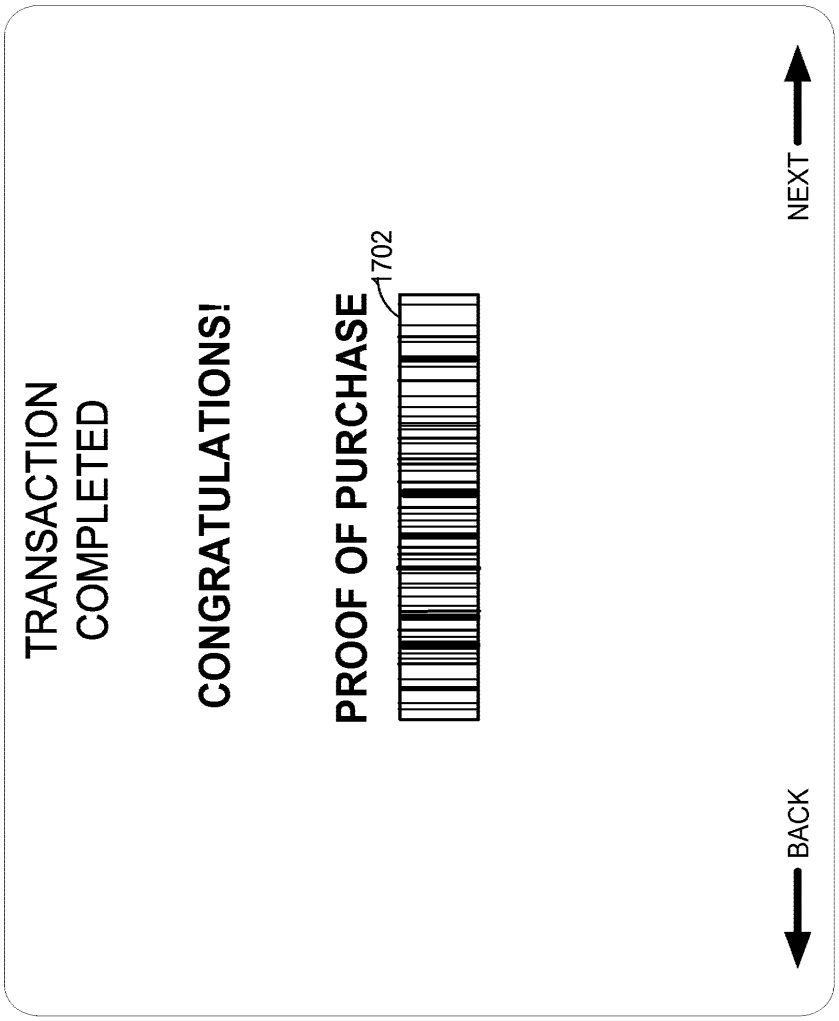

TRANSACTION COMPLETED
CONGRATULATIONS!
PROOF OF PURCHASE
1702
NEXT
BACK

FIG. 17

1800

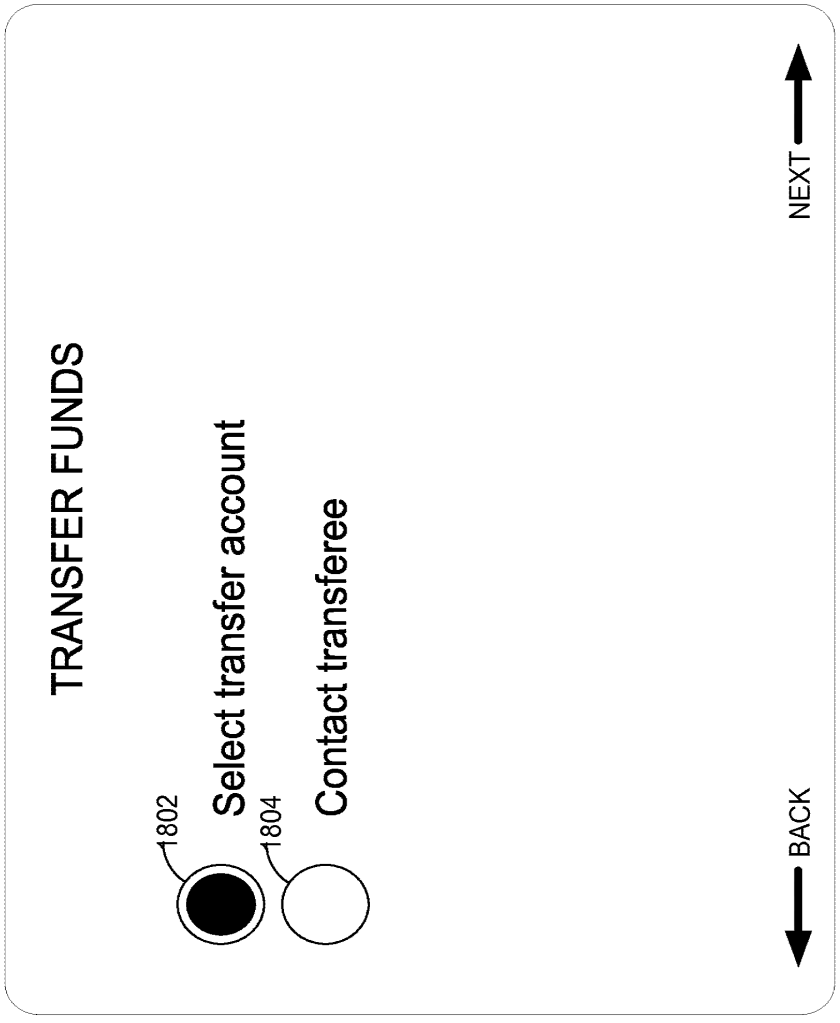

TRANSFER FUNDS
Select transfer account
Contact transferee
1802
1804
NEXT
BACK

FIG. 18

1900

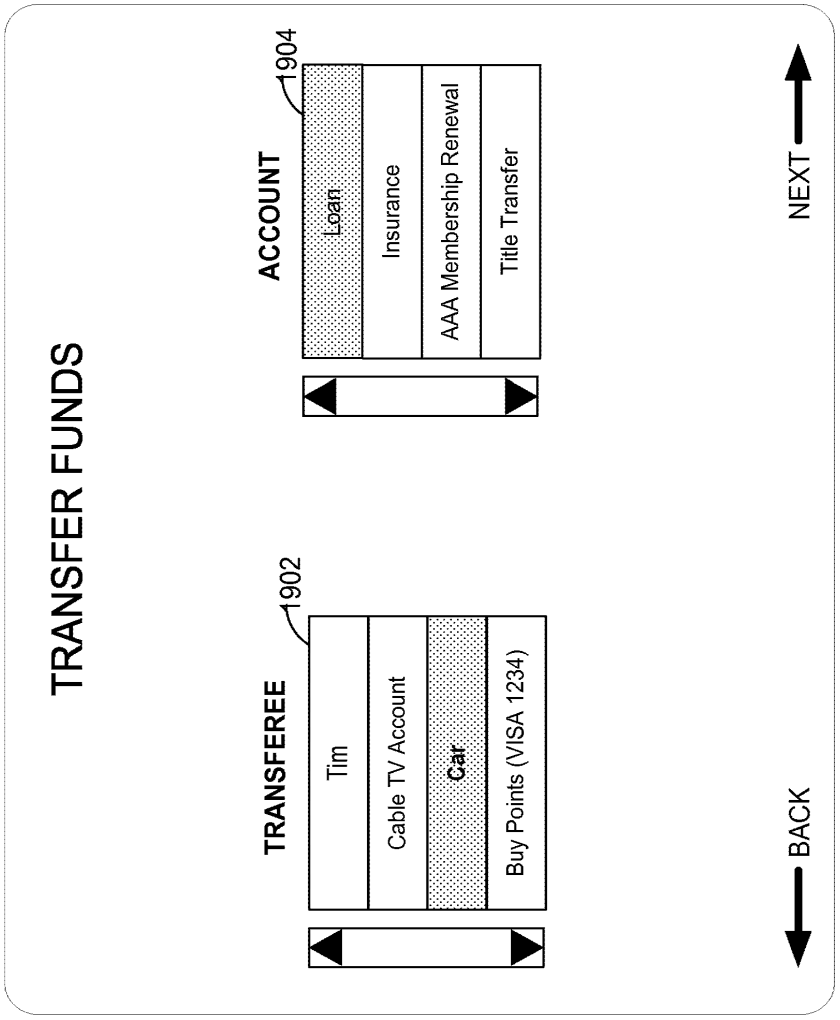

TRANSFER FUNDS
TRANSFEREE
1902
Tim
Cable TV Account
Car
Buy Points (VISA 1234)
ACCOUNT
1904
Loan
Insurance
AAA Membership Renewal
Title Transfer
BACK
NEXT

FIG. 19

2000

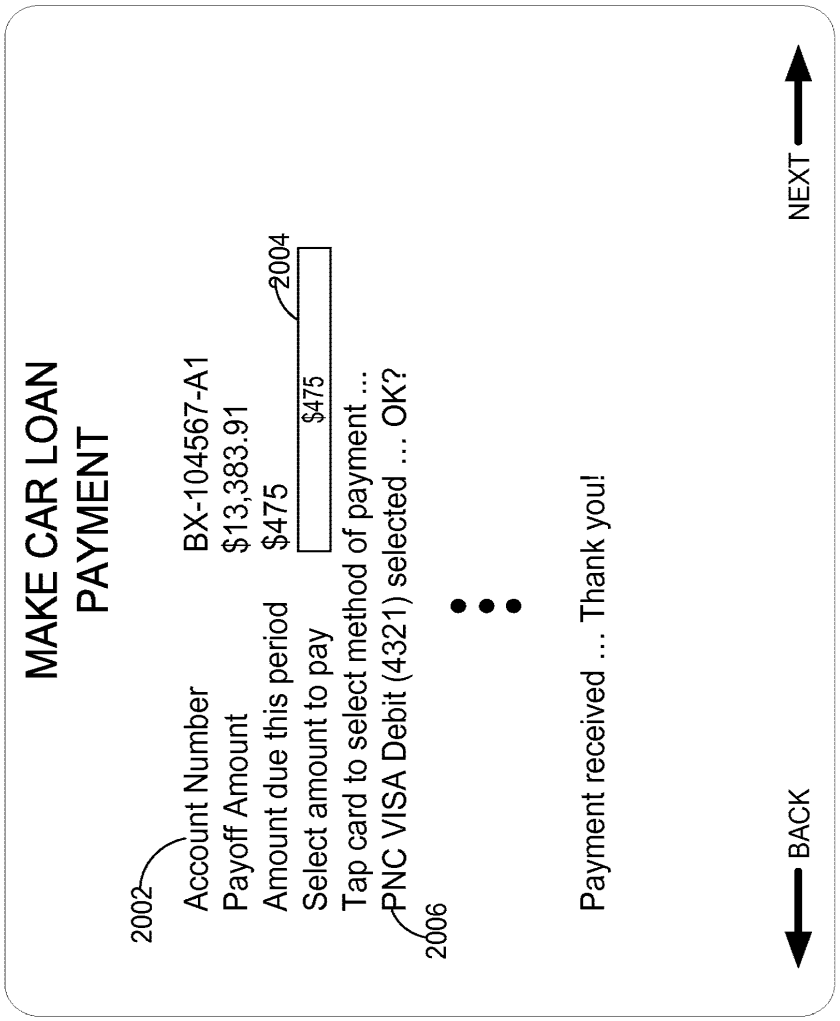

MAKE CAR LOAN PAYMENT
2002
Account Number BX-104567-A1
Payoff Amount $13,383.91
Amount due this period $475
Select amount to pay $475
2004
Tap card to select method of payment ...
PNC VISA Debit (4321) selected ... OK?
2006
Payment received ... Thank you!
BACK
NEXT

FIG. 20

2100

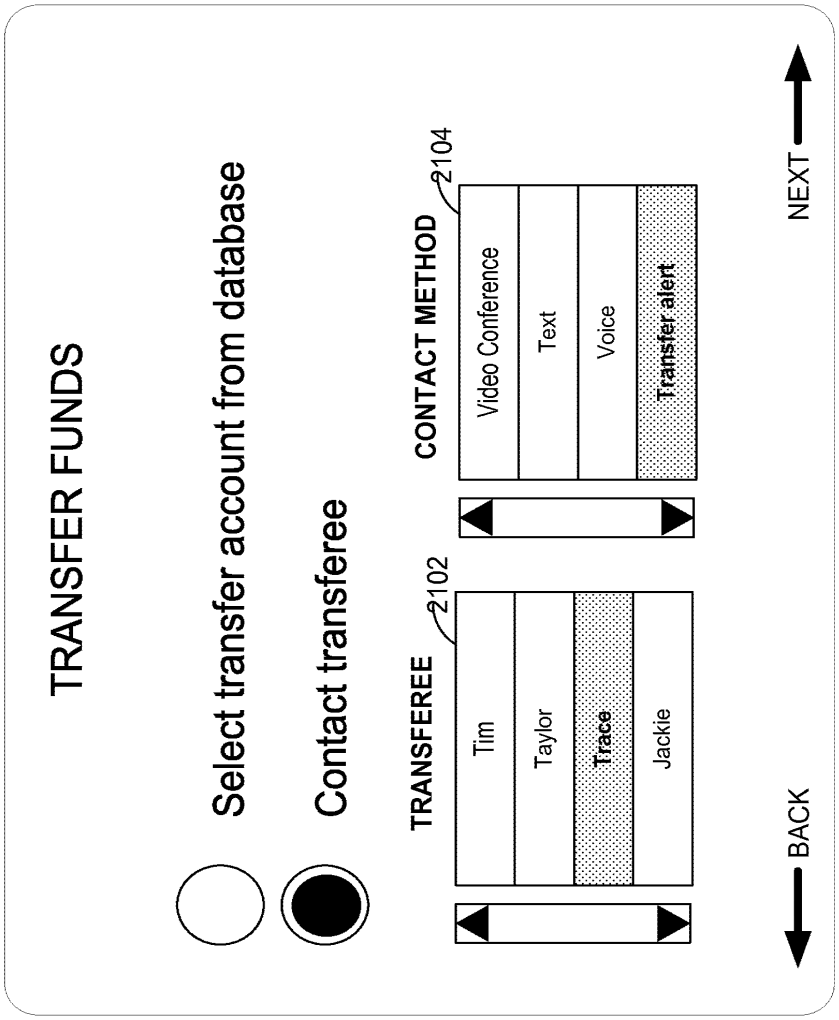

TRANSFER FUNDS
Select transfer account from database
Contact transferee
TRANSFEREE
2102
Tim
Taylor
Trace
Jackie
CONTACT METHOD
2104
Video Conference
Text
Voice
Transfer alert
BACK
NEXT

FIG. 21

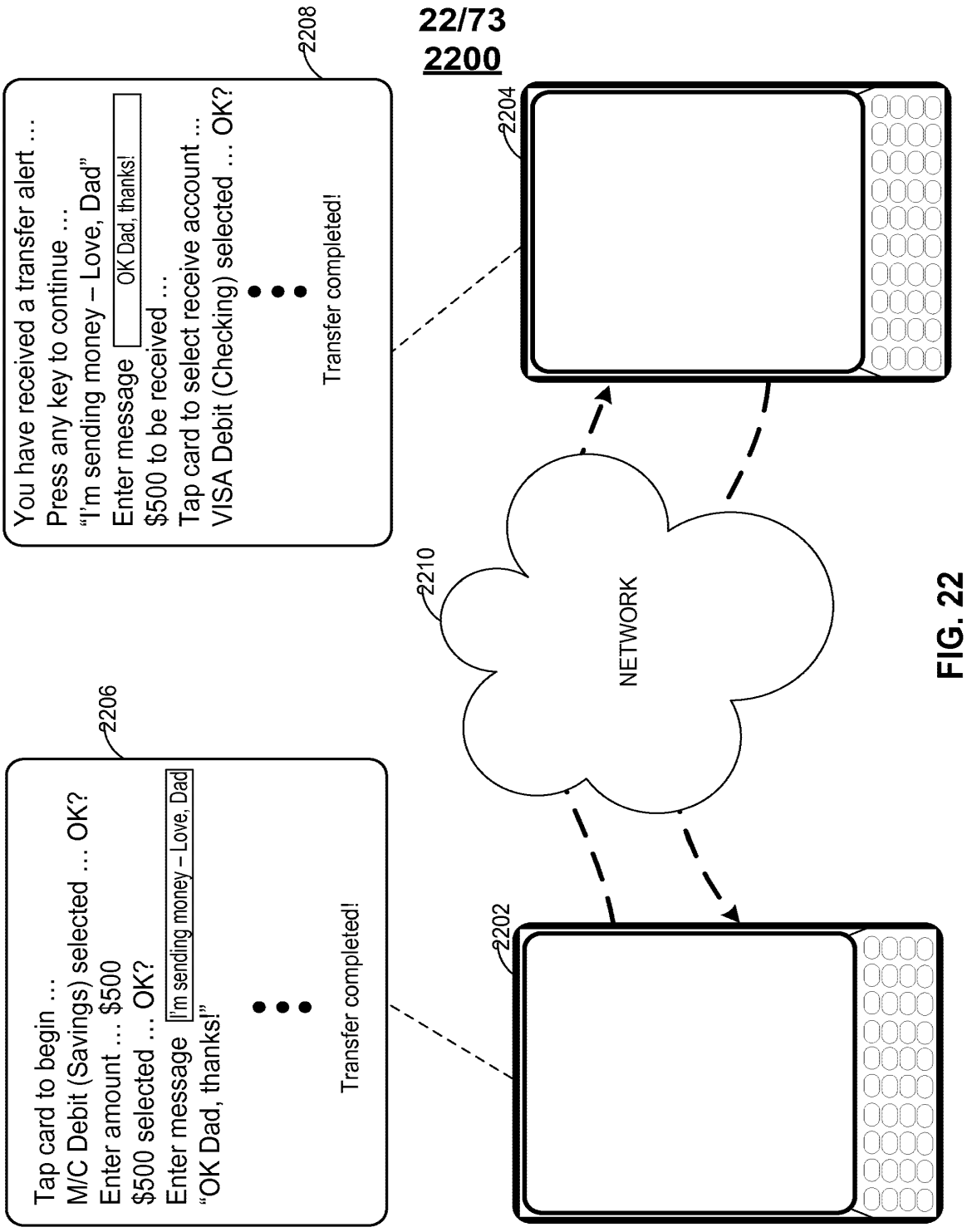

2200
2202
2204
2206
Tap card to begin ...
M/C Debit (Savings) selected ... OK?
Enter amount ... $500
$500 selected ... OK?
Enter message I'm sending money – Love, Dad
"OK Dad, thanks!"
Transfer completed!
2208
You have received a transfer alert ...
Press any key to continue ...
"I'm sending money – Love, Dad"
Enter message OK Dad, thanks!
$500 to be received ...
Tap card to select receive account ...
VISA Debit (Checking) selected ... OK?
Transfer completed!
2210
NETWORK

FIG. 22

2300

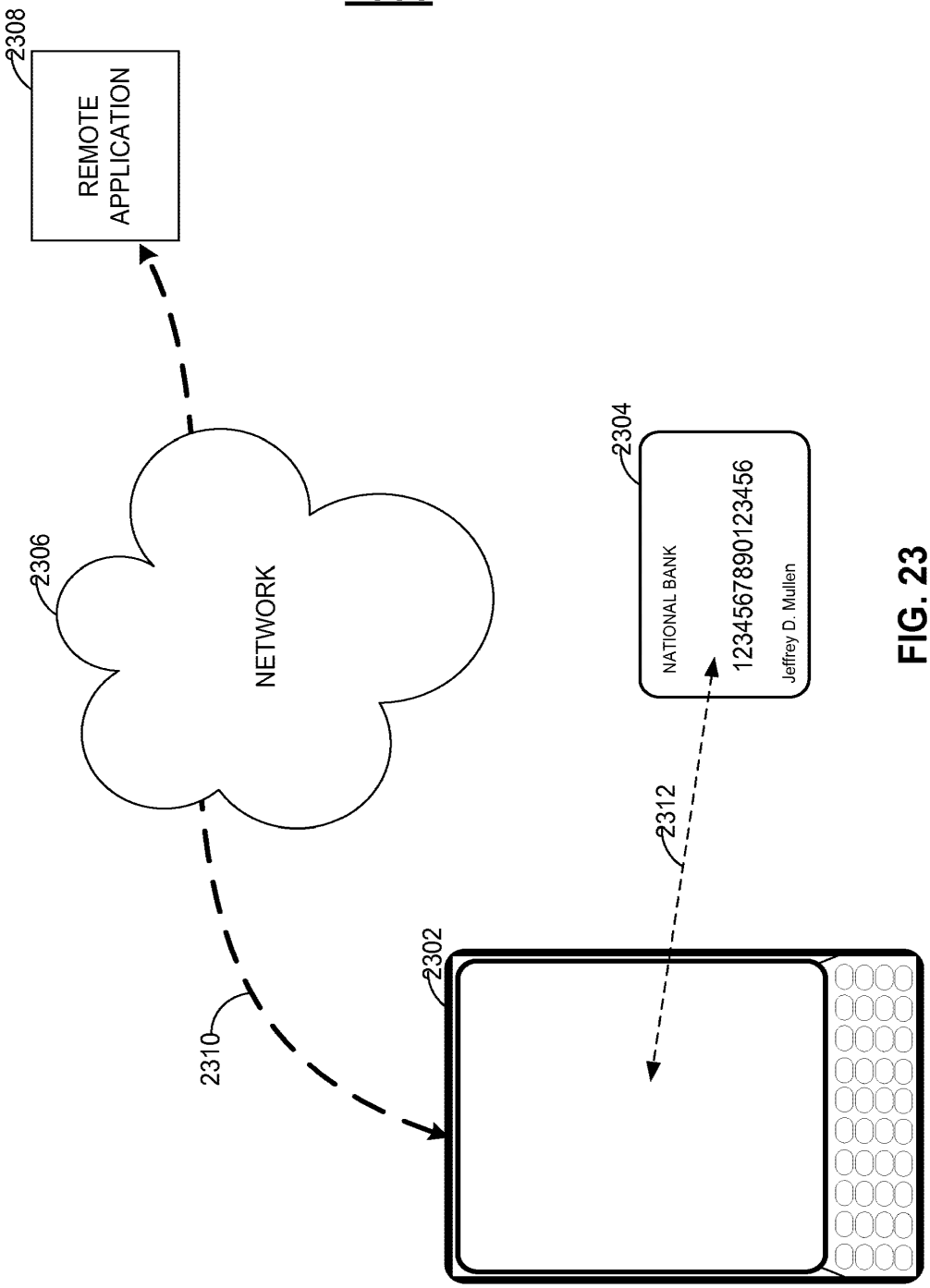

2308
REMOTE APPLICATION
2306
NETWORK
2304
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
2312
2302
2310

FIG. 23

24/73
2400

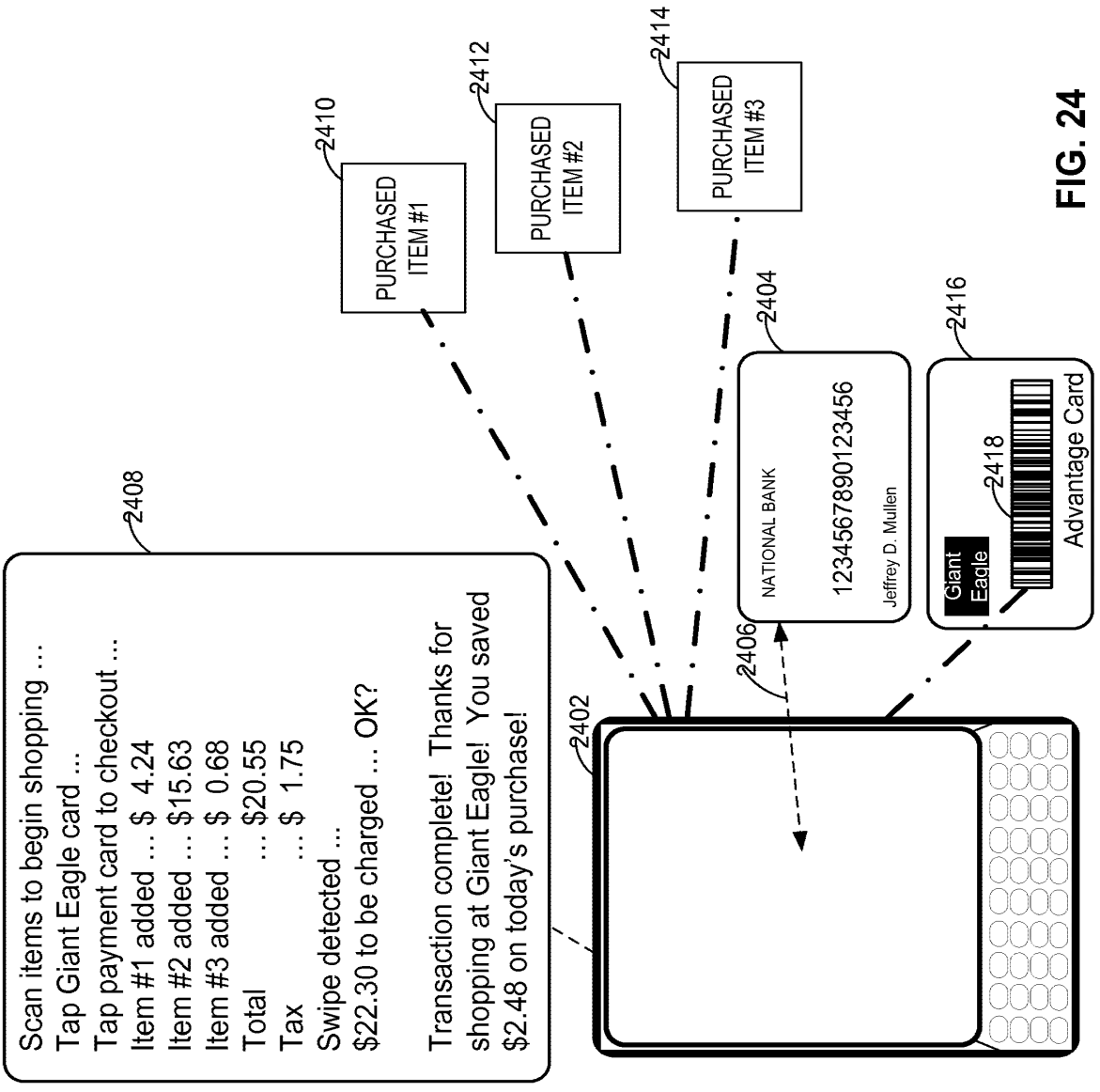


FIG. 24

25/73

2500

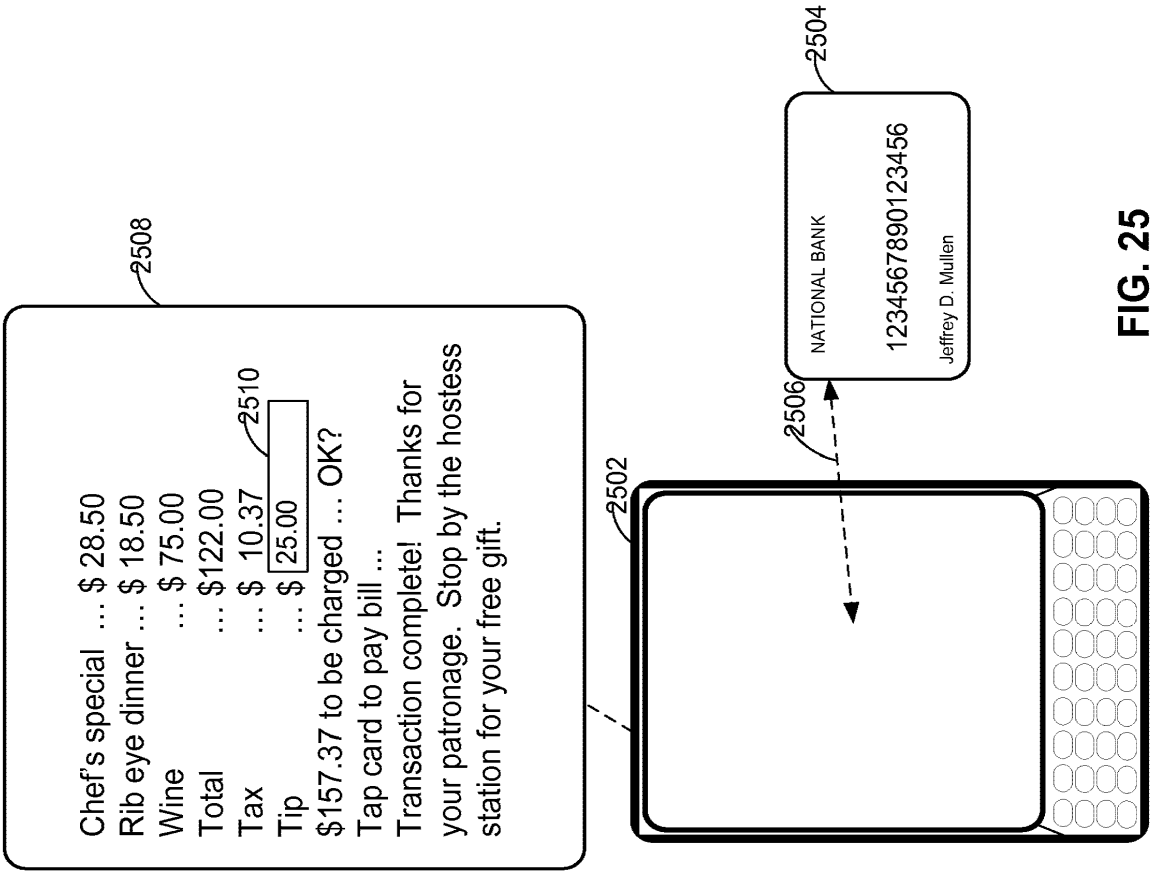


FIG. 25

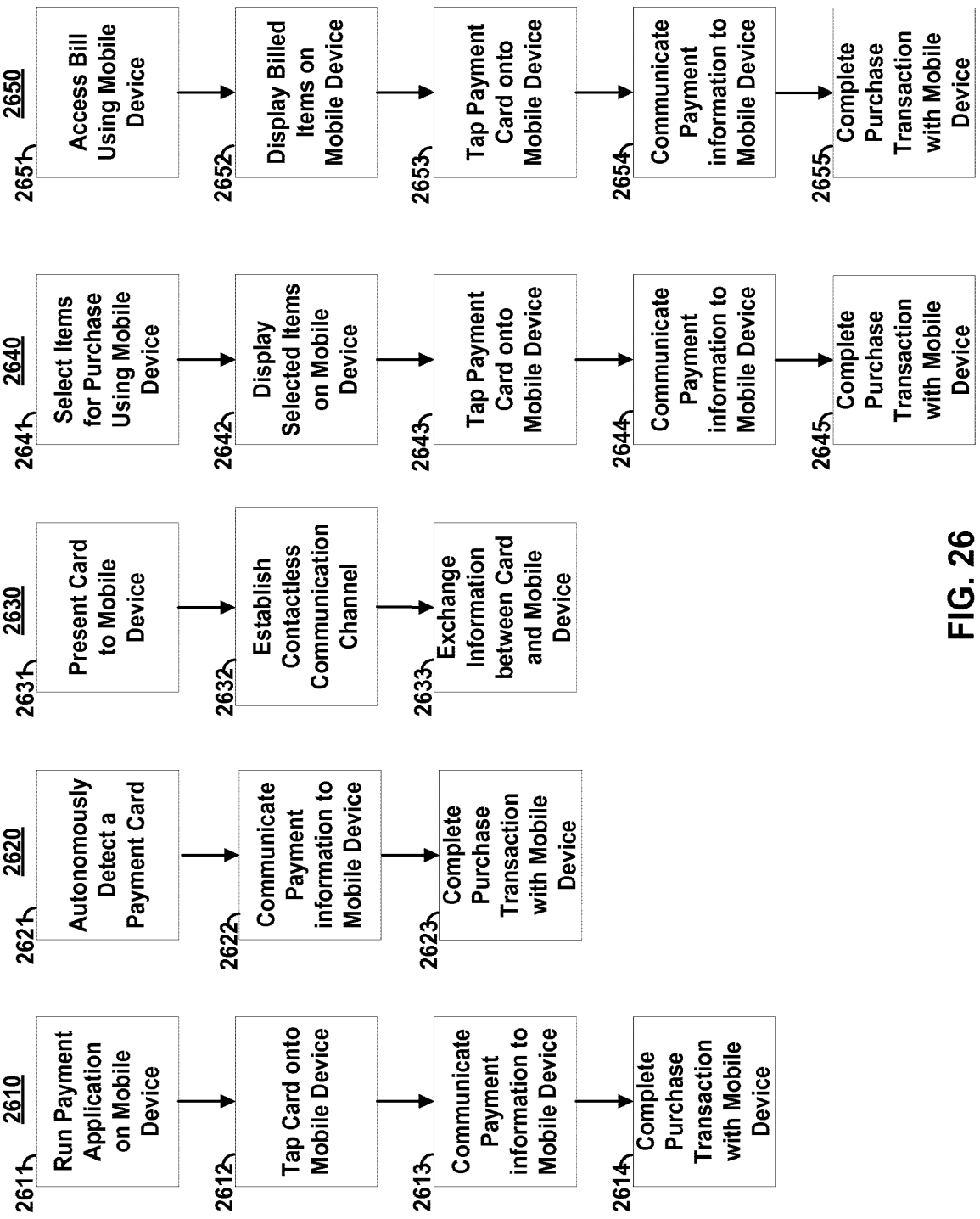

2610
2611
Run Payment Application on Mobile Device
2612
Tap Card onto Mobile Device
2613
Communicate Payment information to Mobile Device
2614
Complete Purchase Transaction with Mobile Device
2620
2621
Autonomously Detect a Payment Card
2622
Communicate Payment information to Mobile Device
2623
Complete Purchase Transaction with Mobile Device
2630
2631
Present Card to Mobile Device
2632
Establish Contactless Communication Channel
2633
Exchange Information between Card and Mobile Device
2640
2641
Select Items for Purchase Using Mobile Device
2642
Display Selected Items on Mobile Device
2643
Tap Payment Card onto Mobile Device
2644
Communicate Payment information to Mobile Device
2645
Complete Purchase Transaction with Mobile Device
2650
2651
Access Bill Using Mobile Device
2652
Display Billed Items on Mobile Device
2653
Tap Payment Card onto Mobile Device
2654
Communicate Payment information to Mobile Device
2655
Complete Purchase Transaction with Mobile Device

FIG. 26

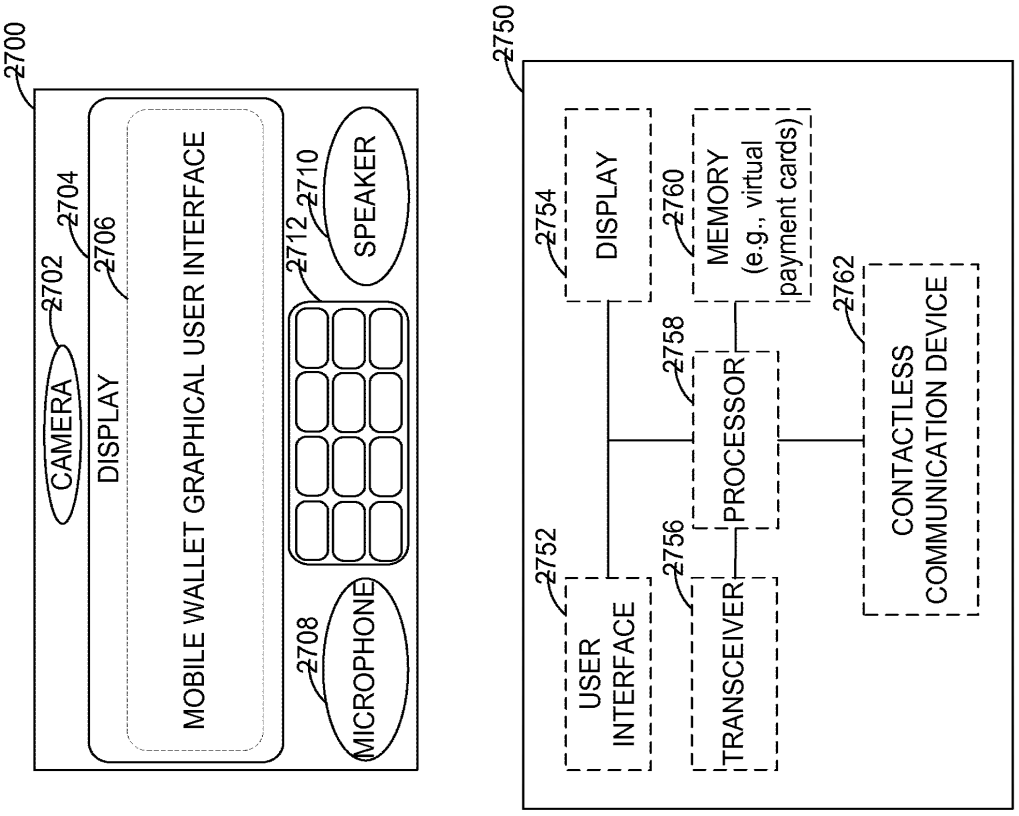

2700
CAMERA
2702
DISPLAY
2704
2706
MOBILE WALLET GRAPHICAL USER INTERFACE
2712
2710
SPEAKER
MICROPHONE
2708
2750
USER INTERFACE
2752
DISPLAY
2754
TRANSCEIVER
2756
PROCESSOR
2758
MEMORY (e.g., virtual payment cards)
2760
CONTACTLESS COMMUNICATION DEVICE
2762

FIG. 27

2800

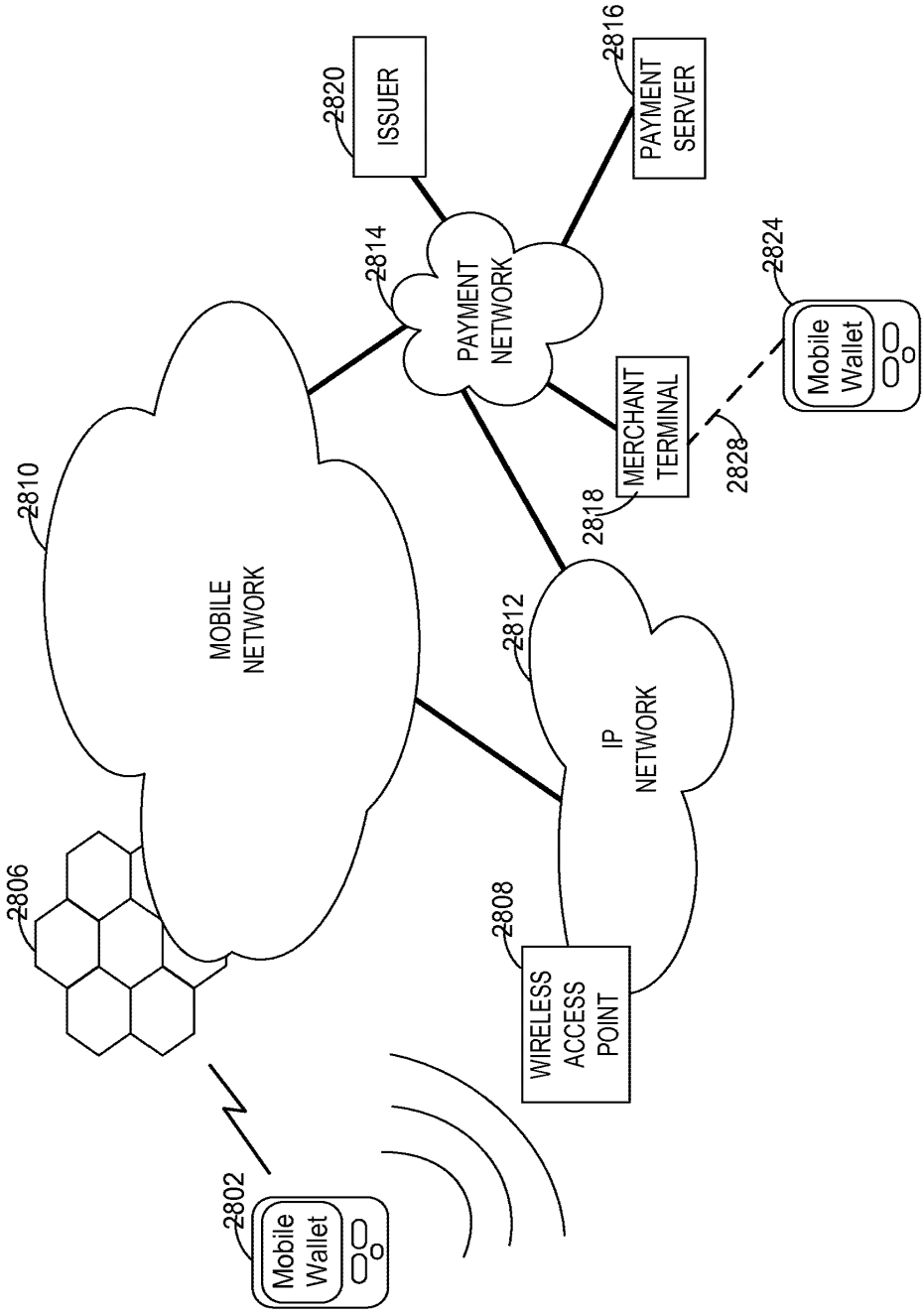

2820
ISSUER
2816
PAYMENT SERVER
2814
PAYMENT NETWORK
2824
Mobile Wallet
2828
MERCHANT TERMINAL
2818
2810
MOBILE NETWORK
2812
IP NETWORK
2806
2808
WIRELESS ACCESS POINT
2802
Mobile Wallet

FIG. 28

2900

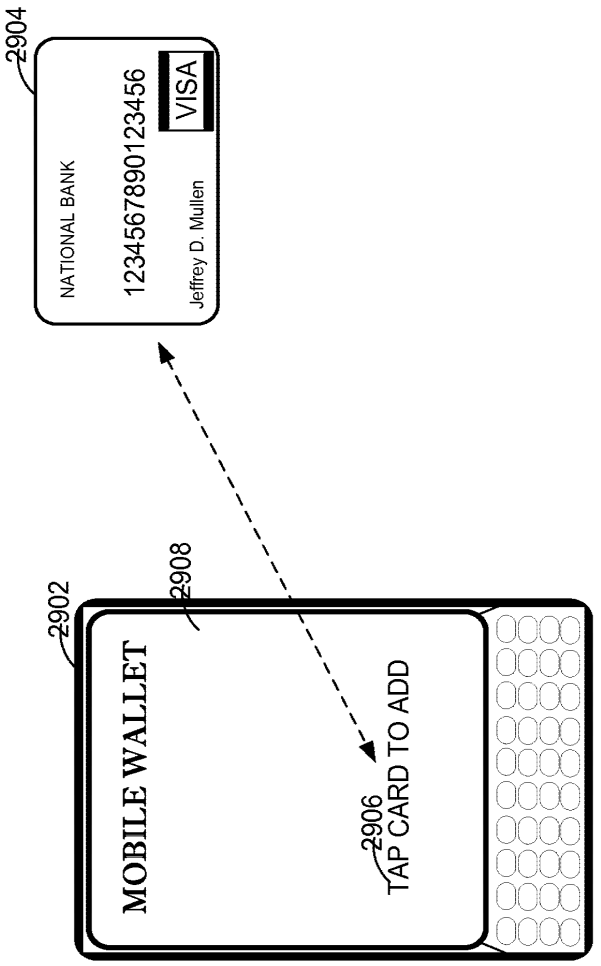

2904
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
2902
2908
MOBILE WALLET
2906
TAP CARD TO ADD

FIG. 29

3000

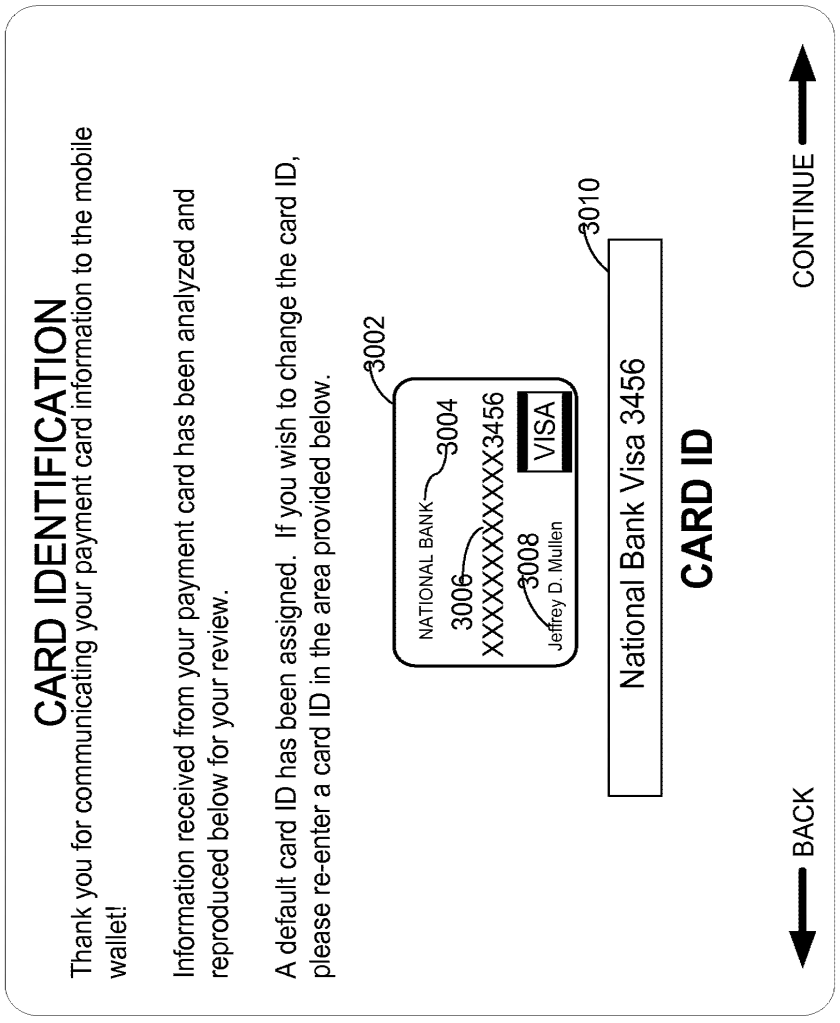

CARD IDENTIFICATION
Thank you for communicating your payment card information to the mobile wallet!
Information received from your payment card has been analyzed and reproduced below for your review.
A default card ID has been assigned. If you wish to change the card ID, please re-enter a card ID in the area provided below.
3002
NATIONAL BANK
3004
3006
XXXXXXXXXXXX3456
VISA
3008
Jeffrey D. Mullen
3010
National Bank Visa 3456
CARD ID
BACK
CONTINUE

FIG. 30

3100

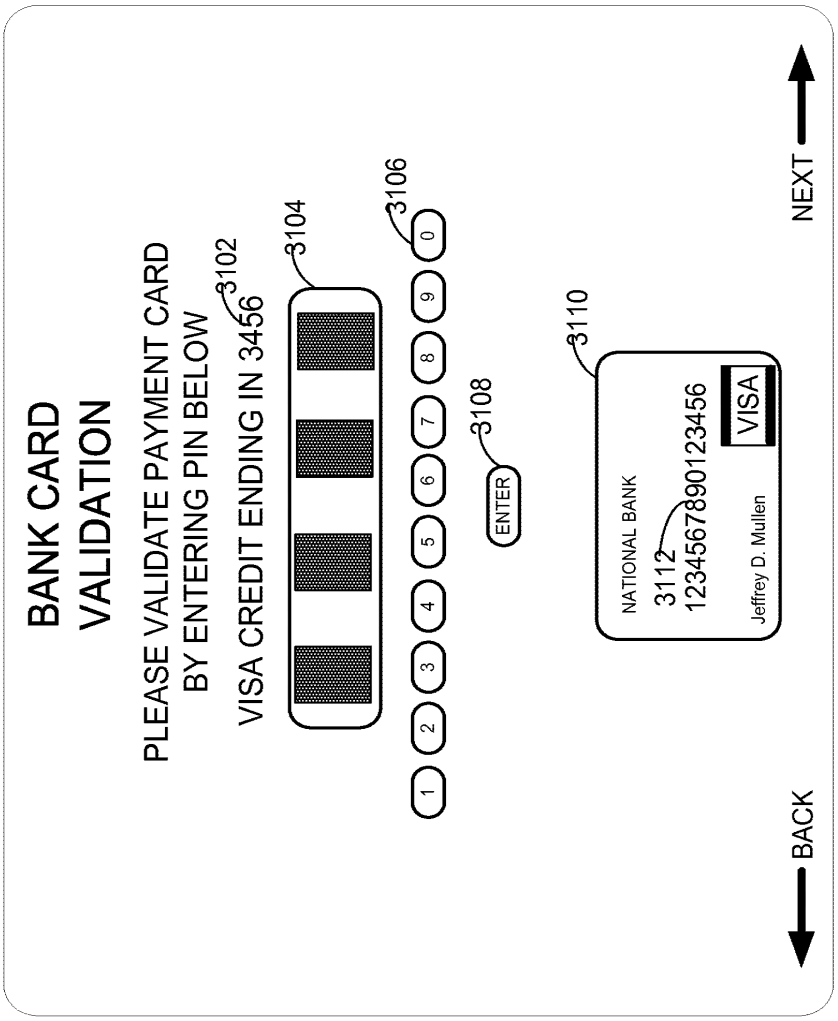

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING PIN BELOW
VISA CREDIT ENDING IN 3456
3102
3104
3106
1
2
3
4
5
6
7
8
9
0
ENTER
3108
3110
NATIONAL BANK
3112
1234567890123456
Jeffrey D. Mullen
VISA
BACK
NEXT

FIG. 31

3200

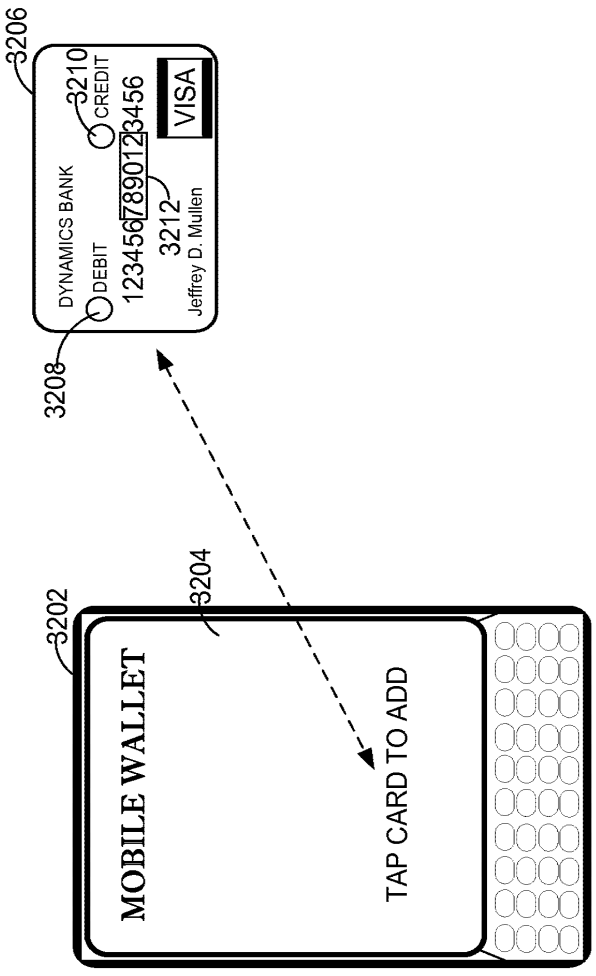

3206
3210
CREDIT
VISA
DYNAMICS BANK
DEBIT
1234567890123456
3212
Jeffrey D. Mullen
3208
3204
3202
MOBILE WALLET
TAP CARD TO ADD

FIG. 32

3300

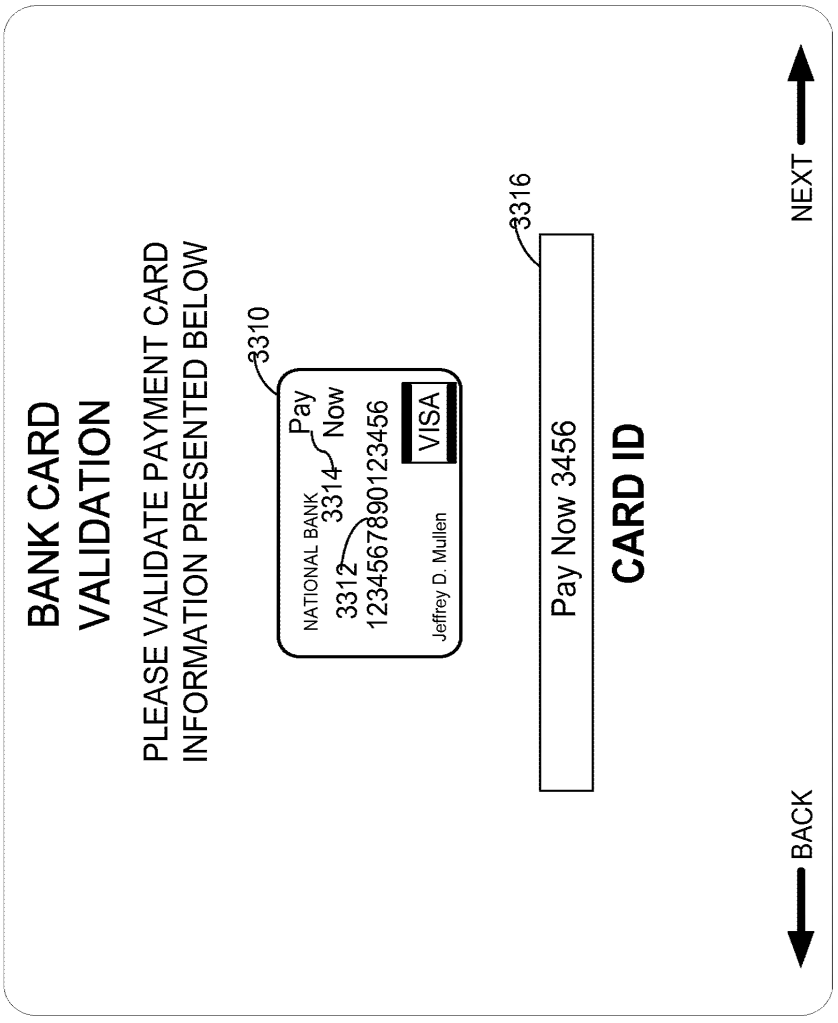

BANK CARD VALIDATION
PLEASE VALIDATE PAYMENT CARD INFORMATION PRESENTED BELOW
3310
NATIONAL BANK
3314
Pay Now
3312
1234567890123456
Jeffrey D. Mullen
VISA
3316
Pay Now 3456
CARD ID
NEXT
BACK

FIG. 33

34/73
3400

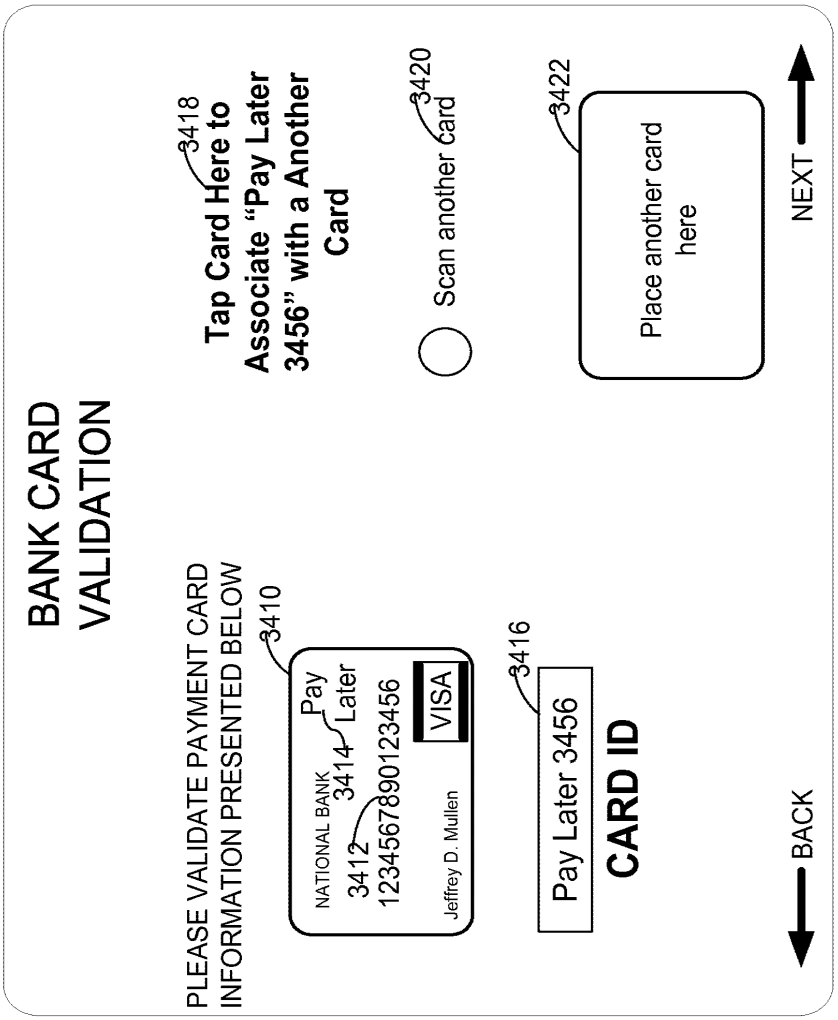


FIG. 34

3500

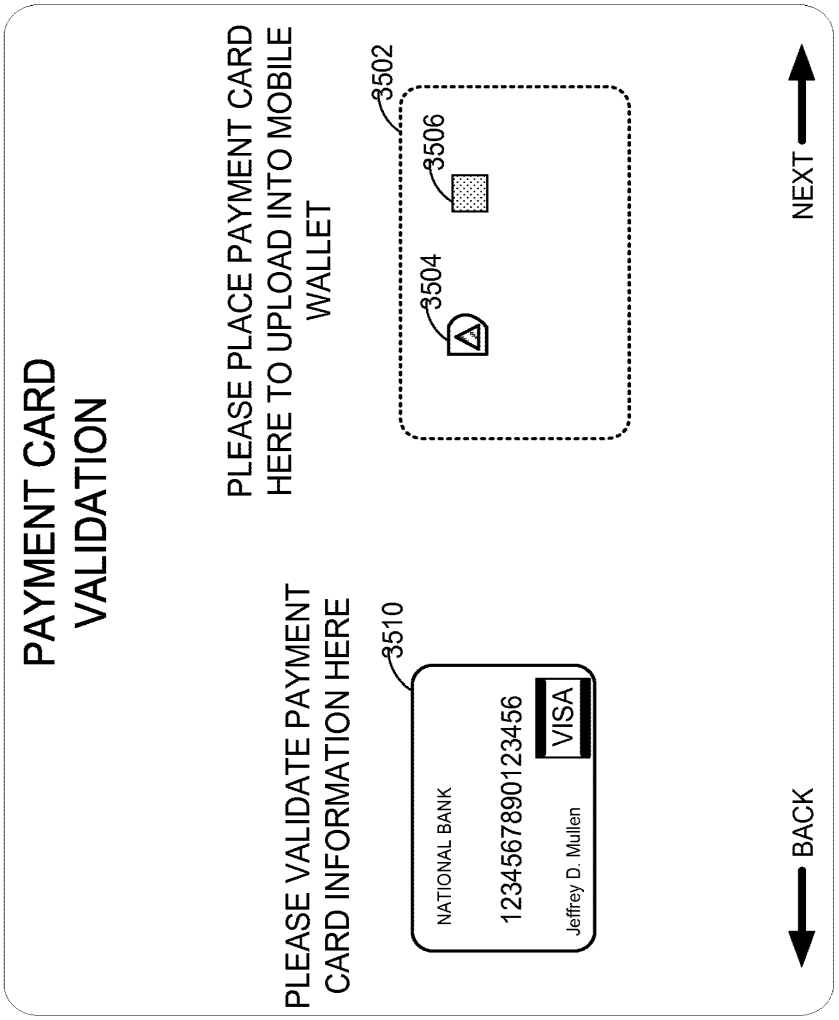

PAYMENT CARD VALIDATION
PLEASE PLACE PAYMENT CARD HERE TO UPLOAD INTO MOBILE WALLET
3502
3506
3504
PLEASE VALIDATE PAYMENT CARD INFORMATION HERE
3510
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
BACK
NEXT

FIG. 35

3600

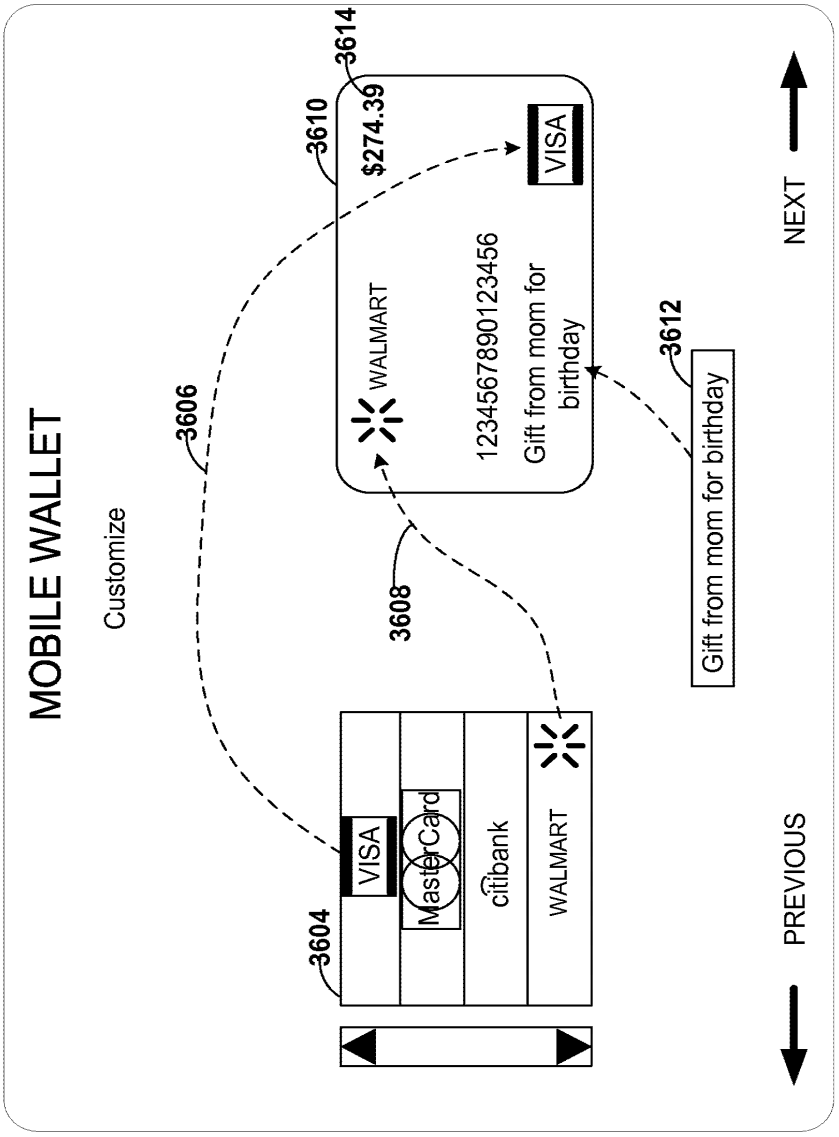

MOBILE WALLET
Customize
3606
3610
3614
$274.39
VISA
WALMART
1234567890123456
Gift from mom for birthday
3612
Gift from mom for birthday
3608
3604
VISA
MasterCard
citibank
WALMART
NEXT
PREVIOUS

FIG. 36

37/73
3700

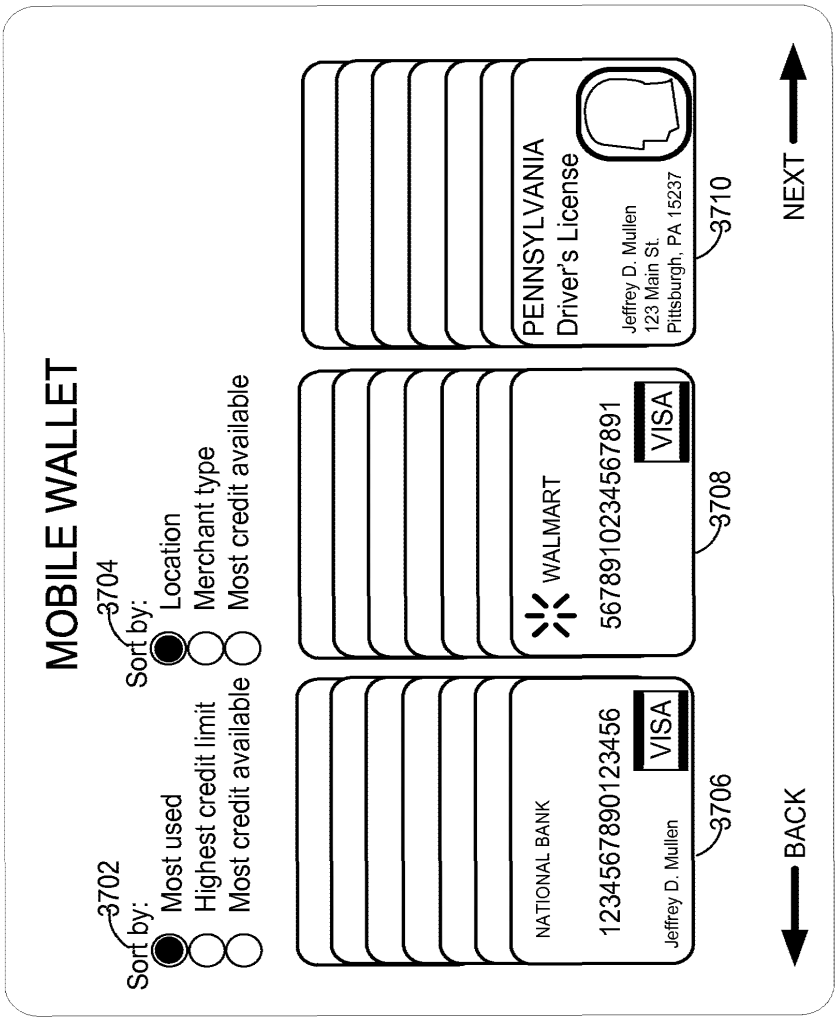


FIG. 37

38/73
3800

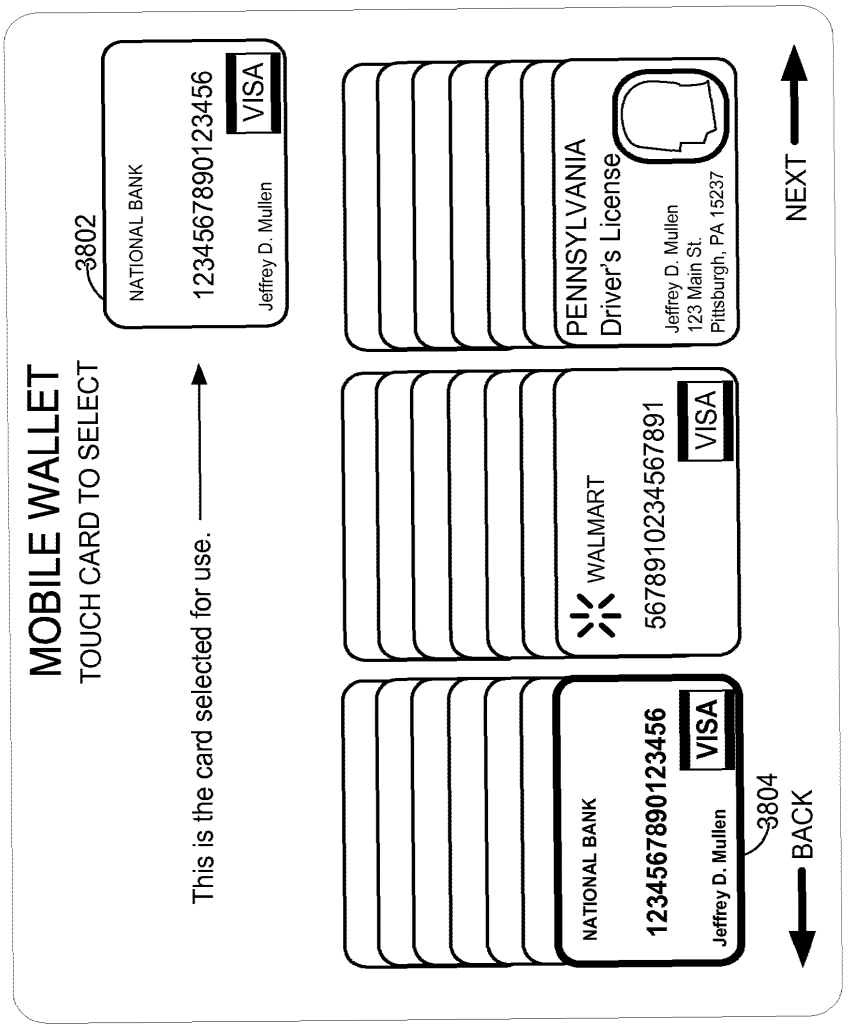


FIG. 38

3900

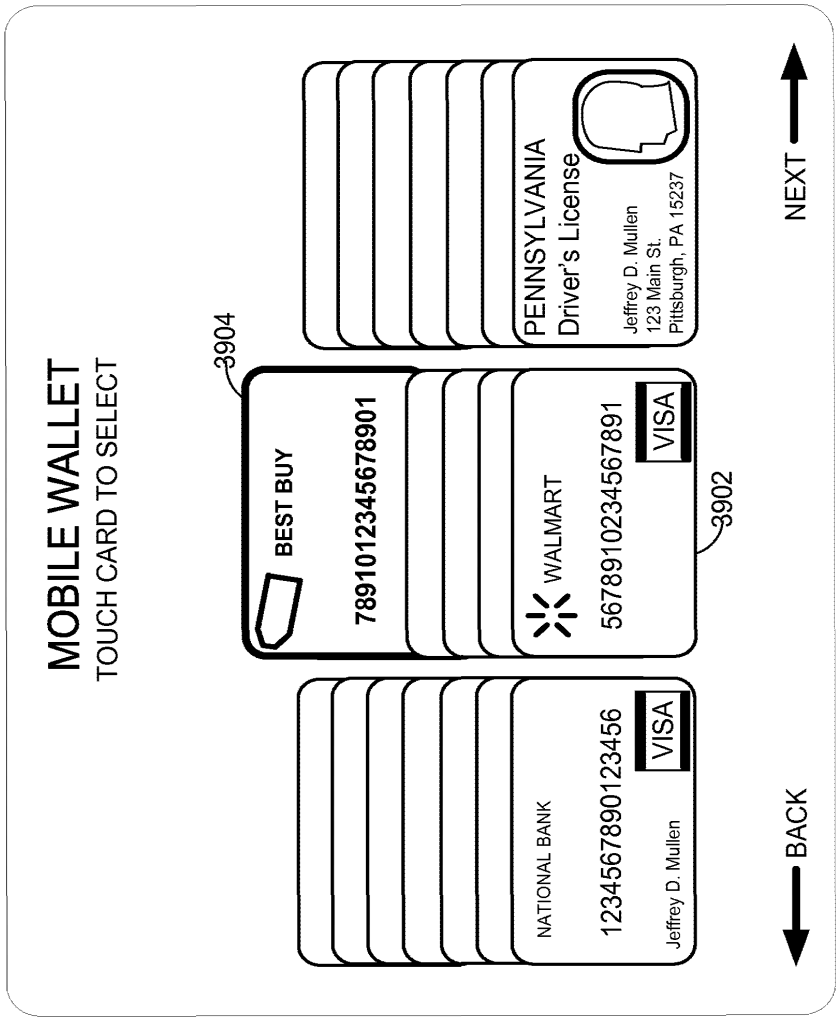

MOBILE WALLET
TOUCH CARD TO SELECT
3904
BEST BUY
7891012345678901
WALMART
5678910234567891
VISA
3902
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
NEXT
BACK

FIG. 39

4000

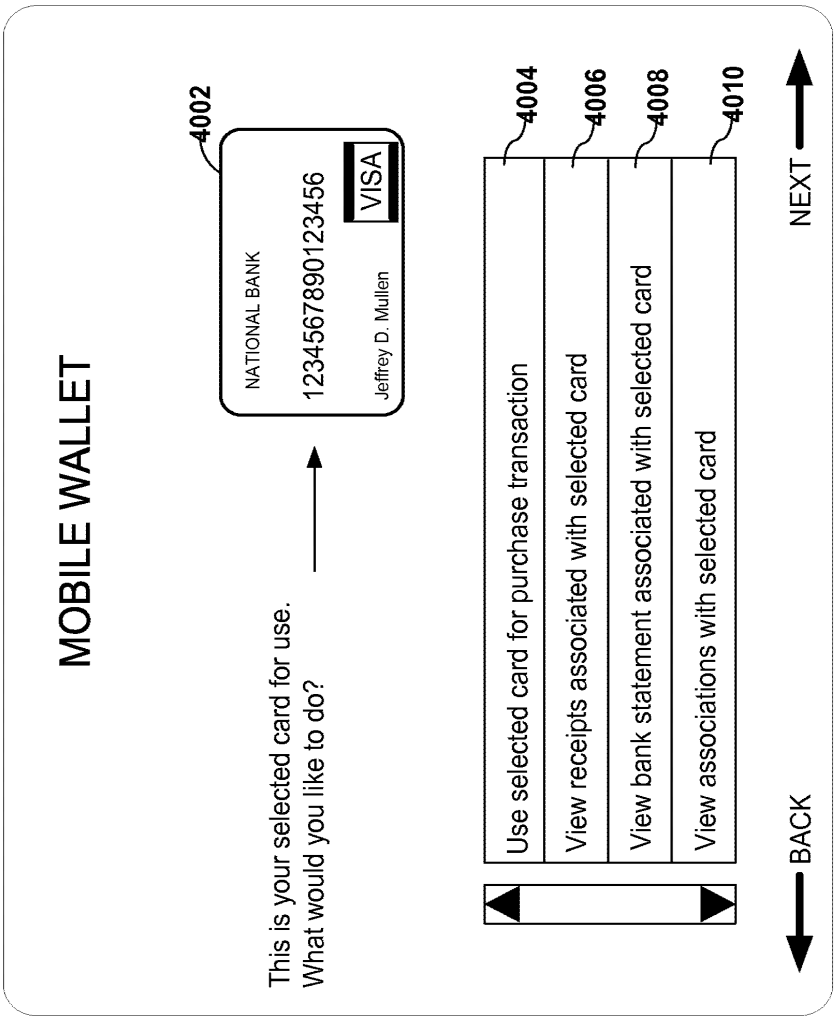

MOBILE WALLET
4002
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
This is your selected card for use.
What would you like to do?
4004
Use selected card for purchase transaction
4006
View receipts associated with selected card
4008
View bank statement associated with selected card
4010
View associations with selected card
BACK
NEXT

FIG. 40

4100

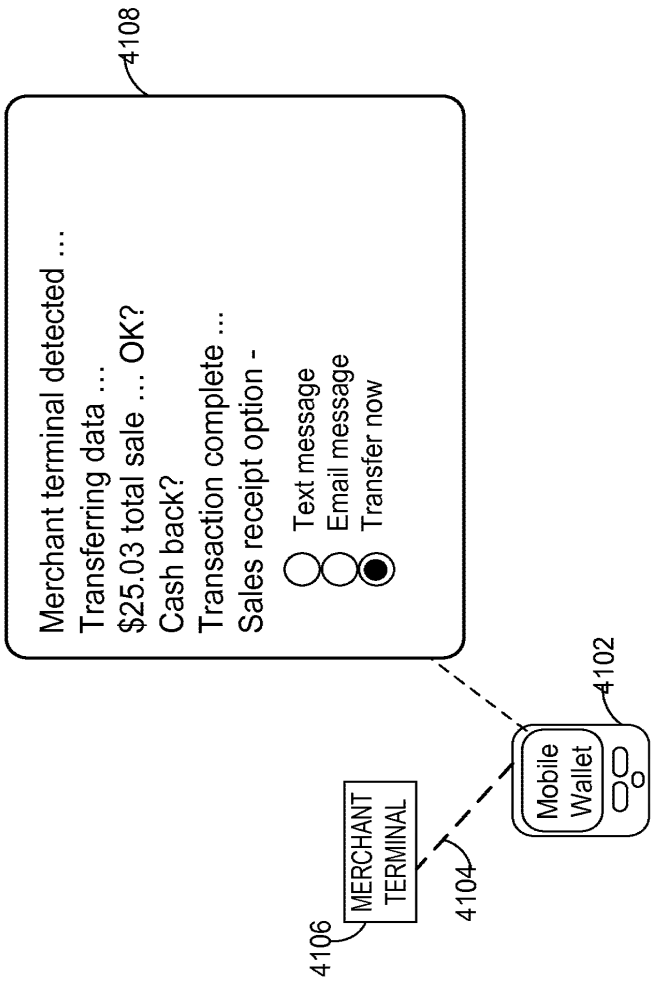

4108
Merchant terminal detected ...
Transferring data ...
$25.03 total sale ... OK?
Cash back?
Transaction complete ...
Sales receipt option -
Text message
Email message
Transfer now
4102
Mobile Wallet
MERCHANT TERMINAL
4104
4106

FIG. 41

4200

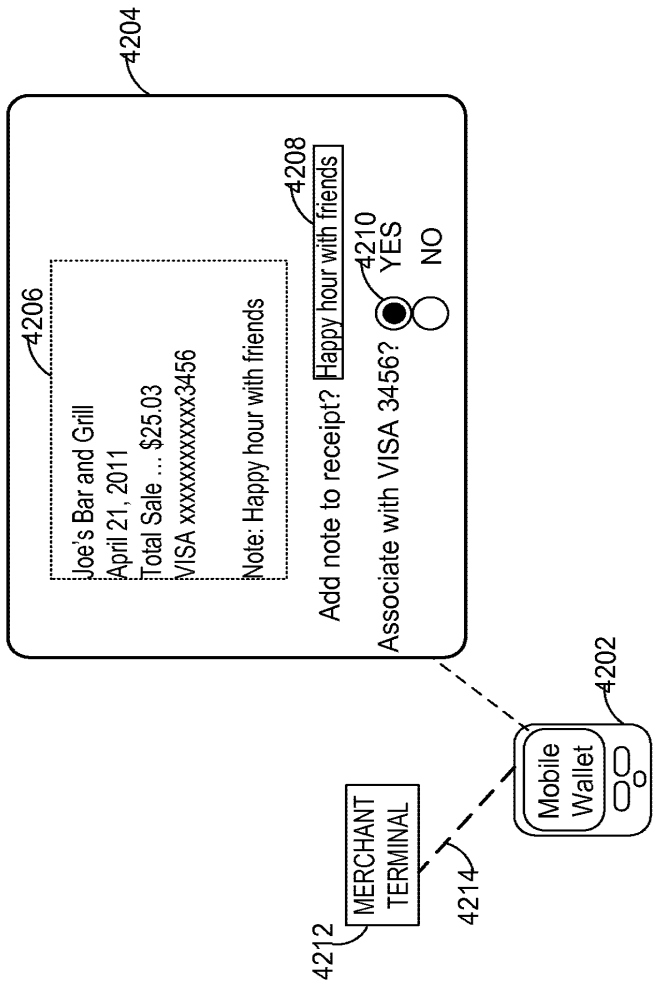

4204
4206
Joe's Bar and Grill
April 21, 2011
Total Sale ... $25.03
VISA xxxxxxxxxx3456
Note: Happy hour with friends
4208
Add note to receipt? Happy hour with friends
4210
Associate with VISA 3456?
YES
NO
4202
Mobile Wallet
4212
MERCHANT TERMINAL
4214

FIG. 42

4300

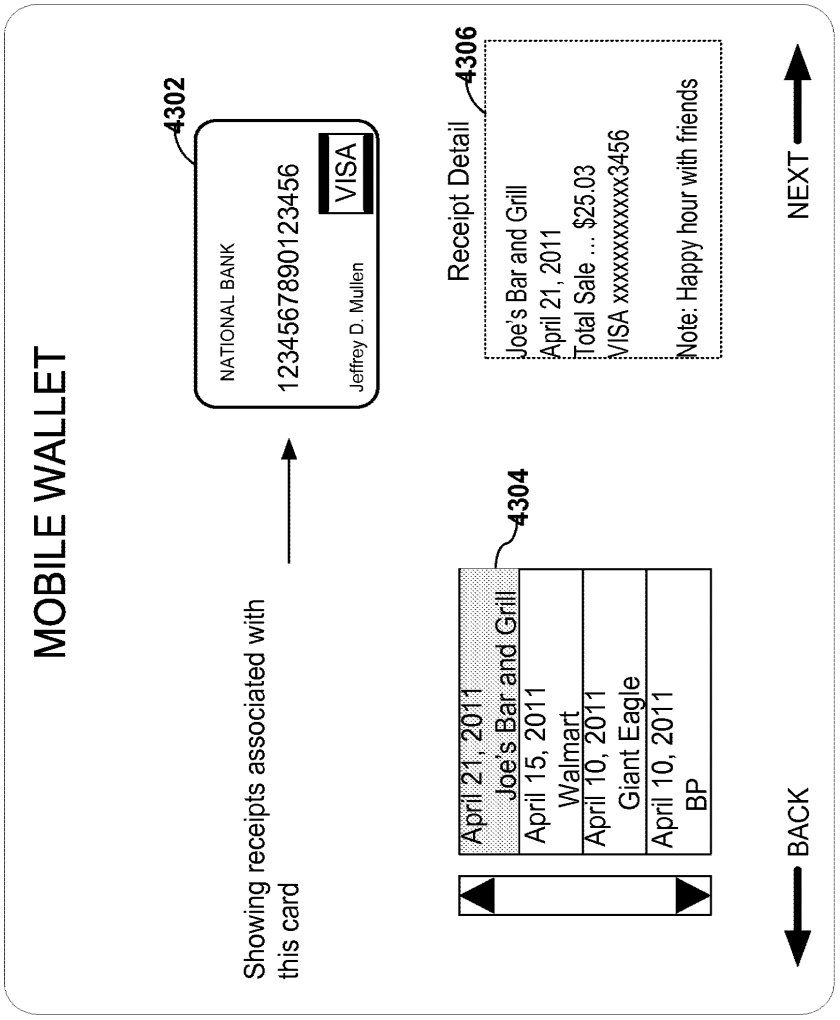

MOBILE WALLET
4302
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
Showing receipts associated with this card
4304
April 21, 2011
Joe's Bar and Grill
April 15, 2011
Walmart
April 10, 2011
Giant Eagle
April 10, 2011
BP
Receipt Detail
4306
Joe's Bar and Grill
April 21, 2011
Total Sale ... $25.03
VISA xxxxxxxxxxx3456
Note: Happy hour with friends
BACK
NEXT

FIG. 43

4400

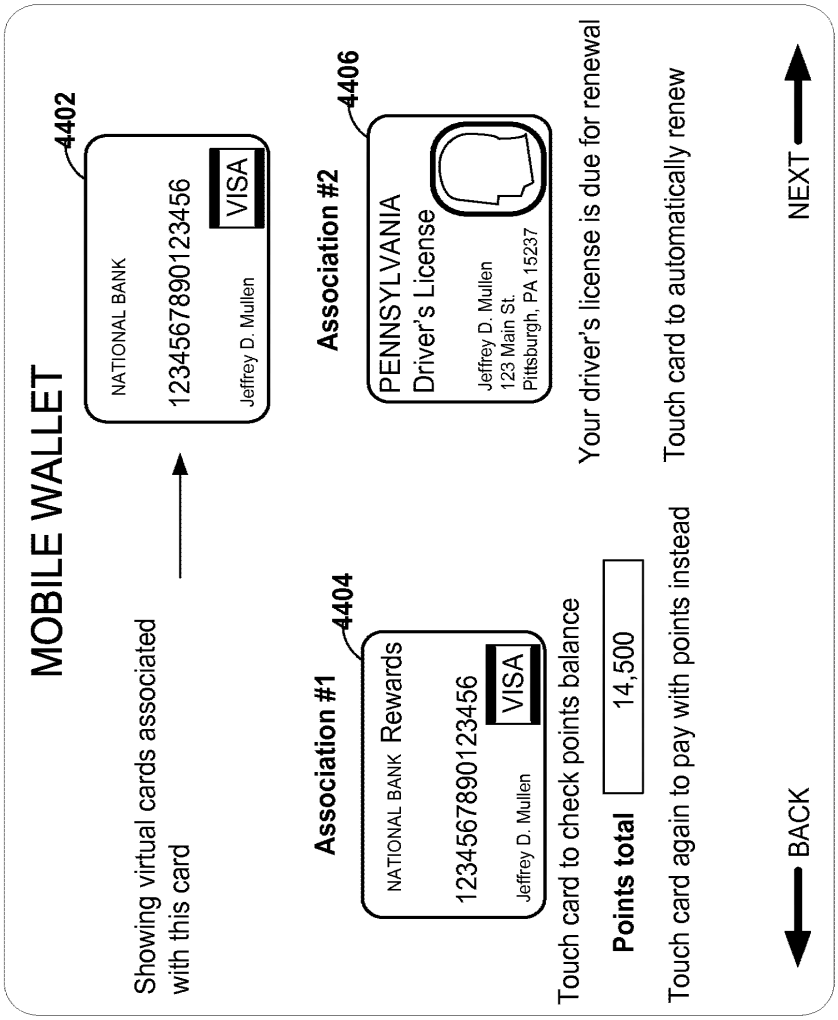

MOBILE WALLET
4402
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
Showing virtual cards associated with this card
Association #2
4406
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
Your driver's license is due for renewal
Association #1
4404
NATIONAL BANK Rewards
1234567890123456
VISA
Jeffrey D. Mullen
Touch card to check points balance
Points total
14,500
Touch card again to pay with points instead
Touch card to automatically renew
BACK
NEXT

FIG. 44

4500

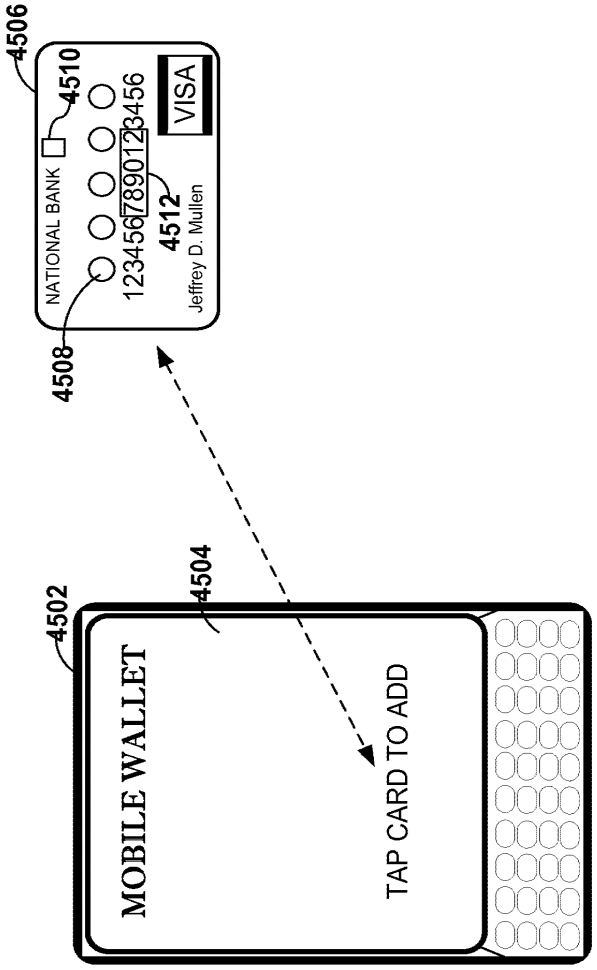

4506
4510
NATIONAL BANK
123456789012 3456
VISA
4512
Jeffrey D. Mullen
4508
4502
4504
MOBILE WALLET
TAP CARD TO ADD

FIG. 45

4600

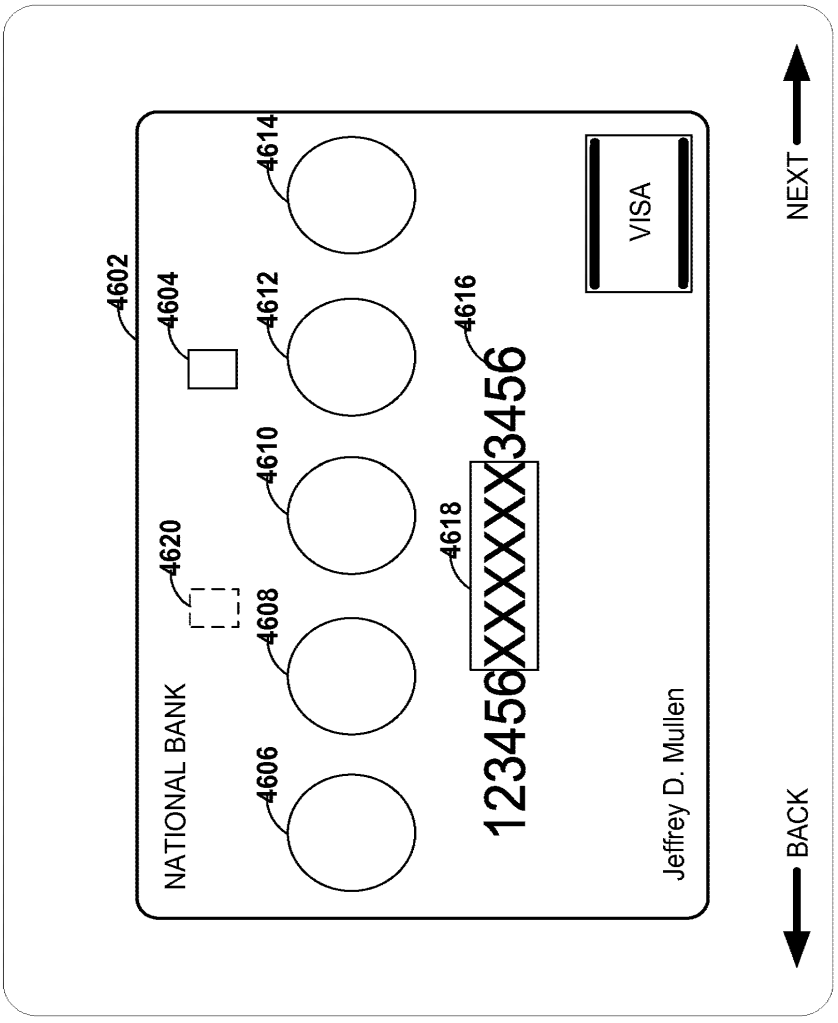

4602
4604
4606
4608
4610
4612
4614
4616
4618
4620
NATIONAL BANK
123456XXXXXX3456
Jeffrey D. Mullen
VISA
NEXT
BACK

FIG. 46

47/73
4700

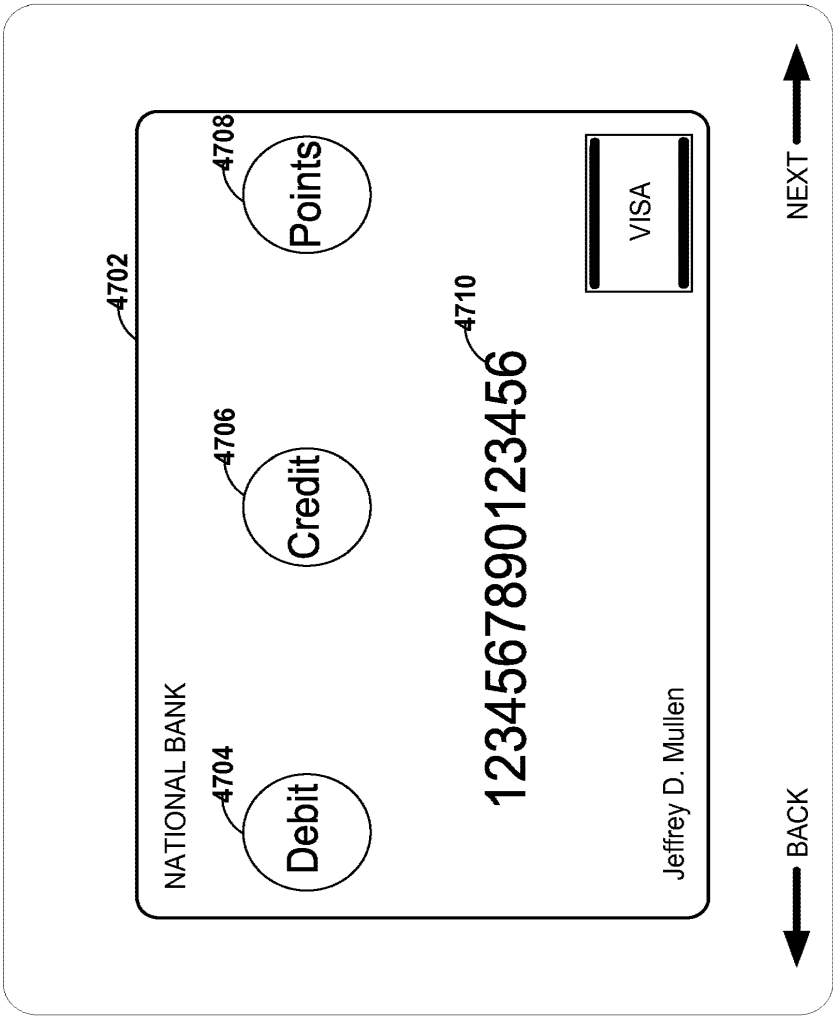


FIG. 47

48/73
4800

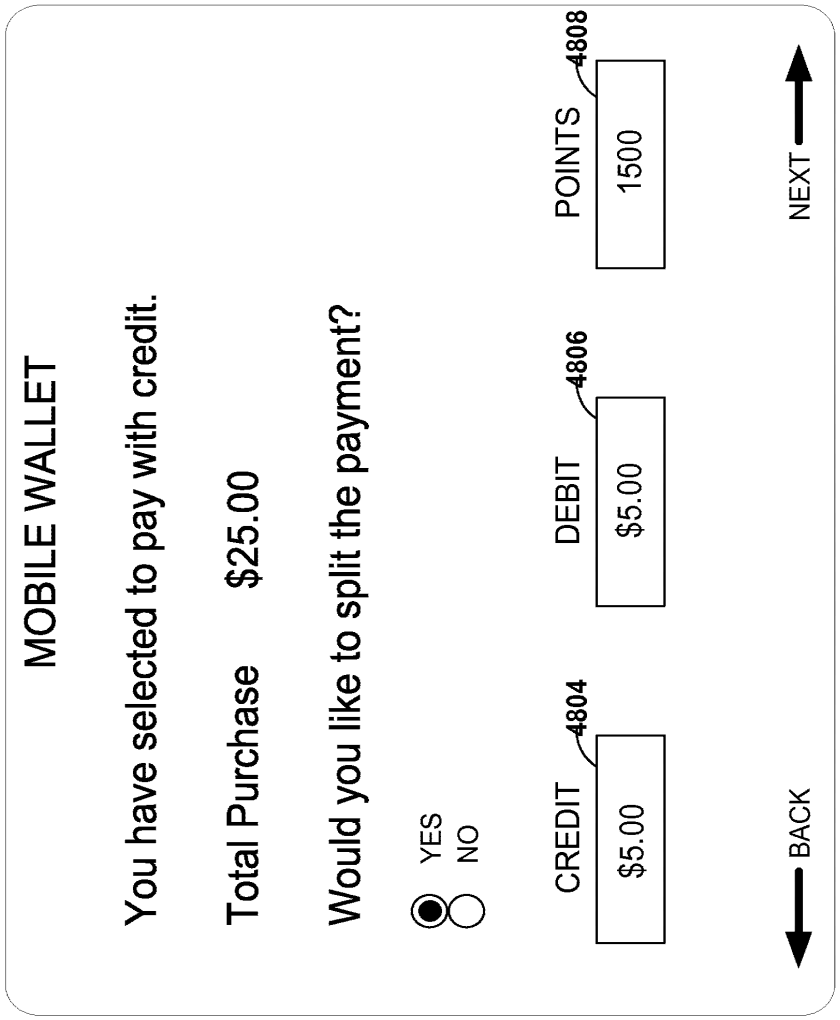


FIG. 48

49/73

4900

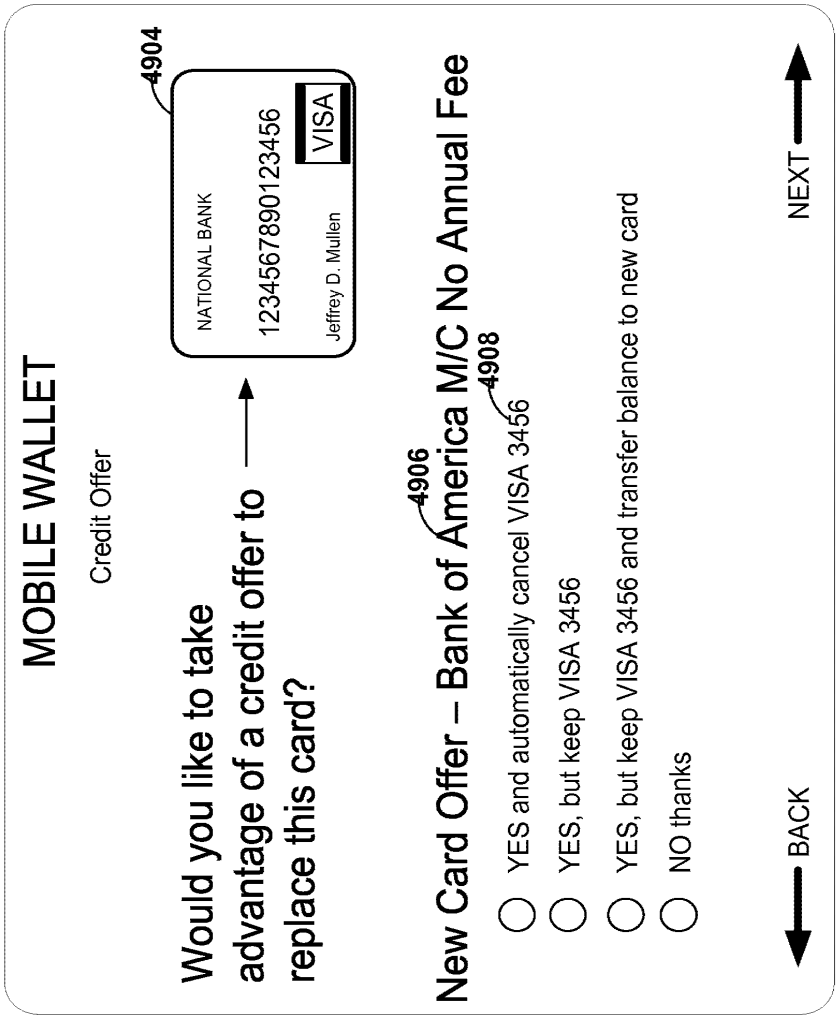


FIG. 49

50/73
5000

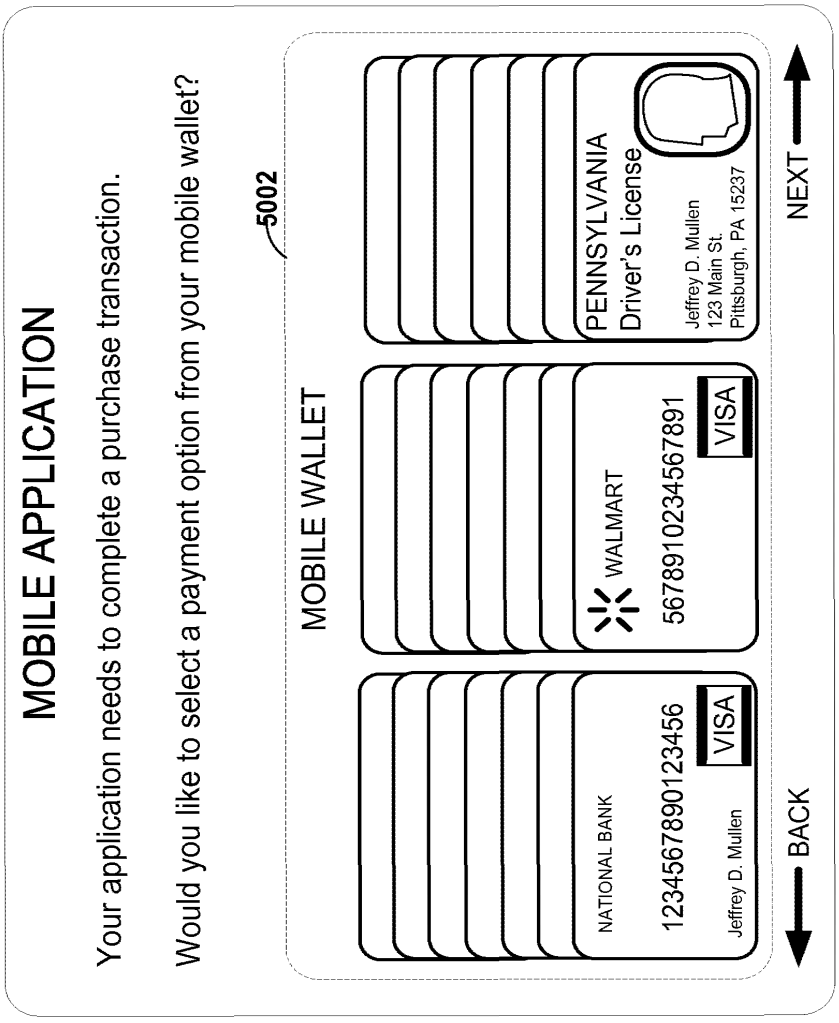


FIG. 50

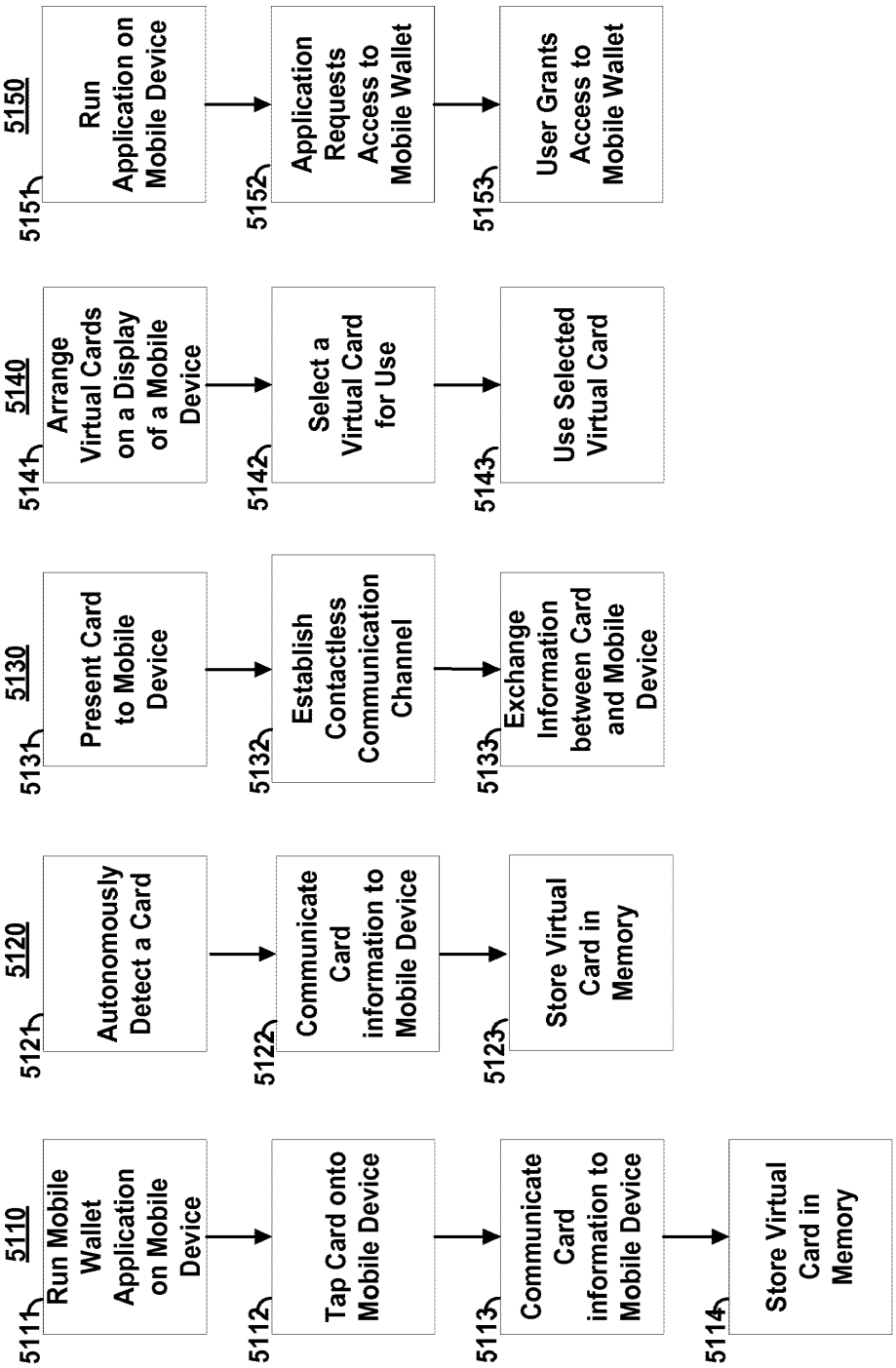

5110
Run Mobile Wallet Application on Mobile Device
5111
Tap Card onto Mobile Device
5112
Communicate Card information to Mobile Device
5113
Store Virtual Card in Memory
5114
5120
Autonomously Detect a Card
5121
Communicate Card information to Mobile Device
5122
Store Virtual Card in Memory
5123
5130
Present Card to Mobile Device
5131
Establish Contactless Communication Channel
5132
Exchange Information between Card and Mobile Device
5133
5140
Arrange Virtual Cards on a Display of a Mobile Device
5141
Select a Virtual Card for Use
5142
Use Selected Virtual Card
5143
5150
Run Application on Mobile Device
5151
Application Requests Access to Mobile Wallet
5152
User Grants Access to Mobile Wallet
5153

FIG. 51

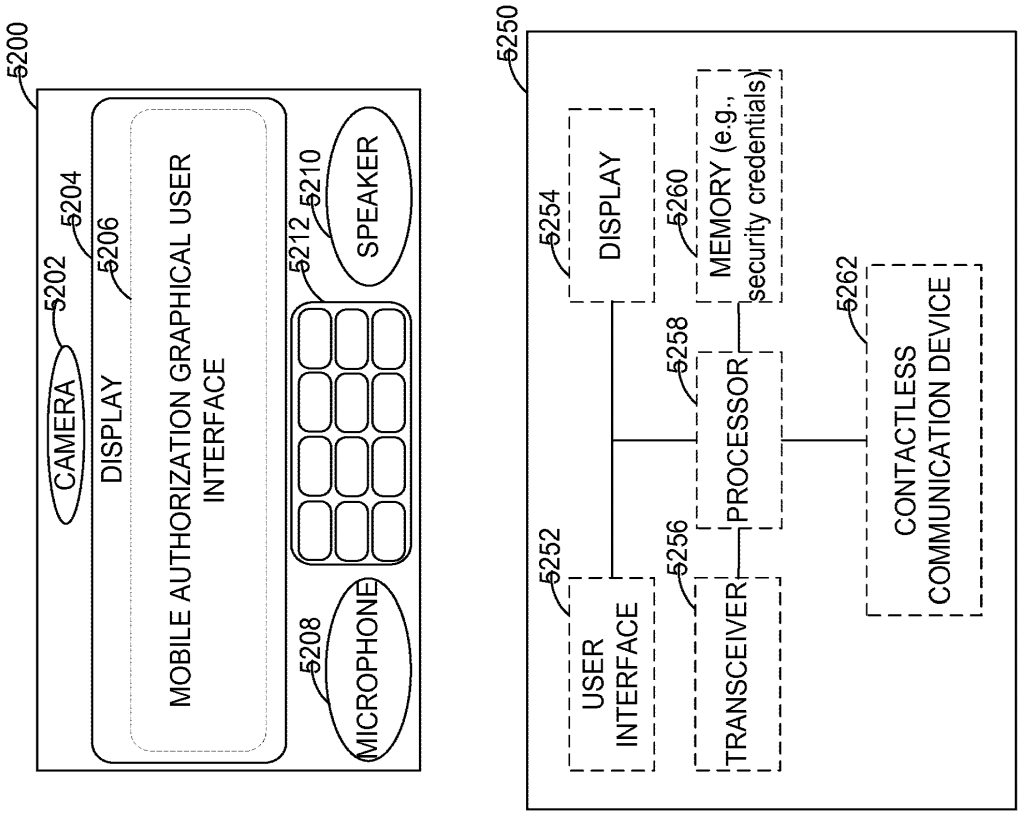

5200
CAMERA
5202
DISPLAY
5204
MOBILE AUTHORIZATION GRAPHICAL USER INTERFACE
5206
5208
MICROPHONE
5210
SPEAKER
5212
5250
USER INTERFACE
5252
DISPLAY
5254
TRANSCEIVER
5256
PROCESSOR
5258
MEMORY (e.g., security credentials)
5260
CONTACTLESS COMMUNICATION DEVICE
5262

FIG. 52

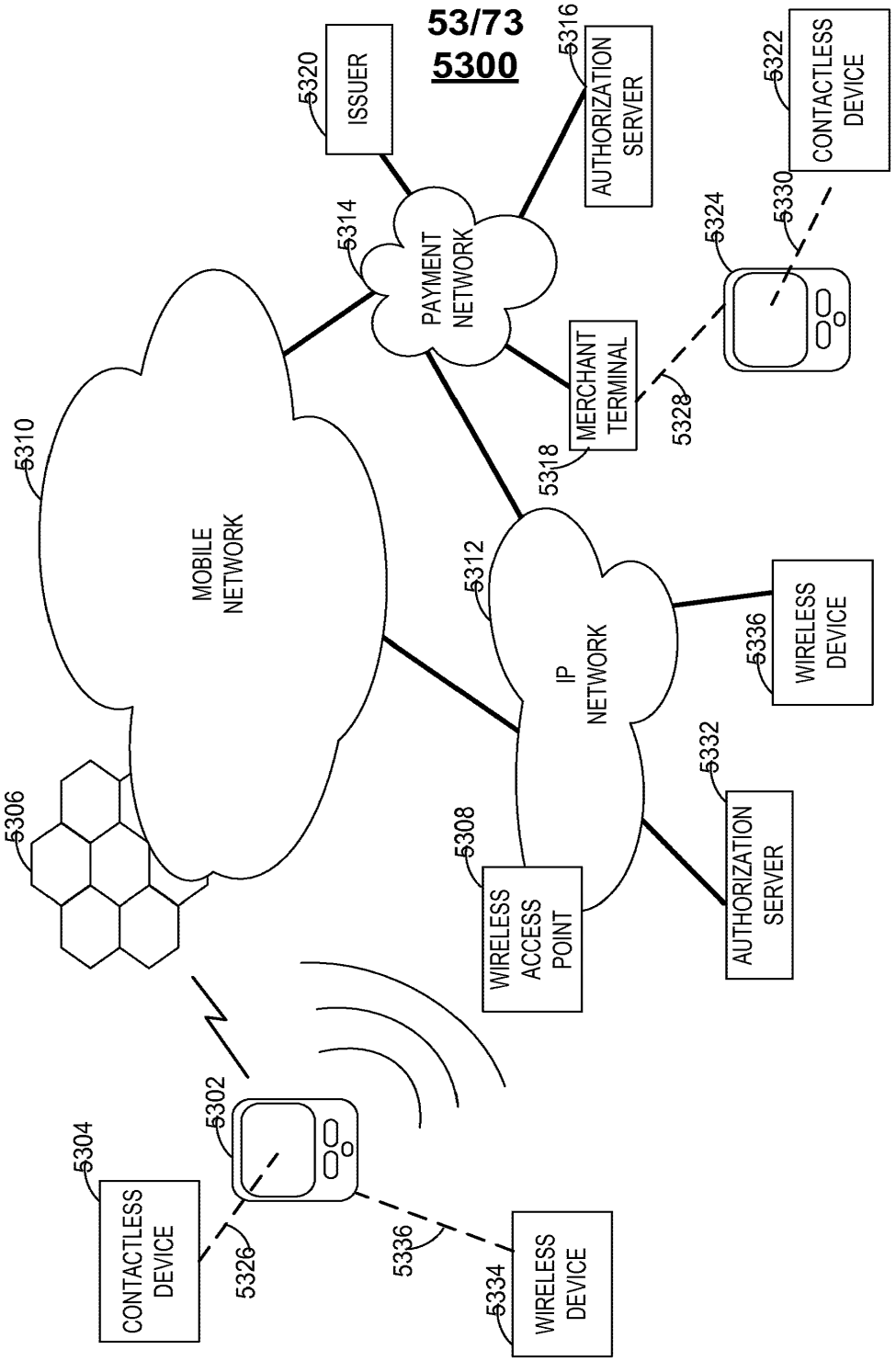

53/73
5300
5320
ISSUER
5316
AUTHORIZATION SERVER
5322
CONTACTLESS DEVICE
5314
PAYMENT NETWORK
5330
5324
5310
MOBILE NETWORK
MERCHANT TERMINAL
5318
5328
5312
IP NETWORK
5336
WIRELESS DEVICE
5306
5332
AUTHORIZATION SERVER
5308
WIRELESS ACCESS POINT
5302
5304
CONTACTLESS DEVICE
5326
5336
5334
WIRELESS DEVICE

FIG. 53

5400

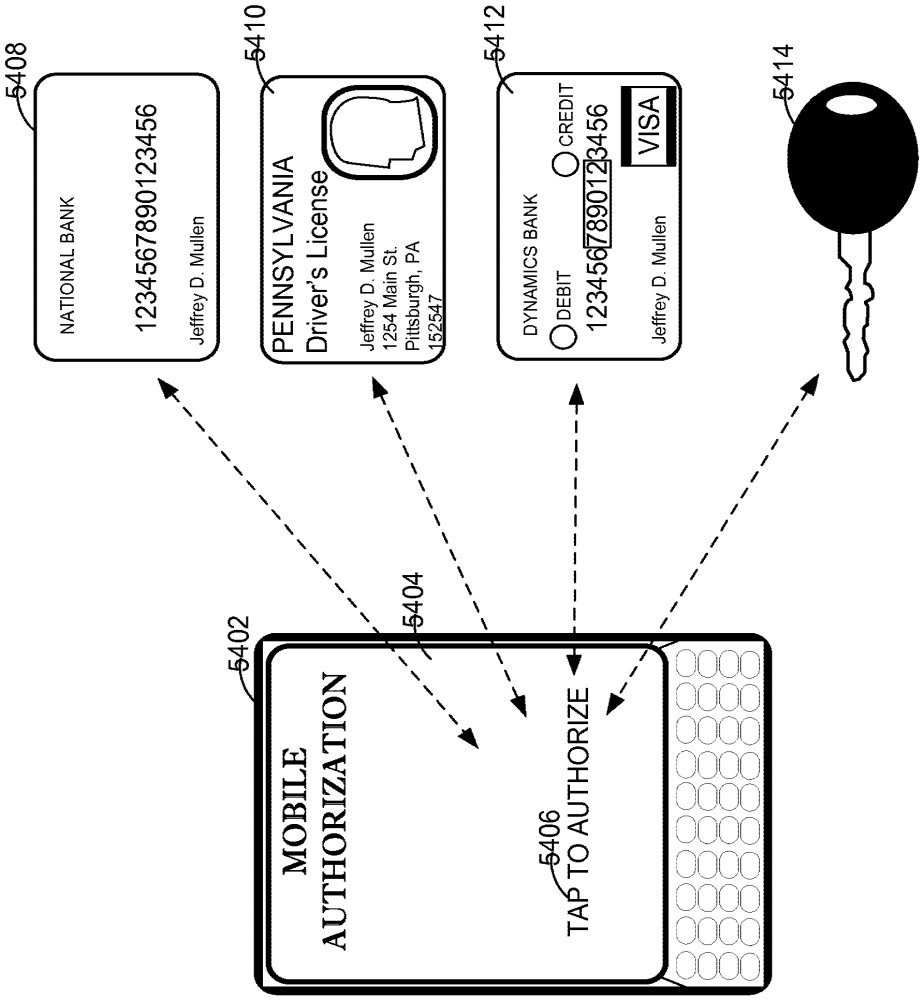

5408
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
5410
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
1254 Main St.
Pittsburgh, PA
152547
5412
DYNAMICS BANK
DEBIT
CREDIT
1234567890123456
VISA
Jeffrey D. Mullen
5414
5402
MOBILE
AUTHORIZATION
5404
5406
TAP TO AUTHORIZE

FIG. 54

5500

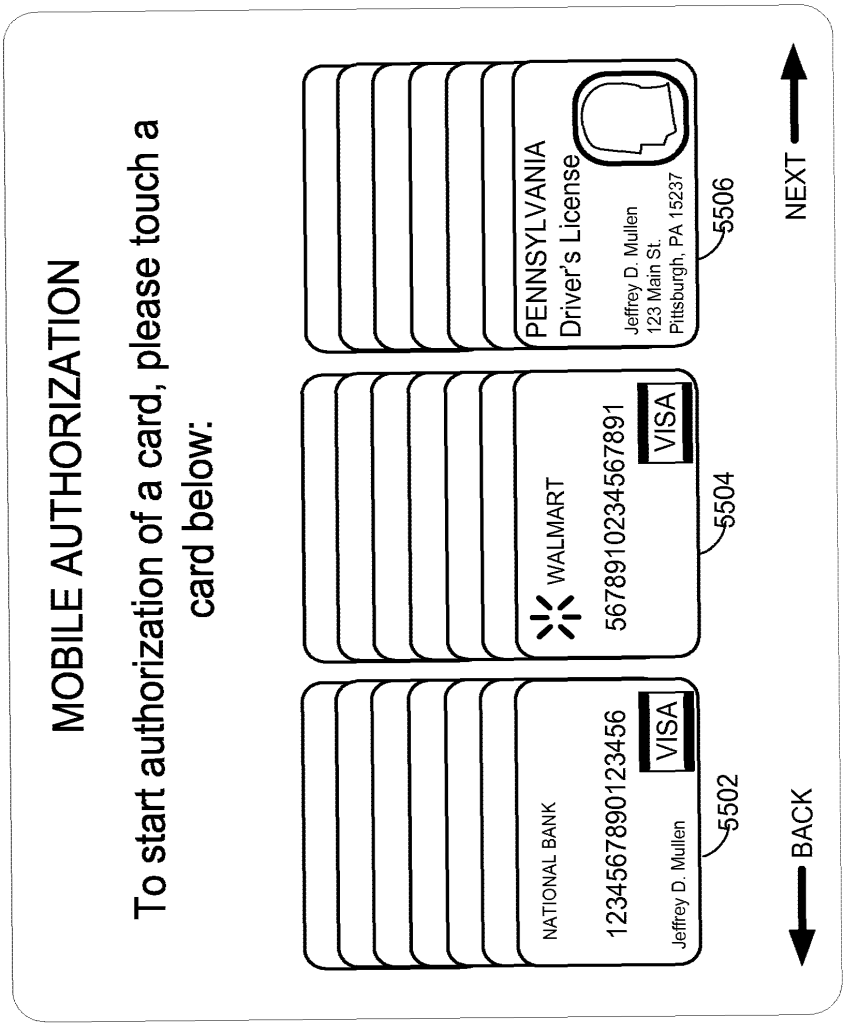

MOBILE AUTHORIZATION
To start authorization of a card, please touch a card below:
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
5502
WALMART
5678910234567891
VISA
5504
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
5506
BACK
NEXT

FIG. 55

5600

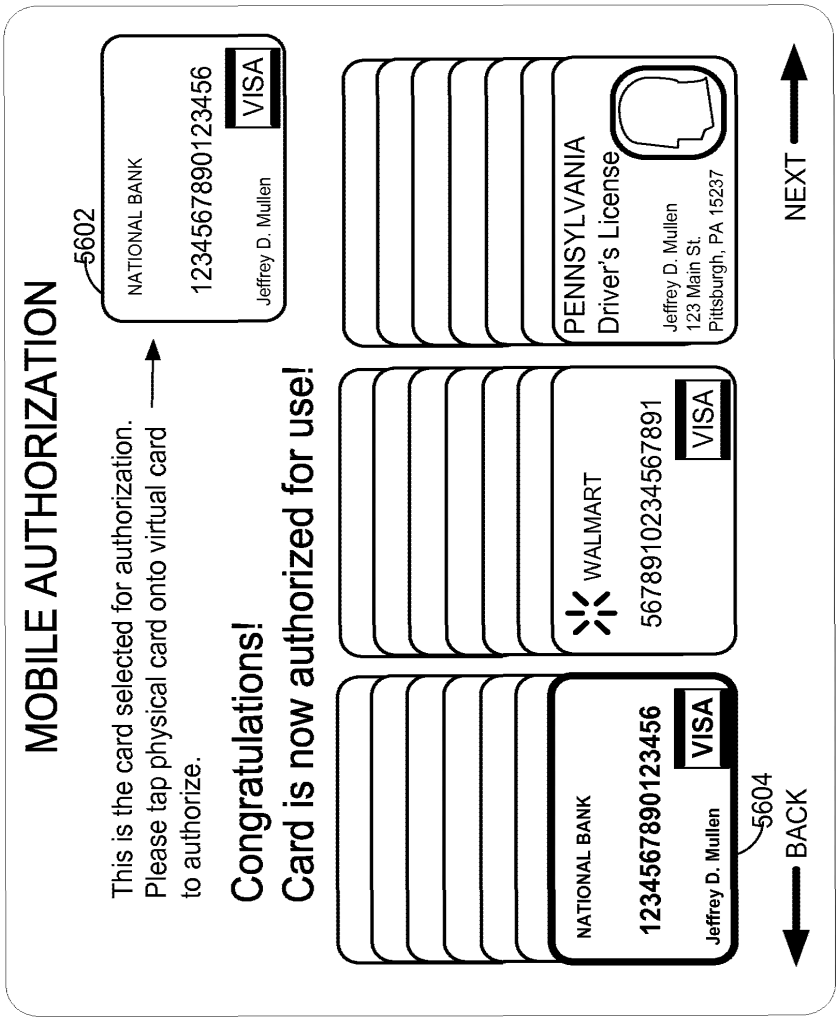

MOBILE AUTHORIZATION
5602
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
This is the card selected for authorization.
Please tap physical card onto virtual card
to authorize.
Congratulations!
Card is now authorized for use!
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
WALMART
5678910234567891
VISA
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
5604
BACK
NEXT

FIG. 56

57/73
5700

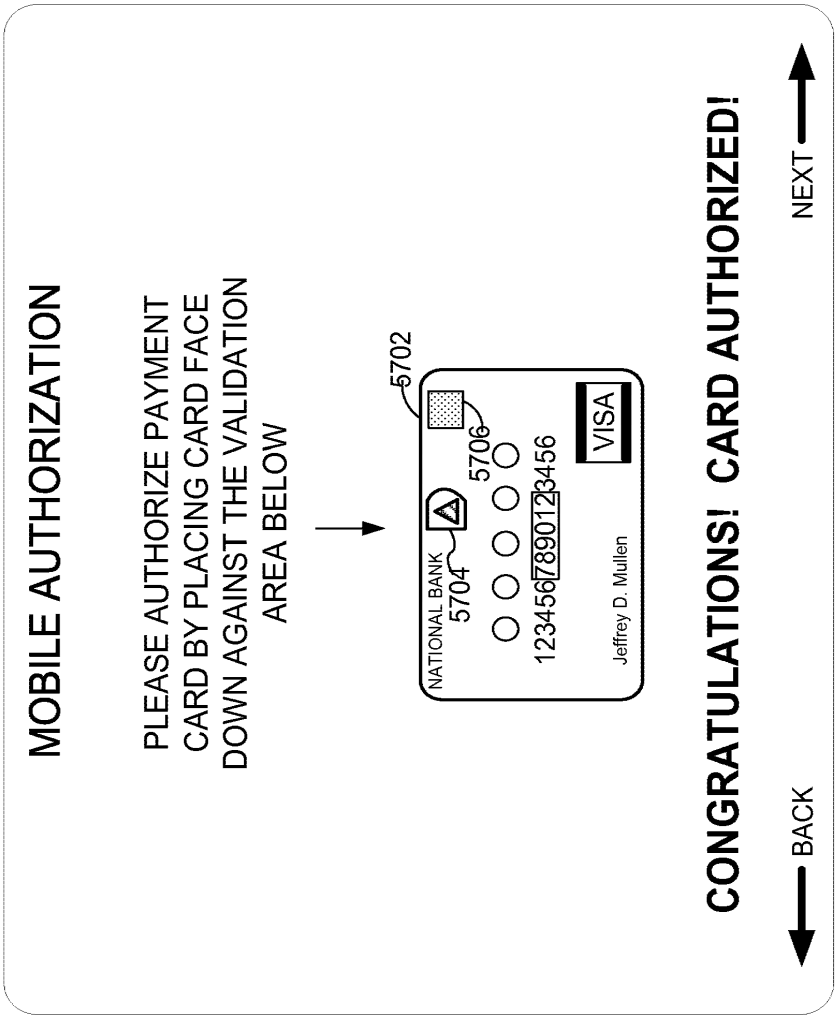


FIG. 57

58/73
5800

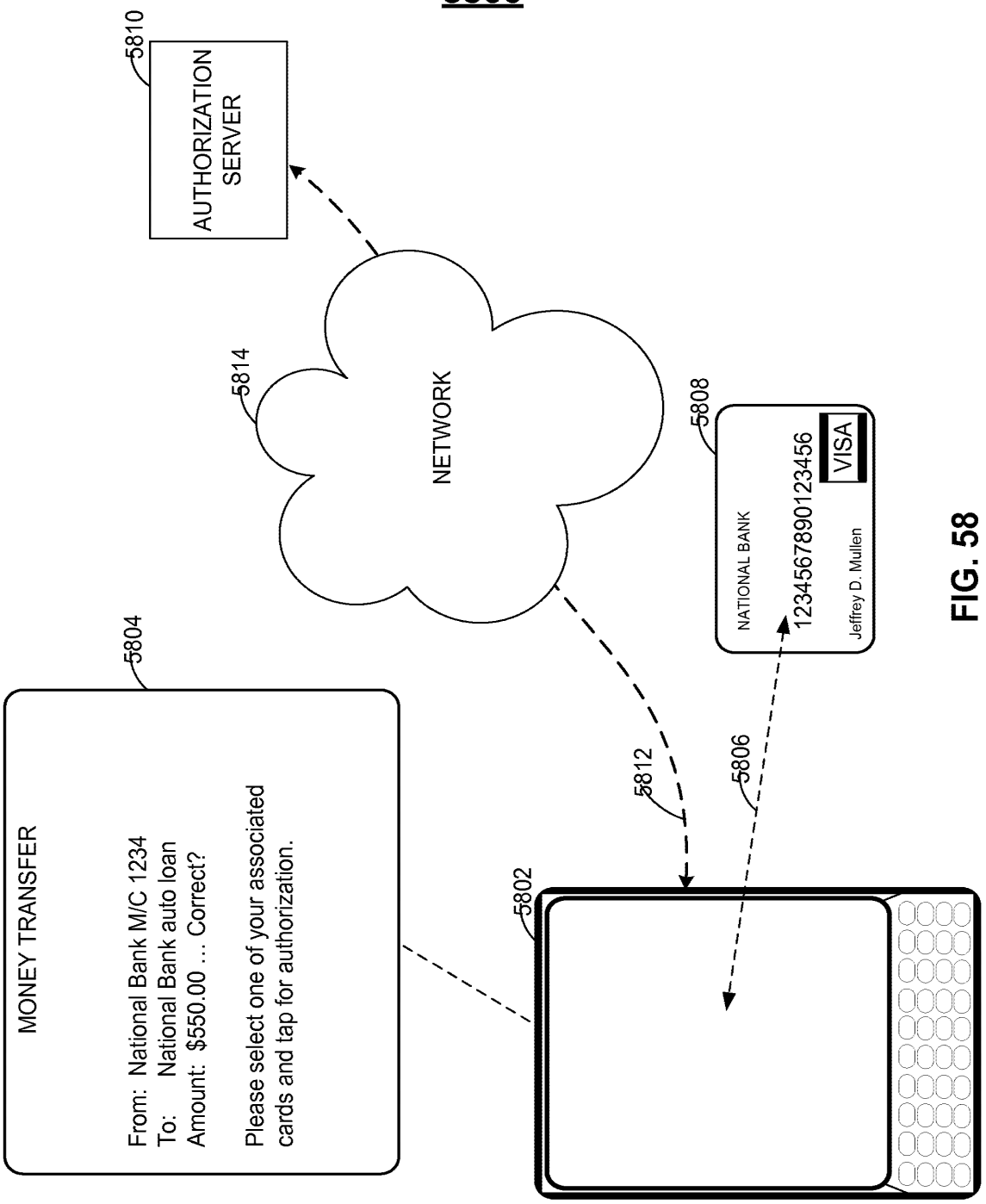


FIG. 58

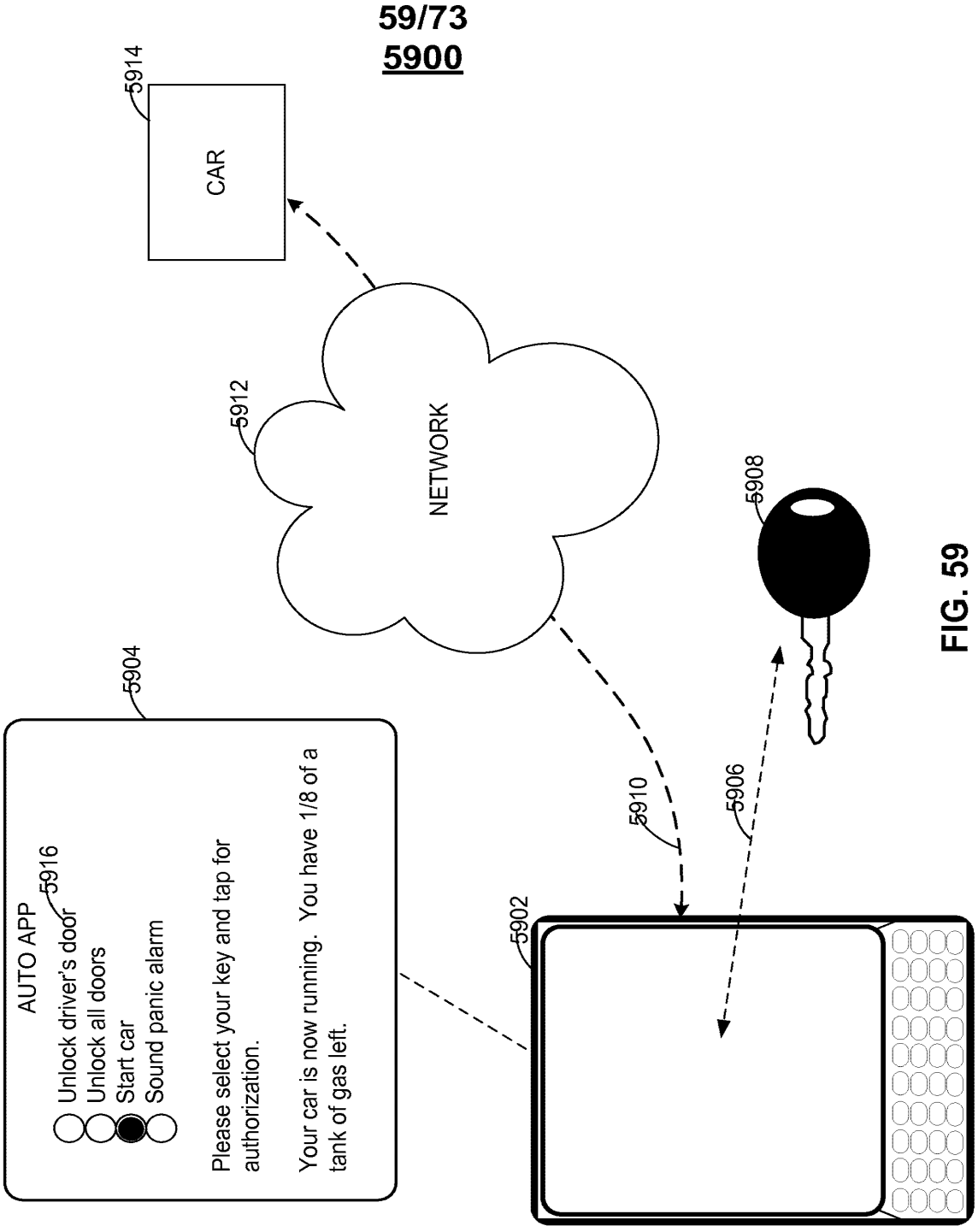

5900
5914
CAR
5912
NETWORK
5908
5904
AUTO APP
5916
Unlock driver's door
Unlock all doors
Start car
Sound panic alarm
Please select your key and tap for authorization.
Your car is now running. You have 1/8 of a tank of gas left.
5910
5906
5902

FIG. 59

6000

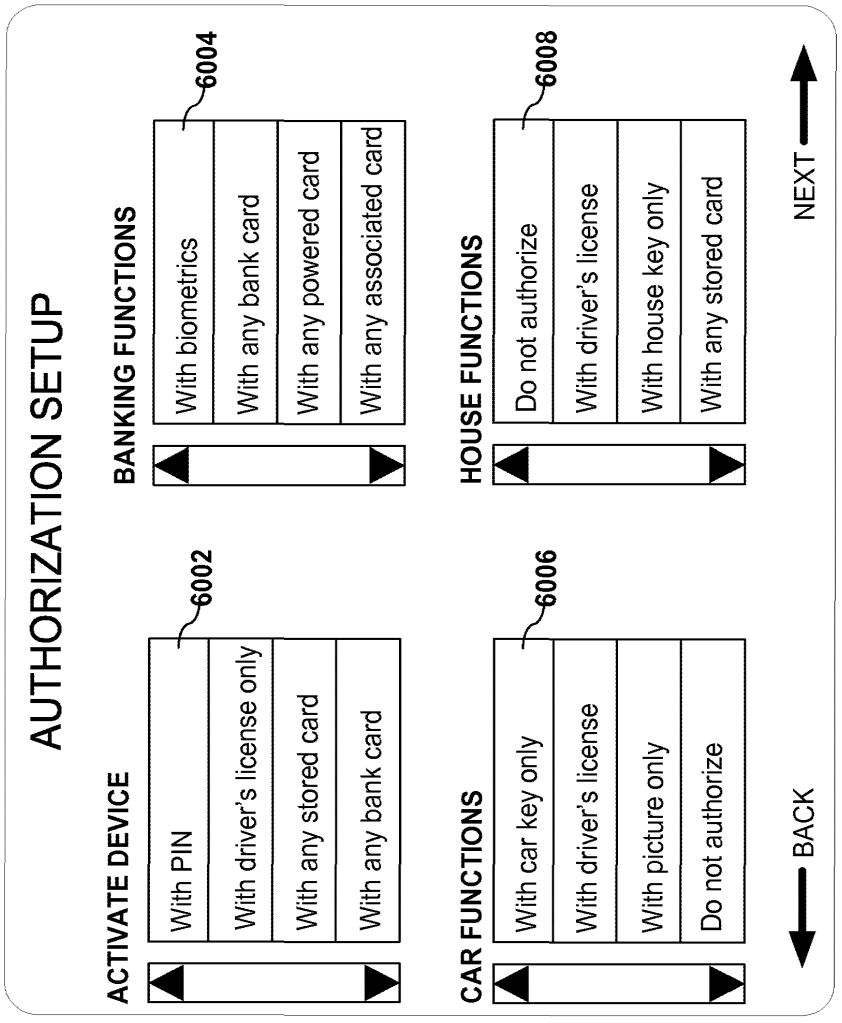

AUTHORIZATION SETUP
ACTIVATE DEVICE
6002
With PIN
With driver's license only
With any stored card
With any bank card
BANKING FUNCTIONS
6004
With biometrics
With any bank card
With any powered card
With any associated card
CAR FUNCTIONS
6006
With car key only
With driver's license
With picture only
Do not authorize
HOUSE FUNCTIONS
6008
Do not authorize
With driver's license
With house key only
With any stored card
BACK
NEXT

FIG. 60

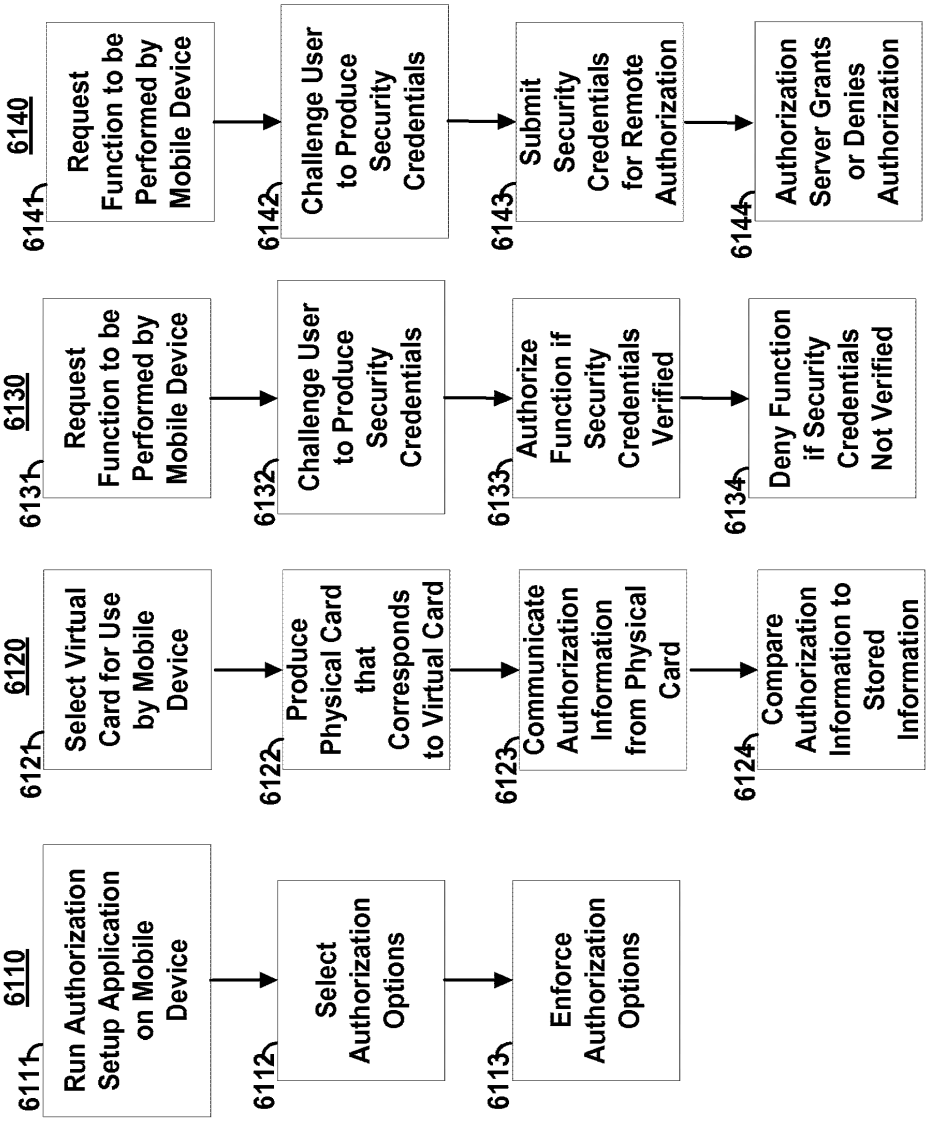

6110
6111
Run Authorization Setup Application on Mobile Device
6112
Select Authorization Options
6113
Enforce Authorization Options
6120
6121
Select Virtual Card for Use by Mobile Device
6122
Produce Physical Card that Corresponds to Virtual Card
6123
Communicate Authorization Information from Physical Card
6124
Compare Authorization Information to Stored Information
6130
6131
Request Function to be Performed by Mobile Device
6132
Challenge User to Produce Security Credentials
6133
Authorize Function if Security Credentials Verified
6134
Deny Function if Security Credentials Not Verified
6140
6141
Request Function to be Performed by Mobile Device
6142
Challenge User to Produce Security Credentials
6143
Submit Security Credentials for Remote Authorization
6144
Authorization Server Grants or Denies Authorization

FIG. 61

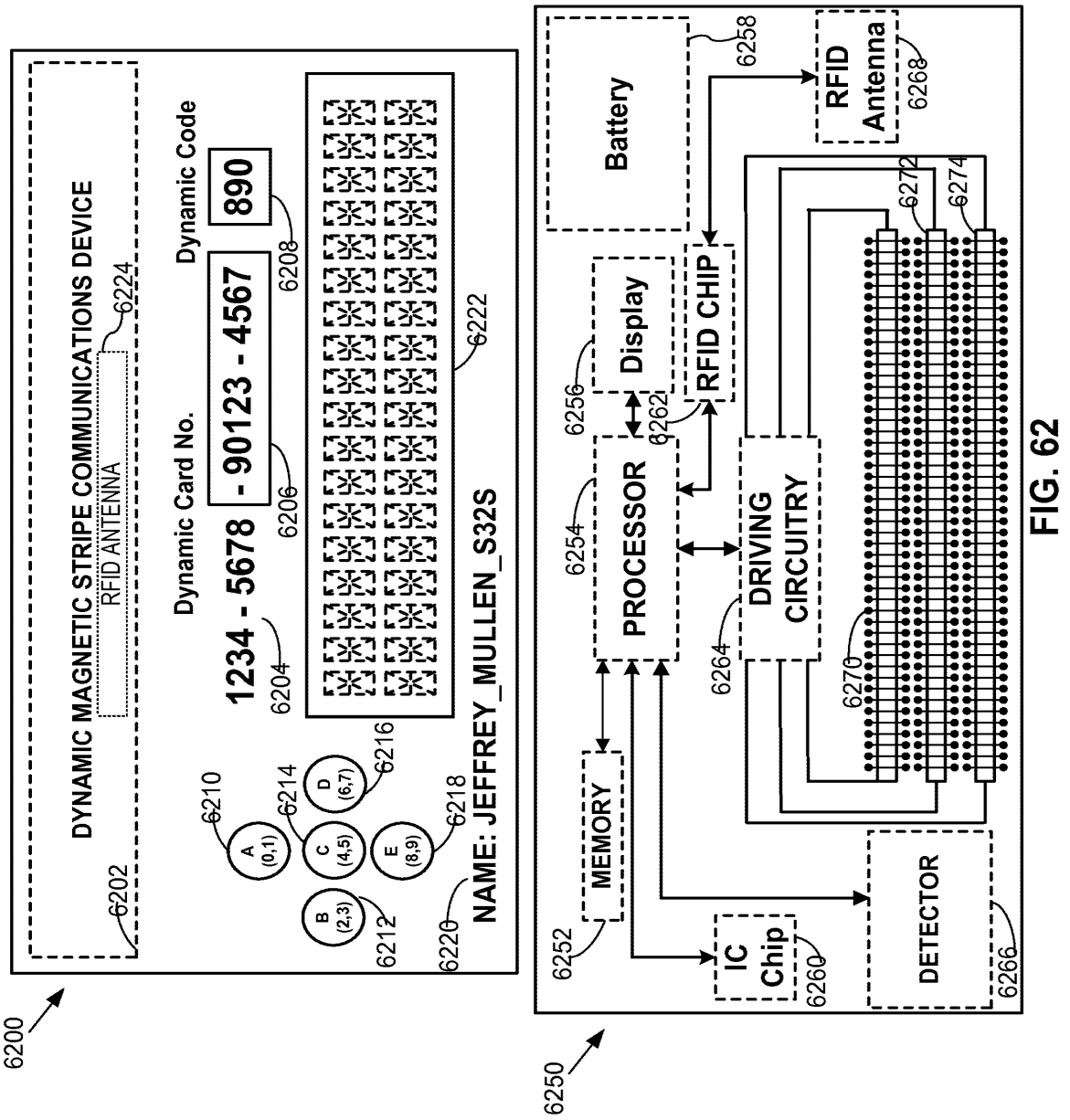

6200
DYNAMIC MAGNETIC STRIPE COMMUNICATIONS DEVICE
RFID ANTENNA
6224
6202
Dynamic Card No.
1234 - 5678 - 90123 - 4567
6204
6206
Dynamic Code
890
6208
6222
A (0,1)
B (2,3)
C (4,5)
D (6,7)
E (8,9)
6210
6212
6214
6216
6218
6220
NAME: JEFFREY_MULLEN_S32S
6250
Battery
6258
RFID Antenna
6268
6272
6274
Display
6256
RFID CHIP
6262
PROCESSOR
6254
DRIVING CIRCUITRY
6264
6270
MEMORY
6252
IC Chip
6260
DETECTOR
6266

FIG. 62

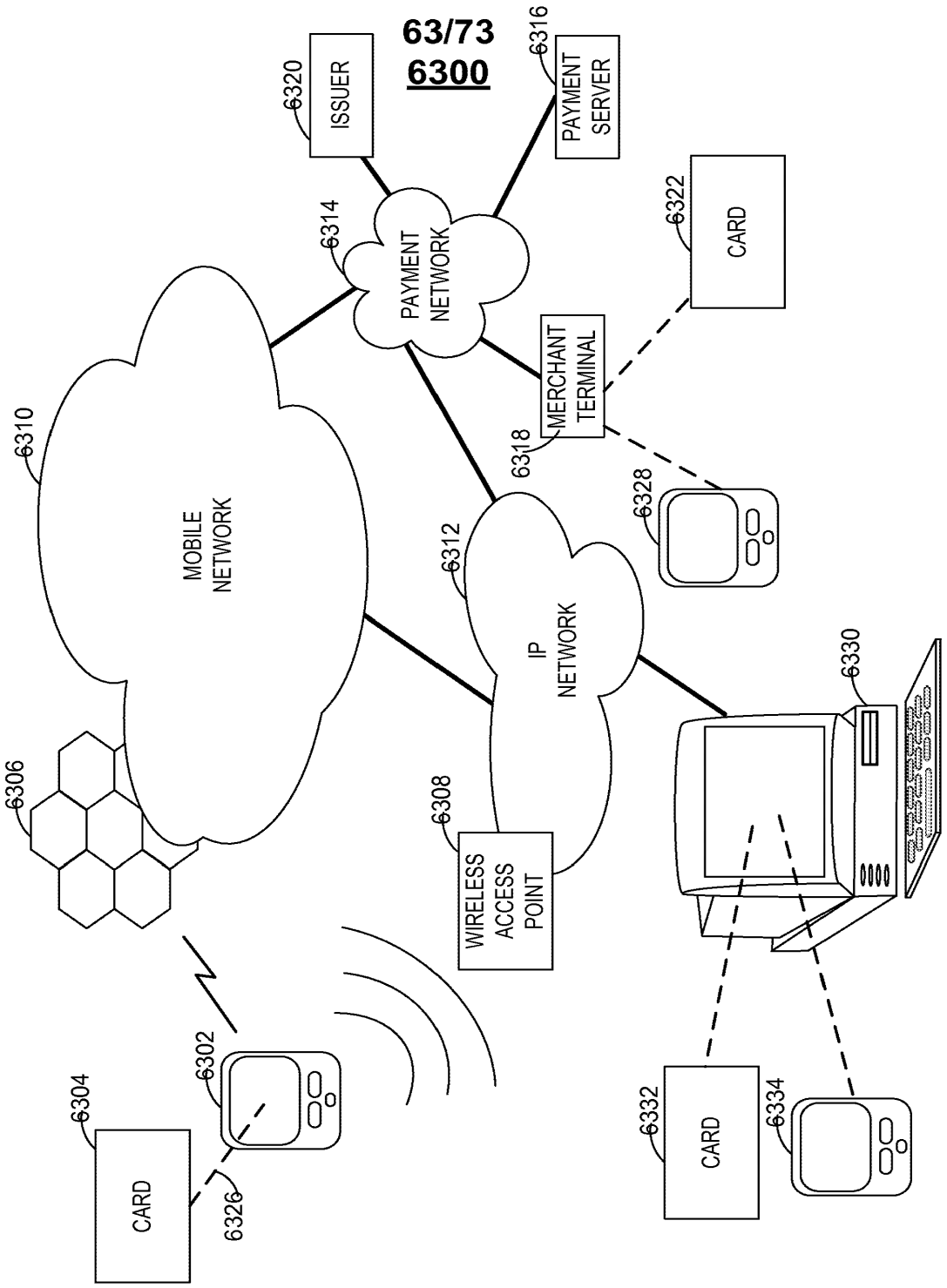

63/73
6300
6320
ISSUER
6316
PAYMENT SERVER
6314
PAYMENT NETWORK
6322
CARD
6310
MOBILE NETWORK
MERCHANT TERMINAL
6318
6328
6312
IP NETWORK
6330
6306
6308
WIRELESS ACCESS POINT
6302
6304
CARD
6326
6332
CARD
6334

FIG. 63

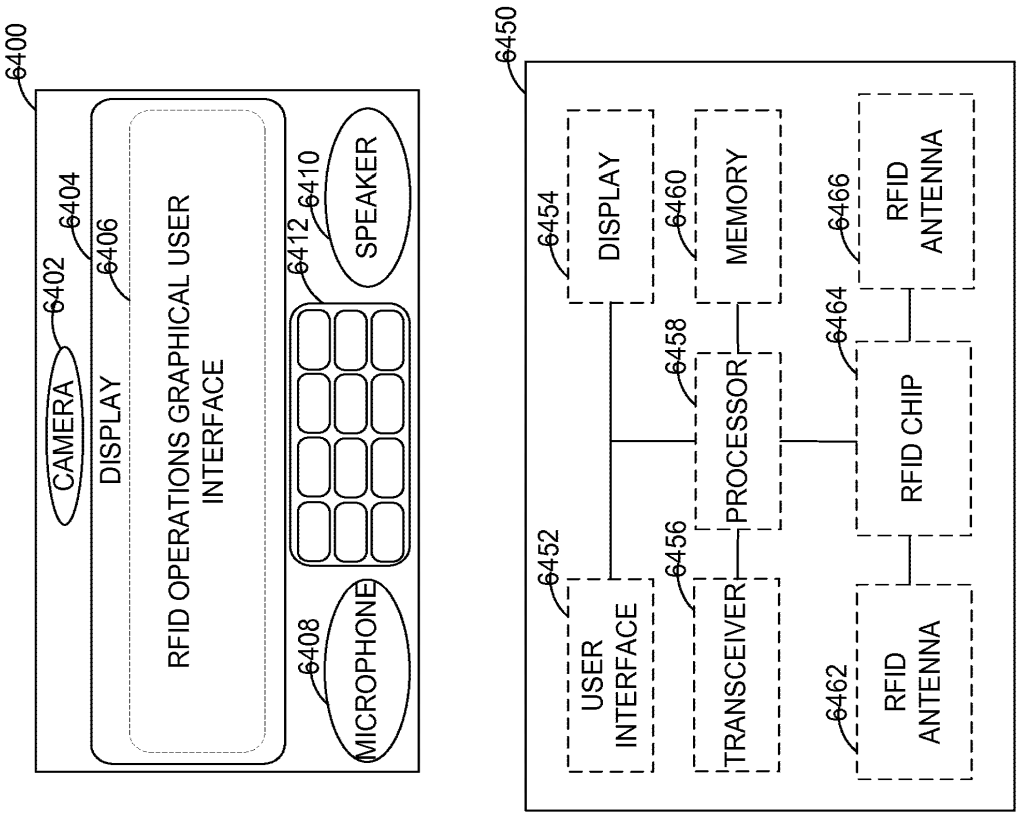

6400
CAMERA
6402
DISPLAY
6404
RFID OPERATIONS GRAPHICAL USER INTERFACE
6406
6408
MICROPHONE
6410
SPEAKER
6412
6450
USER INTERFACE
6452
TRANSCEIVER
6456
PROCESSOR
6458
DISPLAY
6454
MEMORY
6460
RFID CHIP
6464
RFID ANTENNA
6462
RFID ANTENNA
6466

FIG. 64

65/73
6500

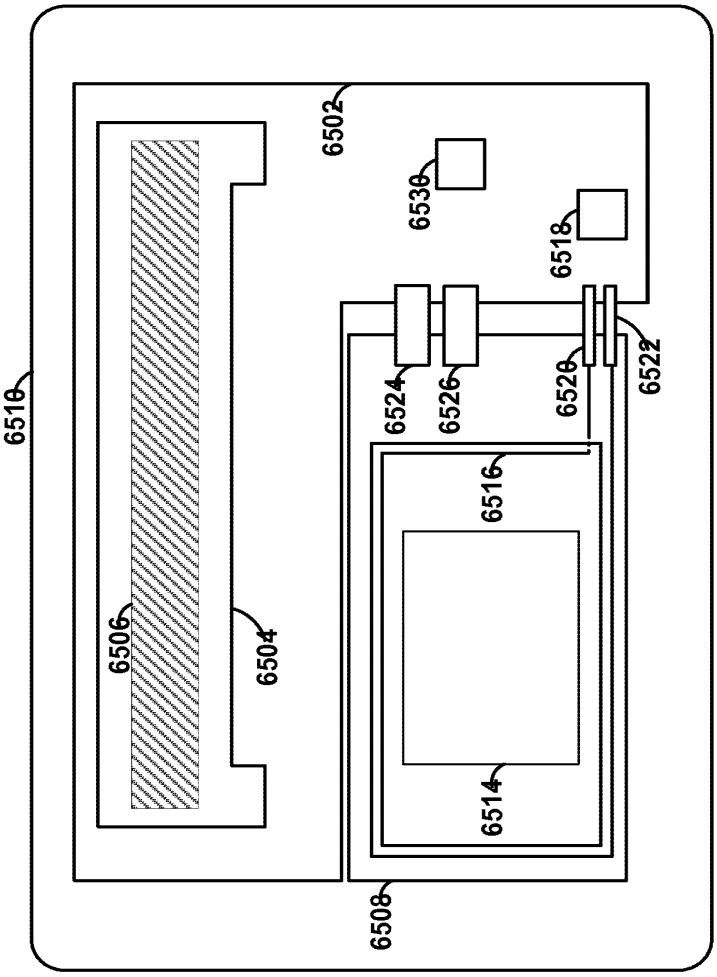


FIG. 65

6600

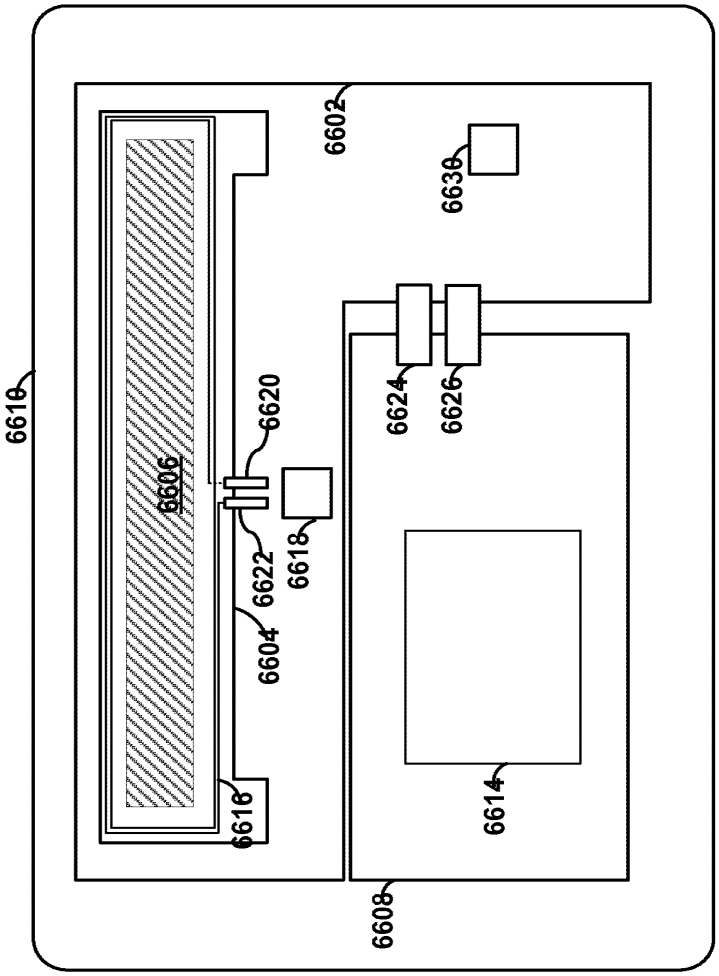

6602
6638
6624
6626
6610
6620
6606
6622
6618
6604
6616
6614
6608

FIG. 66

67/73

6700

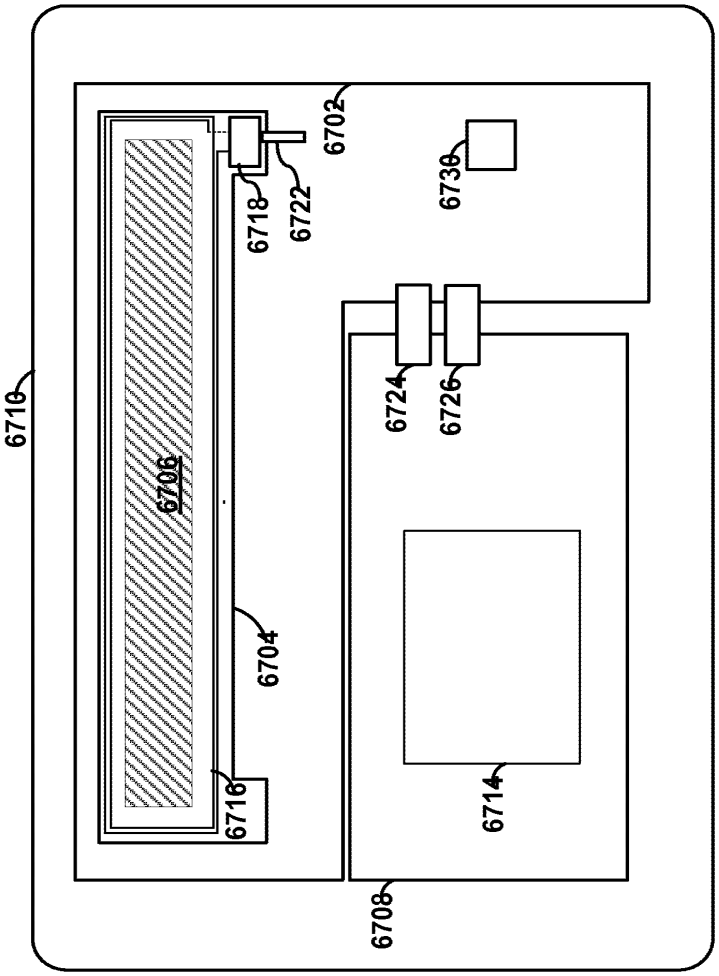


FIG. 67

68/73

6800

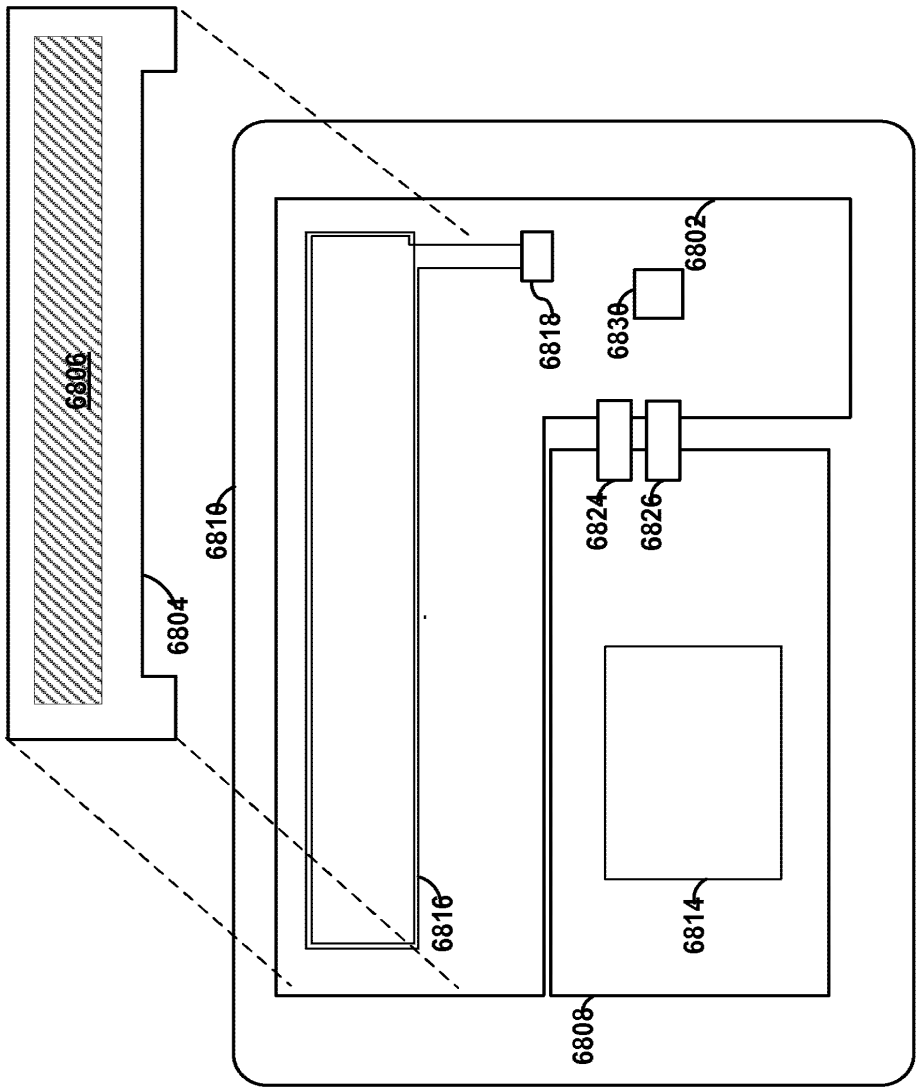


FIG. 68

69/73

6900

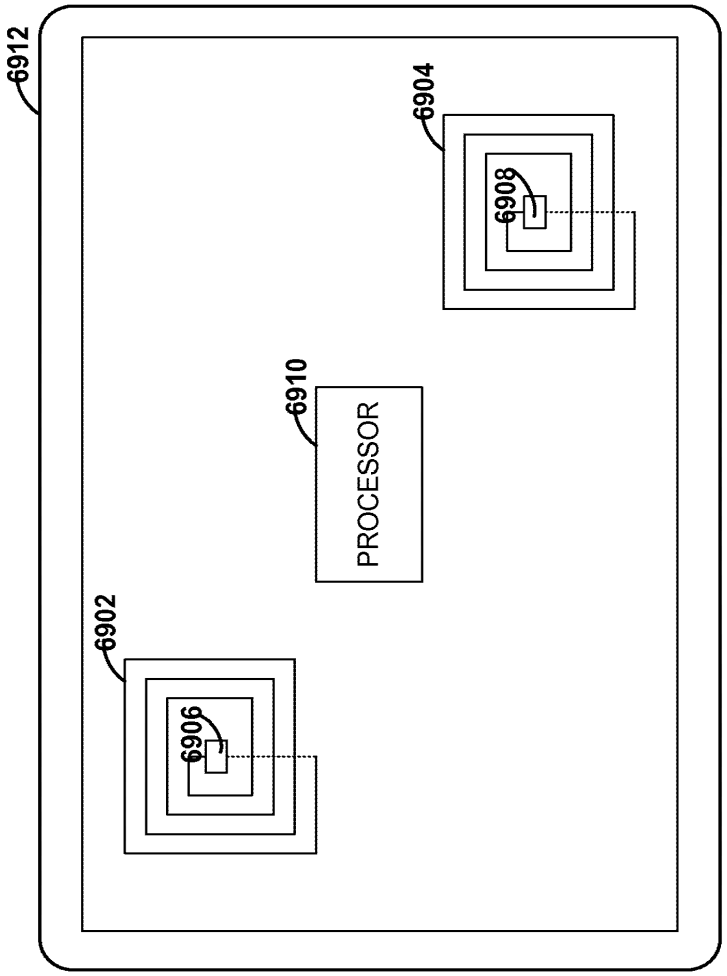


FIG. 69

70/73
7000

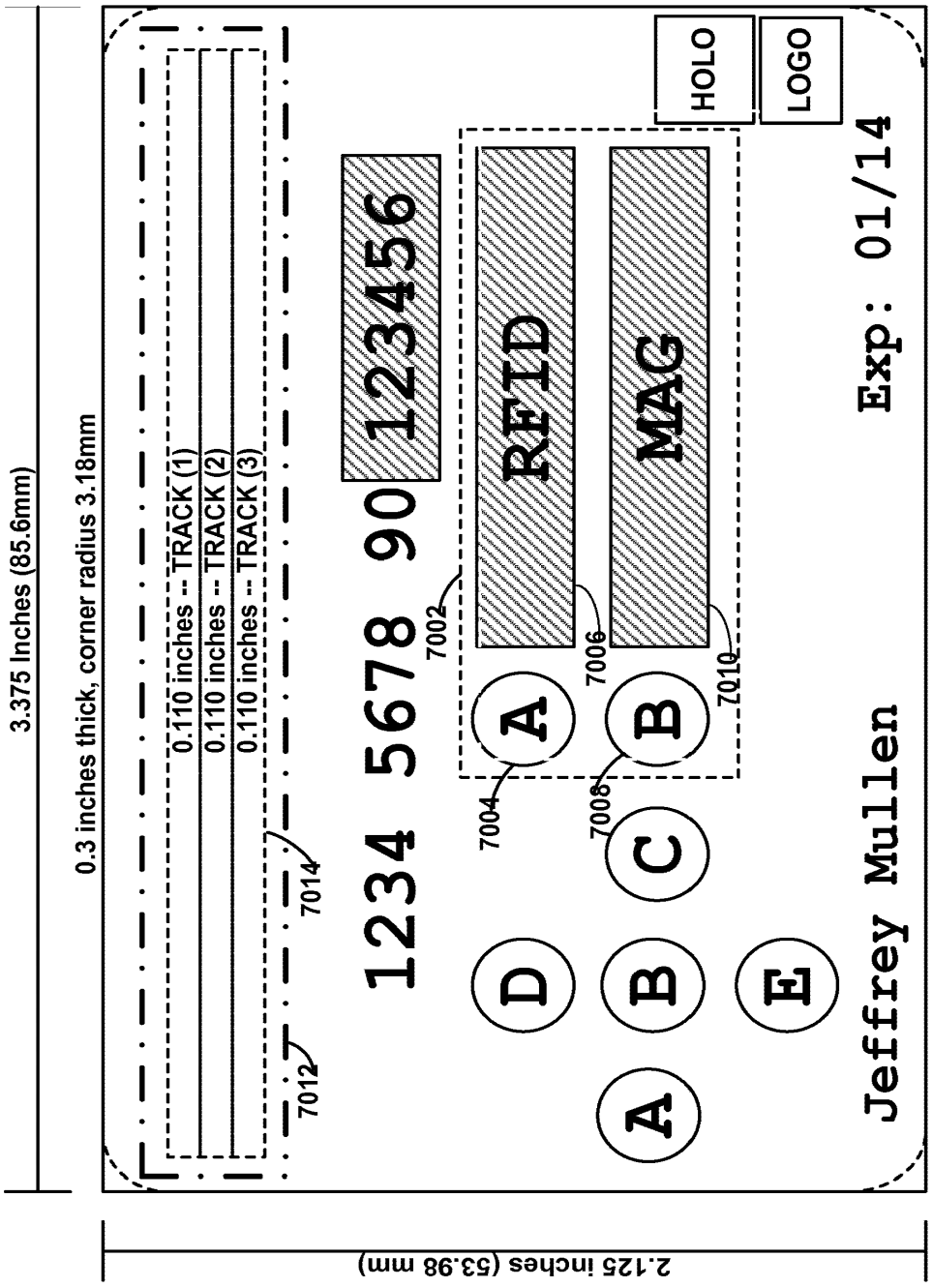


FIG. 70

71/73
7100

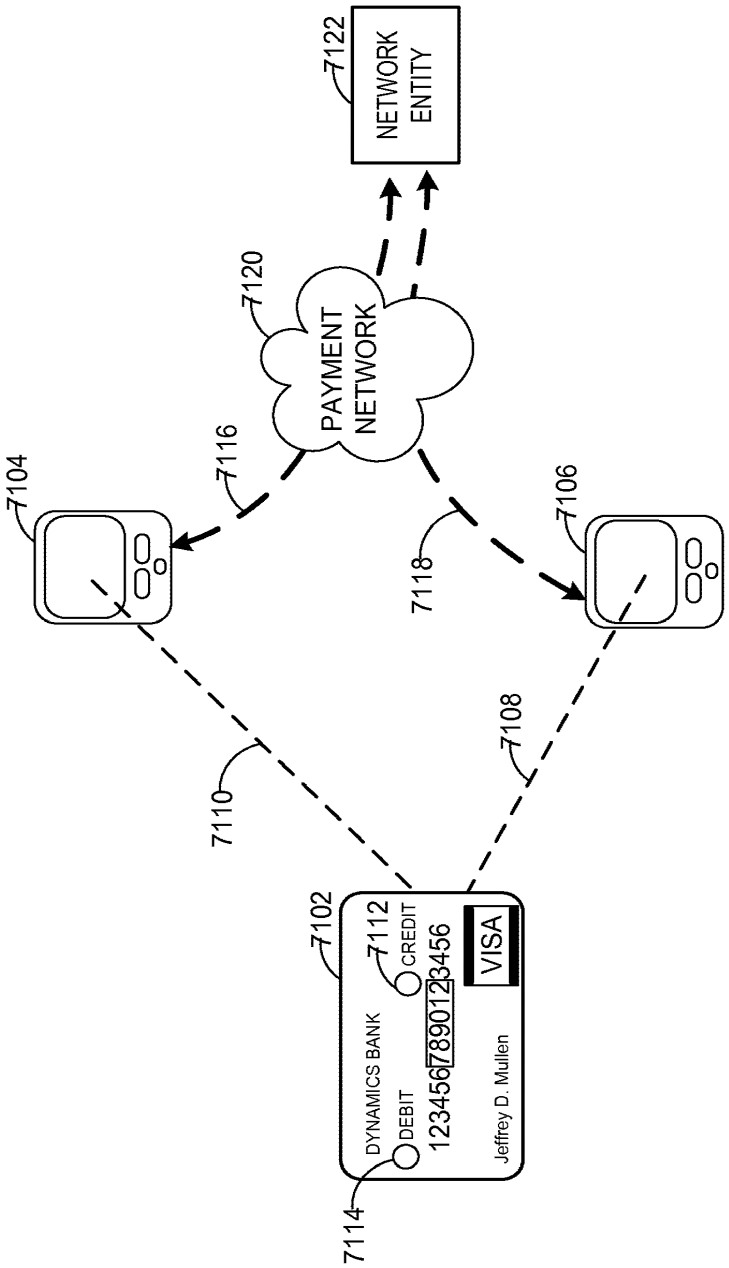


FIG. 71

72/73
7200

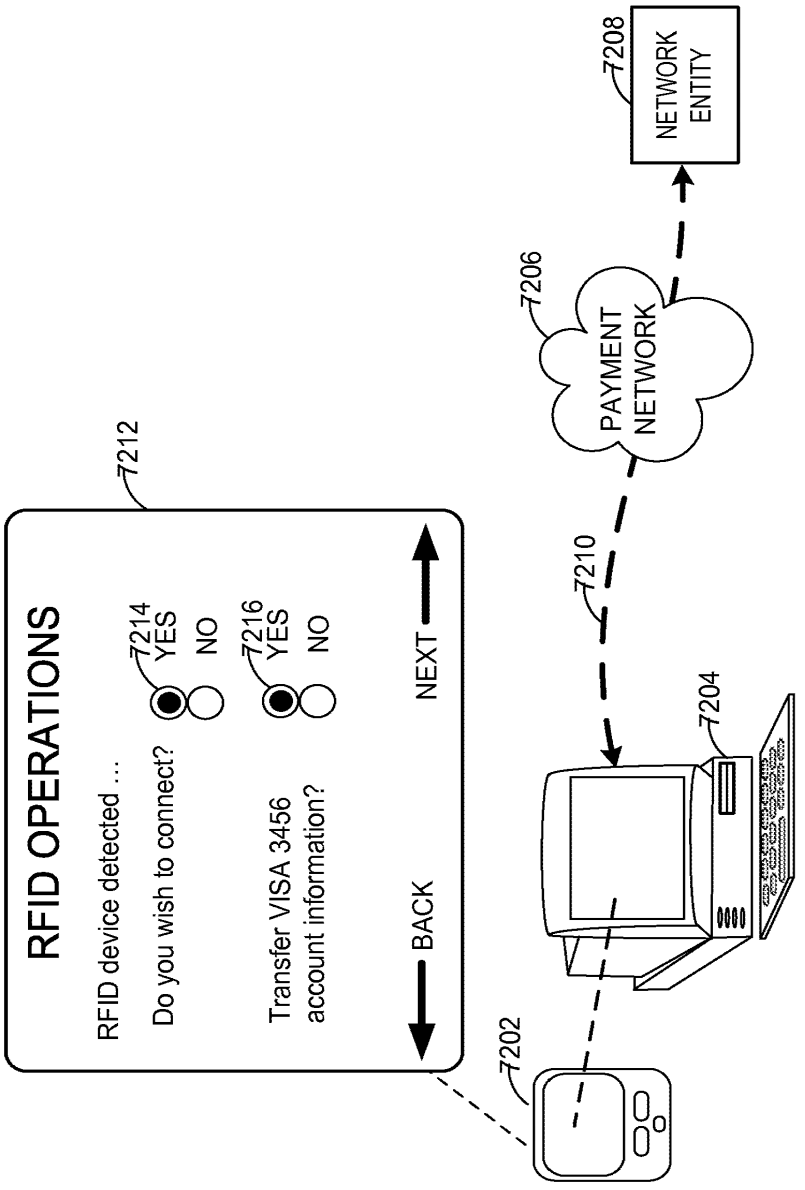


FIG. 72

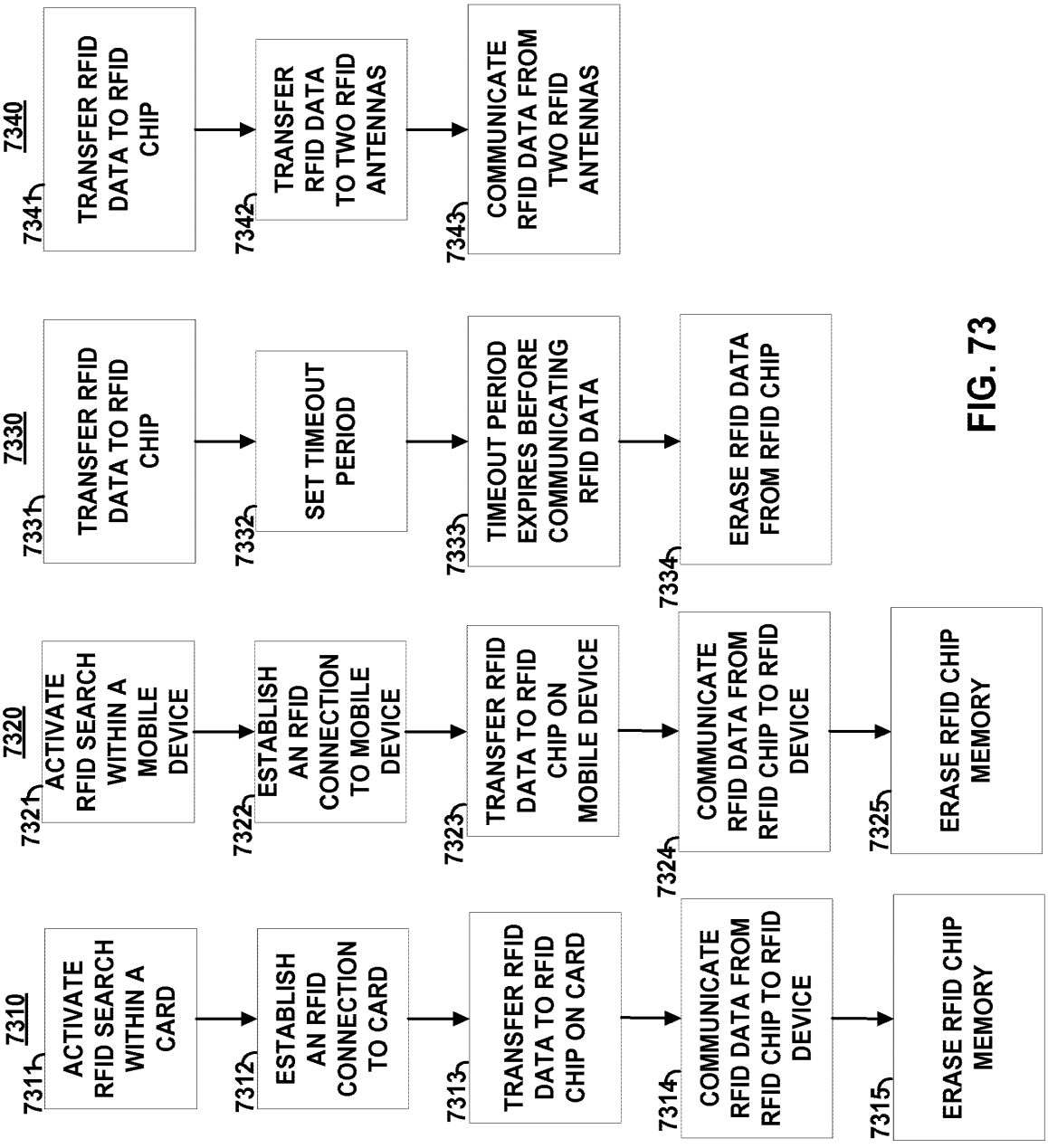

7310
7311
ACTIVATE RFID SEARCH WITHIN A CARD
7312
ESTABLISH AN RFID CONNECTION TO CARD
7313
TRANSFER RFID DATA TO RFID CHIP ON CARD
7314
COMMUNICATE RFID DATA FROM RFID CHIP TO RFID DEVICE
7315
ERASE RFID CHIP MEMORY
7320
7321
ACTIVATE RFID SEARCH WITHIN A MOBILE DEVICE
7322
ESTABLISH AN RFID CONNECTION TO MOBILE DEVICE
7323
TRANSFER RFID DATA TO RFID CHIP ON MOBILE DEVICE
7324
COMMUNICATE RFID DATA FROM RFID CHIP TO RFID DEVICE
7325
ERASE RFID CHIP MEMORY
7330
7331
TRANSFER RFID DATA TO RFID CHIP
7332
SET TIMEOUT PERIOD
7333
TIMEOUT PERIOD EXPIRES BEFORE COMMUNICATING RFID DATA
7334
ERASE RFID DATA FROM RFID CHIP
7340
7341
TRANSFER RFID DATA TO RFID CHIP
7342
TRANSFER RFID DATA TO TWO RFID ANTENNAS
7343
COMMUNICATE RFID DATA FROM TWO RFID ANTENNAS

FIG. 73

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/037237

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/02 (2012.01)
USPC - 705/41
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06Q 30/06, 40/00, 40/02 (2012.01)
USPC - 455/41.1, 705/39, 40, 41, 42

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Google Patents, Google.com

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/0210308 A1 (TOOMER et al) 20 August 2009 (20.08.2009) entire document	1, 3-11, 81
X	US 2009/0191811 A1 (GRIFFIN et al) 30 July 2009 (30.07.2009) entire document	2, 12-21, 82
A	US 2010/0304670 A1 (SHUO) 02 December 2010 (02.12.2010) entire document	1-21, 81-82
A	US 2010/0023449 A1 (SKOWRONEK et al) 28 January 2010 (28.01.2010) entire document	1-21, 81-82
A	US 2009/0170432 A1 (LORTZ) 02 July 2009 (02.07.2009) entire document	1-21, 81-82
A	US 2010/0153269 A1 (MCCABE) 17 June 2010 (17.06.2010) abstract, Fig. 1-2, paragraphs 13, 15, 30-31, 36-40, 47.	1-21, 81-82

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 September 2012	16 OCT 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/037237

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-21, 81-82

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

IPR2025-01150
Apple EX1071 Page 1079

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/037237

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-21, 81-82, drawn to a method and system comprising accessing a network using a mobile device, selecting an object for purchase from said network, communicating payment information/target account information to a second device, and completing a purchase transaction/coordinating a money transfer.
Group II, claims 22-41, 83, drawn to a method and system comprising creating a mobile wallet of virtual cards within a memory of a mobile device from communicated information, and selecting one of said virtual cards to complete a purchase transaction.
Group III, claims 42-61, 84, drawn to a method and system comprising executing an application on a processor of a mobile device to perform a function, communicating information to said mobile device, confirming said communicated information matches at least a portion of predetermined information, and executing said function from said mobile device based on said confirmation.
Group IV, claims 62-78, drawn to a card comprising a second board including a processor, wherein first data is transferred from a processor to a first RFID chip via conductive terminals between first and second boards and wherein said first data is communicated from said first RFID chip to a first RFID communication channel via said first RFID antenna.
Group V, claims 79-80, drawn to a method comprising communicating second data from a device to a reader via a second RFID communication channel, receiving first and second data via said reader and avoiding collisions between said first and second data within said reader.

The inventions listed as Groups I, II, III, IV and IV do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: a method and system comprising accessing a network using a mobile device, selecting an object for purchase from said network, communicating payment information/target account information to a second device as claimed therein is not present in the invention of Groups II, III, IV or V. The special technical feature of the Group II invention: a method and system comprising creating a mobile wallet of virtual cards within a memory of a mobile device from communicated information, and selecting one of said virtual cards as claimed therein is not present in the invention of Groups I, III, IV or V. The special technical feature of the Group III invention: a method and system comprising executing an application on a processor of a mobile device to perform a function, confirming that communicated information matches at least a portion of predetermined information, and executing said function from said mobile device based on said confirmation as claimed therein is not present in the invention of Groups I, II, IV or V. The special technical feature of the Group IV invention: a card comprising a second board including a processor, wherein first data is transferred from a processor to a first RFID chip via conductive terminals between first and second boards as claimed therein is not present in the invention of Groups I, II, III or V. The special technical feature of the Group V invention: a method comprising communicating second data from a device to a reader via a second RFID communication channel, receiving first and second data via said reader and avoiding collisions between said first and second data within said reader as claimed therein is not present in the invention of Groups I, II, III or IV.

Groups I, II, III, IV and V lack unity of invention because even though the inventions of these groups require the technical feature of a method, system and card comprising establishing a contactless communication channel between a physical card and a mobile device through a first board including a first RFID chip and a first RFID antenna; communicating payment/source account information from a payment card to a mobile device using a contactless communication channel wherein first data is communicated from said first RFID chip to a first RFID communication channel visa said first RFID antenna; completing a purchase transaction/coordinating a money transfer, this technical feature is not a special technical feature as it does not make a contribution over the prior art in view of US 2010/0153269 A1 (MCCABE) 17 June 2010 (17.06.2010), abstract, Fig. 1-2, paragraphs 13, 15, 30-31, 36-40, 47.

Since none of the special technical features of the Group I, II, III, IV or V inventions are found in more than one of the inventions, unity of invention is lacking.

IPR2025-01150
Apple EX1071 Page 1080

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 April 2010 (22.04.2010)

PCT

(10) International Publication Number
WO 2010/043974 A1

(51) International Patent Classification:
G06Q 20/00 (2006.01) *H04L 9/32* (2006.01)
G06K 7/10 (2006.01) *H04K 3/00* (2006.01)

(21) International Application Number:
PCT/IB2009/007364

(22) International Filing Date:
16 October 2009 (16.10.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/136,945 16 October 2008 (16.10.2008) US

(72) Inventor; and
(71) Applicant : **RICHARD, Christian** [CA/CA]; 187 Dieppe, Pointe Claire, Quebec, H9R 1X8 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,

[Continued on next page]

(54) **Title**: SYSTEM FOR SECURE CONTACTLESS PAYMENT TRANSACTIONS

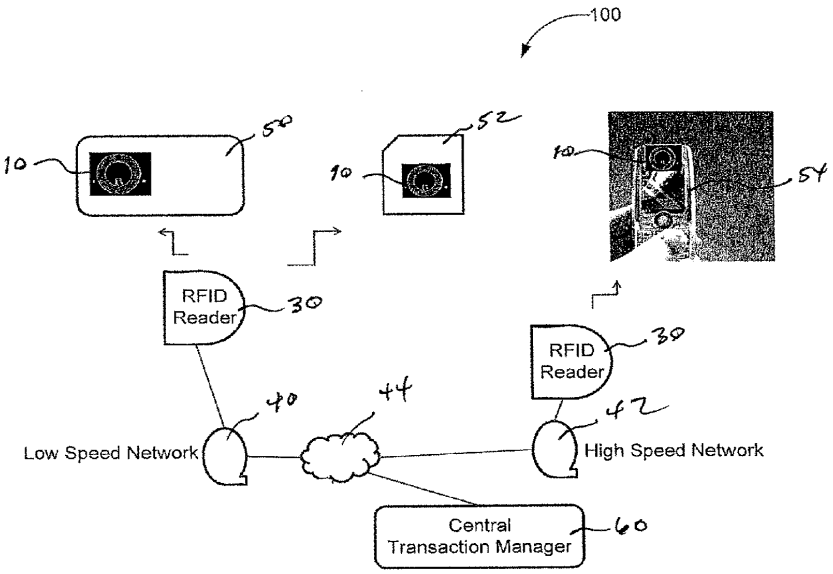


Figure 1

[Continued on next page]

WO 2010/043974 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(57) Abstract: The present invention is directed to a system that includes a transaction unit that includes a microchip having a computer readable medium configured to store a unit identifier (UI) and at least one one-time-password (OTP) therein. The UI and the at least one OTP comprising transaction authentication data. The transaction unit is configured to transmit the transaction authentication data in response to receiving a predetermined signal. A reader device is configured to transmit the predetermined signal to interrogate the transaction unit and read the transaction authentication data. The reader device is configured to generate at least one authentication indicia in response to receiving an authentication signal. A server is coupled to the reader device. The server includes a database having at least one server OTP related to at least one unit identifier stored therein, the at least one server OTP and the at least one unit identifier comprising transaction verification data. The server is configured to compare the transaction authentication data with the transaction verification data. The server also is configured to transmit the authentication signal to the reader device if the transaction authentication data matches the transaction verification data.

SYSTEM FOR SECURE CONTACTLESS PAYMENT TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of priority under 35 U.S.C. §119(e) and 35 U.S.C. §365, to U.S. Provisional Patent Application Serial No. 61/136,945, filed on October 16, 2008, the content of which is relied upon and incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0002] The present invention relates generally to RFID systems, and particularly to a method and system for secure contactless payment transactions.

2. Technical Background

[0003] Contactless "smartcards" have been used for payment for many years. Smartcards and other such contactless payment schemes were originally promoted for use in a category of payment defined as micropayment. The smartcard typically included an RFID chip disposed therein. The RFID chip included memory for storing the payment information. The payment information was accessed by a reader. Micropayment was originally created for the purchase of products under a given price, e.g., $50, without any receipt. Micropayment was originally contemplated as a means for simplifying payment for small items such as newspapers, fast food and other similar purchases. The card may, for example, be issued by a merchant and include a $50 credit amount recorded in memory.

[0004] In another example, Paypass ™ is a smart credit card system adopted by various credit card companies. In fact, approximately 80 million credit cards with a contactless inlay using the ISO 14443A or B protocols were released into the stream of commerce. When the credit card is read through its RFID chip, the information that is transmitted to the bank is the same as the standard credit card track A and B data. The

IPR2025-01150
Apple EX1071 Page 1083

system attempted to protect the sensitive financial data using the Texas Instruments ™ Digital Signal Transponder (DST) 24 to 40 bits protocol. One drawback with this method is that is vulnerable to "sniffing" attacks. *Sniffing* refers to a technique wherein a thief surreptitiously captures the transmissions between the smart card and the reader. This may be accomplished, for example, by hiding an unauthorized read in close proximity to the authorized reader. This technique often resulted in the fraudulent acquisition of many credit card numbers in a short span of time. For example, it was widely reported that one hacker was able to sniff thousands of credit cards using the contactless payment system over a span of a few hours using a $150 device.

[0005] What is needed, therefore, is a system for improving the security of contactless payment transactions.

SUMMARY OF THE INVENTION

[0006] The present invention addresses the needs described above by providing a system for improving the security of contactless payment transactions.

[0007] One aspect of the present invention is directed to a system that includes a transaction unit having a microchip that includes a computer readable medium. The computer readable medium is configured to store a unit identifier (UI) and at least one one-time-password (OTP) therein. The UI and the at least one OTP comprising transaction authentication data. The transaction unit is configured to transmit the transaction authentication data in response to receiving a predetermined signal. A reader device is configured to transmit the predetermined signal to interrogate the transaction unit and read the transaction authentication data. The reader device is configured to generate at least one authentication indicia in response to receiving an authentication signal. A server is coupled to the reader device. The server includes a database having at least one server OTP related to at least one unit identifier stored therein, the at least one server OTP and the at least one unit identifier comprising transaction verification data. The server is configured to compare the transaction authentication data with the transaction verification data. The server also is configured

IPR2025-01150
Apple EX1071 Page 1084

to transmit the authentication signal to the reader device if the transaction authentication data matches the transaction verification data.

[0008] Another aspect of the present invention is directed to a system that includes a contactless transaction unit having an RFID assembly disposed therein. The RFID assembly includes an RFID coupler and a microchip having a computer readable medium configured to store transaction authentication data. The RFID coupler includes a detuned inlay, the detuned inlay including an LC circuit having a resonant frequency calculated to correspond to a sub-harmonic of the main frequency of a predetermined signal. The transaction unit is configured to transmit the transaction authentication data in response to receiving the predetermined signal. A contactless RFID reader device is configured to transmit the predetermined signal when the transaction unit is disposed within a predetermined distance from the reader device to thereby interrogate the contactless transaction unit and read the transaction authentication data. The contactless RFID reader device is configured to generate at least one authentication indicia in response to receiving an authentication signal. A server is coupled to the contactless RFID reader device. The server includes a database having transaction verification data stored therein. The server is configured to compare the transaction authentication data with the transaction verification data. The server is configured to transmit the authentication signal to the contactless RFID reader device if the transaction authentication data matches the transaction verification data.

[0009] Yet another aspect of the present invention is directed to a system that includes a transaction unit having an RFID assembly disposed therein. The RFID assembly includes an RFID coupler and a microchip having a computer readable medium. The computer readable medium is configured to store transaction authentication data. The transaction unit is also configured to transmit the transaction authentication data in response to receiving the predetermined signal. An RFID reader device is configured to transmit the predetermined signal when the transaction unit is disposed within a predetermined distance from the RFID reader device to thereby interrogate the transaction unit and read the transaction authentication data. The RFID reader includes a jammer coupler disposed proximate a reader coupler such that the

IPR2025-01150
Apple EX1071 Page 1085

RFID reader device includes a sensing zone wherein the RFID reader device interrogates the transaction unit and a jamming zone wherein the RFID reader device transmits a jamming signal substantially outside of the sensing zone. The RFID reader device is also configured to generate at least one authentication indicia in response to receiving an authentication signal. A server is coupled to the RFID reader device, the server including a database having transaction verification data stored therein. The server is configured to compare the transaction authentication data with the transaction verification data. The server is configured to transmit the authentication signal to the RFID reader device if the transaction authentication data matches the transaction verification data.

[0010] Additional features and advantages of the invention will be set forth in the detailed description which follows, and in part will be readily apparent to those skilled in the art from that description or recognized by practicing the invention as described herein, including the detailed description which follows, the claims, as well as the appended drawings.

[0011] It is to be understood that both the foregoing general description and the following detailed description are merely exemplary of the invention, and are intended to provide an overview or framework for understanding the nature and character of the invention as it is claimed. The accompanying drawings are included to provide a further understanding of the invention, and are incorporated in and constitute a part of this specification. The drawings illustrate various embodiments of the invention, and together with the description serve to explain the principles and operation of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 is a block diagram of a secure contactless payment transaction according to an embodiment of the present invention

[0013] Figure 2 is a schematic view of a contactless payment card inlay;

[0014] Figure 3 is an example of a second harmonic of a signal having a main frequency of 13.56 MHz;

IPR2025-01150
Apple EX1071 Page 1086

[0015] Figure 4 is a schematic view of a reader coupler with a concentric jammer; and

[0016] Figures 5A and 5B are schematic views of the reader coupler field and the reader coupler field combined with the concentric jammer field, respectively.

DETAILED DESCRIPTION

[0017] Reference will now be made in detail to the present exemplary embodiments of the invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts. An exemplary embodiment of the system of the present invention is shown in Figure 1, and is designated generally throughout by reference numeral 100.

[0018] As embodied herein, and depicted in Figure 1, a diagrammatic depiction of a secure contactless payment transaction system 100 in accordance with one embodiment of the present invention is disclosed. System 100 may be configured as a hierarchical computer and software system implemented in the well known client-server model with at least one secure database for storing secure data. System 100 may include a server 60, middle layer computer processing nodes associated with the networks 40, 42 and RFID readers 30 at the lowest level. System 100 may also include an RFID card 50, an RFID token 52 and/or an RFID equipped electronic devices 54, e.g., a mobile near field communications (NFC) device 54. Each of these devices may be read by an RFID reader 30 in accordance with the present invention. These devices are coupled to a central transaction management server 60 by way of low speed network 40, high speed network 42, switched network 44, or some combination thereof. Secure data may include cytological keys used to authenticate computer processing nodes and sensors in the network. Of course, one-time passwords (OTPs) are used to authenticate and verify RFID cards 50, tokens 52 and NFC devices 54.

[0019] The switched network 44 may include the public switched telephony network (PSTN) or a packet switched network or a combination thereof. Network 44 may be, for example, the global packet data communication network now commonly

IPR2025-01150
Apple EX1071 Page 1087

referred to as the "Internet." The World Wide Web (WWW) is a system of server computers that is supported and interconnected by the Internet. In the client-server model, the server computer(s) comprising the transaction manager server 60 may provide graphical "web pages" that are provided to a client computers that supports a given RFID reader 30 via the web. The client computer includes a graphical interface which provides an easily understood display that facilitates the POS transaction. Some of the information being served to the client is dynamically retrieved by the server from one or more databases. The graphical interface may allow the sales personnel to perform an identity check of the customer. The identification information may be provided to server along with the OTP data obtained by reader 30.

[0020] In one embodiment of the present invention, RFID reader 30 includes a secure contactless sensor that employs a 13.56 MHz microcircuit. The 13.56 MHz microcircuit is bidirectional and is characterized by a controllable range. Reader 30, therefore, exchanges data with the RFID device (50, 52, 54) at a reasonable speed. Reader 30 may be configured as a low power reader that employs the ISO 14443A protocol. Contactless payment cards are easily read at a range of 12 inches (30.48 cm). This range can be extended up to 3 feet (91.44 cm) when equipped with larger sensors. The RFID reader 30, depending on its sophistication at the point of sale (POS), may be include application programming configured to interact with POS personnel. The application programming may provide access to information retained in the Server databases and also to provide control over the RFID reader 30.

[0021] RFID reader 30 also includes a network interface to couple RFID reader 30 to external computer networks 40, 42, and/or 44. The communication interface may be of any suitable type such as a Universal Serial Bus (USB) interface, cable modem, a digital subscriber line (DSL) card or modem, an integrated services digital network (ISDN) card, a telephone modem, or any other communication interface to provide a data communication connection to a corresponding type of communication line. As another example, communication interface may be a local area network (LAN) or wide area network (WAN) card (e.g. for Ethernet™ or an Asynchronous Transfer Model (ATM) network) to provide a data communication connection to a compatible LAN or

IPR2025-01150
Apple EX1071 Page 1088

WAN. Wireless links can also be implemented. In any such implementation, communication interface may send or receive electrical, electromagnetic, or optical signals that carry digital data streams representing various types of information.

[0022] The term "computer-readable medium" as used herein refers to any medium that participates in providing data and/or instructions to a processor associated with either the RFID reader 30 or the transaction manager server 60 for execution. Such media may take many forms, including but not limited to non-volatile media, volatile media, and transmission media. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, CDRW, DVD, any other optical medium, punch cards, paper tape, optical mark sheets, any other physical medium with patterns of holes or other optically recognizable indicia, a RAM, a PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave, or any other medium from which a computer can read. Transmission media may include coaxial cables, copper wire and/or optical fiber. Transmission media can also take the form of acoustic, optical, or electromagnetic waves, such as those generated during radio frequency (RF) and infrared (IR) data communications. Any of the various forms of computer-readable media described above may be involved in providing instructions to the table computers 210 for execution.

[0023] The transaction manager server 60 refers to both the physical server computers configured to run and manage the various system applications, and the software that resides on the physical server computers. The server manages the proper reading and writing of data in the database. The server also manages the contactless payment sequence enabled by the RFID card 50. The server stores, receives and dispatches alarms over the networks to the clients in the event that an authentication fails.

[0024] One of the drawbacks associated with conventional smartcard systems relates to the use of customer tracking information during the data exchange. It is understood that the use of this data reduces the burden on the merchant by requiring

IPR2025-01150
Apple EX1071 Page 1089

fewer changes to current conventional systems. However, this design makes it very easy and very attractive for thieves to hack these relatively unprotected smart cards.

[0025] The transaction manager server 60 may be configured to generate the one-time pass word and read/write to/from the database using symmetric security keys. The new OTP is written into the chip by the OTP module via the server. Client/server communications may be encrypted using a secure sockets layer (SSL). As will be explained in detail below, the OTP is a security system that changes a secret data key inside the RFID card 50 each time it is read. If the server validates the retrieved OTP, the transaction is written into the database, and a new OTP is retrieved in accordance with a predetermined sequence.

[0026] To generate the one-time password (OTP), a "seed" is provided by the transaction manager server 60 or by an authorized card issuing authority. The seed is combined with a static user password and a user card ID using a hash function. The hash value of the user's static password the session one-time password and the compressed data is used as input to the digital signature algorithm. This guarantees that the one-time password significantly determines the communication stream between the client and the server for each session. The transaction manager server 60 or the authorized card issuing authority computes a set S of independent one-time passwords that are stored in a password file in a database coupled to the transaction manager server 60.

[0027] The RFID card 50, token 52 or NFC device 54 stores the initial one time password word together with the corresponding index. In one embodiment, either the entire set (S) or a small subset (S') of S is stored on the card 50 before issuance in a secure way. At login time, upon presentation of the RFID tag, the transaction server issues a challenge to the tag. The challenge is merely one of the indices selected at random. Of course, the selected index is used by the card to retrieve the one-time password out of the subset S' of one-time passwords that corresponds to the selected index. Once retrieved, the RFID card (50, 52, 54) sends the one-time password stored in memory that corresponds to the challenge I, in response to the challenge. If this one-time password transmitted by the card matches the one stored in the password file at

IPR2025-01150
Apple EX1071 Page 1090

index i, the transaction is authorized. If not, the authentication fails. This approach is not vulnerable to over-the-shoulder attacks since the passwords are stored in the RFID tag. Further, since the one-time passwords are selected at random and the subset S' can be chosen to be small enough to allow frequent refresh of the passwords stored in the RFID tag, a passive eavesdropper that monitors the communication between the RFID tag and the central controller will not be able to predict the next one-time password that the card will send.

[0028] In another embodiment, card 50, token 52 or device 54 is equipped with computing power, and the initial OTP is employed to generate additional passwords by applying a series of iterations of the cryptographic functions f to the initial OTP. In one embodiment, the memory of the contactless payment card would include a 64 bit permanent unique identifier (UIO) and at least one 16 to 63 bit one-time password (OTP) in the read/write memory using a fast encryption algorithm based on, for example, an exponential *Certicom* keying system. The memory would also include a class of service bits and optional challenge complement bits. In order to authenticate to the system, the user applies an iteration of the cryptographic function (f) to the initial OTP. The encrypted information is transmitted to the server 60 via the reader 30. The server 60 verifies the correctness of the information by decoding the encrypted data provided by the RFID card 50, token 52 or device 54. The decoded result is compared to the value previously stored in the server 60. If there is a match, authentication succeeds and the new value of i together with the next iteration of the cryptographic function (f) are stored in the controller. Otherwise, authentication fails and the value of i is discarded.

[0029] In both implementations, the one-time password can be used to secure subsequent communications between the client and the transaction manager server 60. The user password is never transmitted in plain text to the central controller. A slight modification of this approach allows also for server authentication to the client card 50, token 52 or NFC device 54. The set of one-time passwords computed by the client or the server can be either based on Elliptic Curves or on the RSA scheme or on any other pseudo random function.

IPR2025-01150
Apple EX1071 Page 1091

[0030] The present invention envisions several classes of OTP service. The first class (Class 1 OTP) is referred to as close loop fast access. In this embodiment, an OTP server is on site and it facilitates a full OTP exchange. In other words, if the RFID card 50 includes one OTP, the server may cryptographically generate a new OTP and write it into the inlay 10 memory. This approach requires a relatively high speed central server to be efficient. Thus, this approach is particularly efficient in environments such as shopping centers, airports and subways in which the speed of the connection to a central server is not a issue. The second class (Class 2 OTP) is referred to as fast access OTP. In this embodiment, an OTP server may be easily accessible but is not required for every transaction. The third class of service (Class 3 OTP) does not have immediate access to the transaction manager server 60 and relies on the hand shaking key to secure the transaction. It is envisioned that Class 3 OTP would be employed in remote locations. The "hand shaking sequence" would require the reader 30 to have a key to access the data in the RFID card (50, 52, 54), based on the specific time of the transaction. Thus, only an authorized reader can read the RFID card 50, token 52 or NFC device 54 based on the authentication process described. To complement the transaction, human interaction may be required to complete the secure transaction, for example a cashier asking for a picture identification.

[0031] Accordingly, the present system eliminates the drawbacks associated with existing contactless payment systems whereby the RFID microchip can be read at a distance by an unauthorized sensor. Further, an unauthorized sensor placed within or underneath a counter, or within a doorway gate cannot be used to illegally read the data in the RFID card (50, 52, 54) of the present invention. For example, recently conducted tests showed that on low power reader using the ISO 14443A protocol can easily read conventional contactless payment cards at a range of 12 inches (30.48 cm). As noted, this range can be up to 3 feet (91.44 cm) with larger sensors. The OTP of the present invention eliminates this threat. As another example, the 40 bit key used in certain conventional cards has been broken and made public on the Internet. In fact, a group of students from the University of Baltimore, and sponsored by RSA, showed that a

IPR2025-01150
Apple EX1071 Page 1092

particular algorithm could be broken in a few minutes. Again, the OTP of the present invention eliminates this threat.

[0032] One benefit of the present invention relates to the use of a 13.56 MHz RFID reader 30 that is based on the ISO 14443 protocol. Most payment or secure transaction contactless systems commonly use the 13.56 MHz reader. The ISO 14443 protocol (or its ISO 18000 equivalent) was created for secured RF transaction at 13.56 MHz. Thus, the present invention presents certain advantages vis á vis certain conventional systems such as conventional systems employing 125 KHz tokens. At a 6 Kbits/sec throughput, these tokens do not provide for bidirectional exchanges of data at a sufficient speed. There are higher frequency range systems but they also suffer from various deficiencies. For example, the Wall Mart ™ EPC 915 MHz system and the upcoming 915 MHz from EM Marin do not include enough memory capacity. Another issue in the 915 MHz frequency systems relates to the relative inability to control the range and the cross talk. In view of these drawbacks, many security experts prefer the 13.56 MHz system as the frequency of choice for secure applications.

[0033] As noted above, the present invention includes RFID equipped electronic devices 54, such as those configured in accordance with *near field communications* (NFC) technologies. Those of ordinary skill in the art will understand that NFC employs short-range high frequency wireless communication technology for contactless bidirectional transmission of data between devices separated by approximately 10 centimeters, which is about 4 inches. NFC may be thought of as an application or extension of the ISO/IEC 14443 RFID proximity-card standard (described above) in that it incorporates a so-called smart card into a hand held electronic device. NFC is primarily aimed at usage in mobile phones and may be employed in *blackberries* and other such devices. NFC may also combine the interface of a smartcard and a reader into a single device. An NFC device of this type can, therefore, communicate with both existing ISO/IEC 14443 smartcards and readers, as well as with other NFC devices. One of the benefits of NFC devices is that they are compatible with existing contactless infrastructure already in use for public transportation and payment. For example, NFC devices communicate by way of magnetic field induction over the globally available

IPR2025-01150
Apple EX1071 Page 1093

and unlicensed RF-ISM band of 13.56 MHz, with a bandwidth of 14 kHz. As alluded to above, the RFID devices (50, 52, 54) may operate in a passive mode or in an active mode. In the passive RFID mode the RFID reader 30 provides a near magnetic field to interrogate the RFID Device (50, 52, 54). The RFID Device (50, 52, 54) typically employs an LC circuit that is excited by the near field such that the RFID device obtains its operating power from the near field. In the active mode, both the RFID device (50, 52, 54) and the reader 30 communicate by generate their own near field to transmit and deactivate their near field during the receive portion of the communication cycle. As noted above, the RFID device (50, 52, 54) requires a power supply to operate in this mode. Thus, the NFC RFID device 54 is well suited for this application.

[0034] It should be noted that conventional NFC devices may employ the ISO 14443 standard or newer 13.56 MHz implementations, e.g., the SONY™ FELICA™ system. There may be other private protocols being used in the U.S. Each of these protocols recognize the benefits of attaching a NFC chip to a mobile device. Cell phones are ubiquitous and one so equipped would essentially function as an electronic wallet, or an "*e-wallet*." However, the conventional devices briefly described above have drawbacks because the "sniffing" problem remains. Further, the "near field" is not specifically defined. As a matter of fact, this umbrella specification makes it very difficult for RFID chip makers because of the various protocols (e.g., NFC, ISO 14443 and ISO 15693) that must be supported in the same die. The sniffing issue is substantially eliminated by the present invention by use of the OTP, hardware range reduction and jamming of the chips beyond specific reading zone.

[0035] As embodied herein and depicted in Figure 2, a schematic view of a contactless payment card 10 is disclosed. In this embodiment, the inlay 10 is an LC circuit composed of the chip (microchip) and mainly its capacitance (C1) and the inductance (L_1) of the winding 12 attached to the die 14. This combination creates a resonant circuit resonating at a particular frequency. The basic ISO specification is very narrow at 13.56 MHz, +/- 500 KHz. This also applies to the NFC or any radio frequency (RF) payment system.

IPR2025-01150
Apple EX1071 Page 1094

[0036] An effective technique for providing a sorter reading range without affecting the data rate is to detune the inlay of the contactless payment card. To detune the inlay 10, the resonance frequency of the LC circuit is calculated on one of the secondary harmonics of the main frequency, namely:

$$F_{detuned} = 1/2\pi \sqrt{L_1 C_1}. \qquad \text{(Equation 1)}$$

[0037] As previously discussed, controlling the range at which contactless payment cards may be read is one of the features of the present invention that eliminates the sniffing problem. As noted, the operating frequency of the device may be in the HF RFID band at 13.56 MHz, employing inductive coupling to communicate with the RFID reader 30. RFID inlay 10 may include a read/write memory of at least 500 bits. In another embodiment, the memory size is about 2 K bits.

[0038] Referring to Figure 3, an example of a near field signal 20 in accordance with the present invention is depicted. Note that signal 20 includes a second harmonic 22 that has a main frequency of 13.56 Mhz. By detuning the inlay 10 in accordance with Equation 1, only the secondary harmonic will be used in the near field RFID communications between the RFID device (50, 52, 54) and the RFID reader 30. This drastically reduces the range of the reader 30 because only a fraction of the power is transmitted to the LC circuit in RFID card inlay 10. This range may be controlled with a relatively high precision at 13.56 MHz. One benefit of this technique is that is simple to realize. Only the inlay 10 must be detuned for the resultant RFID cards (50, 52, 54) to operate with existing readers. If the OTP is employed in conjunction with the range reduction features described immediately above, the probability of sniffing being an issue is quite low.

[0039] If the present invention is employed in higher frequency range systems (e.g., at 915 MHz or Wi-Fi), the RFID reader 30 may require redesign. Further, the OTP would be required. Another technique that may be employed in high frequency systems employs a predetermined geometric configuration of RFID readers 30. The geometric arrangement of readers 30 provides a means for physically locating the RFID card (50,

IPR2025-01150
Apple EX1071 Page 1095

52, 54). If the RFID card (50, 52, 54) is deemed to be in an authorized location, the transaction is authorized to proceed.

[0040] As embodied herein and depicted in Figure 4, a schematic view of a reader coupler 30 with a concentric jammer is disclosed. In this embodiment, the RFID reader 30 includes a jammer coupler 32 disposed within a perimeter formed by the reader coupler 34. The jammer coupler 32 is shown slightly offset from the center of the reader coupler 34 to compensate for various factors, such as the presence of metal or other conductors, and to provide separation from the reader power input 36. Jamming is a technique whereby potential communications between the contactless RFID card (50, 52, 54) and an unauthorized reader disposed outside of the reading zone of an authorized reader 30 are disturbed and/or interrupted. This is implemented in accordance with the present invention by the jamming coupler 32 which is configured to generate white noise centered around 13.56 MHz. This technique substantially prevents sniffers or hackers from monitoring RFID signals within the reading zone of reader 30.

[0041] Figures 5A and 5B are schematic views of the reader coupler field and the reader coupler field combined with the concentric jammer field, respectively. In Figure 5A, a field 35 generated by the reader coupler 35 is depicted. Figure 5B shows the combination of the field 35 generated by the reader coupler 34 and the field 33 generated by the jammer coupler 32. Figure 5B, therefore, illustrates the coverage of the jammer coupler field 33 relative to the reading zone of RFID reader 30. For example, a reader coupler 34 with a diameter of 6" will have a range of approximately 8.5". If the RFID reader 30 employs a jammer coupler 32 having a diameter of about 70% of that of the reader coupler 34, i.e. 4.2", reader 30 will have a range of about 6".

[0042] The above described techniques may be applied individually or collectively to contactless payment transaction systems in order to enhance the security of such transactions. These techniques may also be applied to any wireless transactions but particularly to payment transactions such as the NFC token system used in cellular phones. As for the OTP technique, it may also be applied to contact payment card

IPR2025-01150
Apple EX1071 Page 1096

systems or to other type of transaction system such as M-commerce, ticket purchase or payment at video terminals.

[0043] All references, including publications, patent applications, and patents, cited herein are hereby incorporated by reference to the same extent as if each reference were individually and specifically indicated to be incorporated by reference and were set forth in its entirety herein.

[0044] The use of the terms "a" and "an" and "the" and similar referents in the context of describing the invention (especially in the context of the following claims) are to be construed to cover both the singular and the plural, unless otherwise indicated herein or clearly contradicted by context. The terms "comprising," "having," "including," and "containing" are to be construed as open-ended terms (i.e., meaning "including, but not limited to,") unless otherwise noted. The term "connected" is to be construed as partly or wholly contained within, attached to, or joined together, even if there is something intervening.

[0045] The recitation of ranges of values herein are merely intended to serve as a shorthand method of referring individually to each separate value falling within the range, unless otherwise indicated herein, and each separate value is incorporated into the specification as if it were individually recited herein.

[0046] All methods described herein can be performed in any suitable order unless otherwise indicated herein or otherwise clearly contradicted by context. The use of any and all examples, or exemplary language (e.g., "such as") provided herein, is intended merely to better illuminate embodiments of the invention and does not impose a limitation on the scope of the invention unless otherwise claimed.

[0047] No language in the specification should be construed as indicating any non-claimed element as essential to the practice of the invention.

[0048] It will be apparent to those skilled in the art that various modifications and variations can be made to the present invention without departing from the spirit and scope of the invention. There is no intention to limit the invention to the specific form or forms disclosed, but on the contrary, the intention is to cover all modifications, alternative constructions, and equivalents falling within the spirit and scope of the

IPR2025-01150
Apple EX1071 Page 1097

invention, as defined in the appended claims. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

IPR2025-01150
Apple EX1071 Page 1098

What is claimed is:

1. A system comprising:

a transaction unit including a microchip having a computer readable medium configured to store a unit identifier (UI) and at least one one-time-password (OTP) therein, the UI and the at least one OTP comprising transaction authentication data, the transaction unit being configured to transmit the transaction authentication data in response to receiving a predetermined signal;

a reader device configured to transmit the predetermined signal to interrogate the transaction unit and read the transaction authentication data, the reader device being configured to generate at least one authentication indicia in response to receiving an authentication signal; and

a server coupled to the reader device, the server including a database having at least one server OTP related to at least one unit identifier stored therein, at least one server OTP and the at least one unit identifier comprising transaction verification data, the server being configured to compare the transaction authentication data with the transaction verification data, the server being configured to transmit the authentication signal to the reader device if the transaction authentication data matches the transaction verification data.

2. The system of claim 1, wherein transaction unit includes an RFID assembly disposed therein, the RFID assembly including an RFID coupler configured to operate at a predetermined frequency, and wherein the reader device is configured as an RFID reader operating at the predetermined frequency.

3. The system of claim 2, wherein the transaction unit is configured as a card, a token or as a mobile communications device.

IPR2025-01150
Apple EX1071 Page 1099

4. The system of claim 3, wherein the mobile communications device includes a graphical user interface (GUI) coupled to at least one microprocessor, the mobile communications device being configured to transmit the transaction authentication data to the server via at least one network by manipulating the GUI.

5. The system of claim 2, wherein the contactless RFID reader includes a jammer coupler disposed proximate a reader coupler such that the RFID reader includes a sensing zone wherein the RFID reader interrogates the contactless payment unit and a jamming zone wherein the RFID reader transmits a jamming signal substantially outside of the sensing zone.

6. The system of claim 1, wherein the predetermined signal is carried by a near field magnetic field, and wherein the RFID coupler includes a detuned inlay, the detuned inlay including an LC circuit having a resonant frequency calculated to correspond to a sub-harmonic of the main frequency of the predetermined signal such that the predetermined distance is less than or equal to approximately eight (8) inches.

7. The system of claim 1, wherein the transaction unit and the reader device are configured to communicate at a frequency substantially equal to 13.56 MHz in accordance with an ISO 14443 standard.

8. The system of claim 1, wherein the transaction authentication data includes timing authentication data and the transaction verification data includes timing verification data.

9. The system of claim 1, wherein the at least one authentication indicia includes a visual indicator or an aural indicator, the visual indicator including an LED indicator configured to provide a color coded response indicative of authentication or authentication denial, or wherein the visual indicator is transmitted by way of a graphical user interface coupled to the RFID reader.

IPR2025-01150
Apple EX1071 Page 1100

10. The system of claim 1, wherein the server is configured to generate the at least one OTP using a predetermined encryption algorithm, the predetermined encryption algorithm is selected from a group of methods that include an Elliptical Curve Cryptography (ECC) encryption method, an Advanced Encryption Standard (AES) encryption method, a Temporal Key Integrity Protocol (TKIP) method, or a Counter-Mode/CBC-Mac protocol (CCMP) method.

11. The system of claim 1, wherein the at least one OTP includes a plurality of one time passwords, each one time password of the plurality of one time passwords being associated with a corresponding index number, and wherein the computer readable medium is configured as a first in first out memory that is configured to store either the plurality of one time passwords or a subset of the plurality of one time passwords.

12. A system comprising:

a contactless transaction unit including an RFID assembly disposed therein, the RFID assembly including an RFID coupler and a microchip having a computer readable medium configured to store transaction authentication data, the RFID coupler including a detuned inlay, the detuned inlay including an LC circuit having a resonant frequency calculated to correspond to a sub-harmonic of the main frequency of a predetermined signal, the transaction unit being configured to transmit the transaction authentication data in response to receiving the predetermined signal;

a contactless RFID reader device configured to transmit the predetermined signal when the transaction unit is disposed within a predetermined distance from the reader device to thereby interrogate the contactless transaction unit and read the transaction authentication data, the contactless RFID reader device being configured to generate at least one authentication indicia in response to receiving an authentication signal; and

IPR2025-01150
Apple EX1071 Page 1101

a server coupled to the contactless RFID reader device, the server including a database having transaction verification data stored therein, the server being configured to compare the transaction authentication data with the transaction verification data, the server being configured to transmit the authentication signal to the contactless RFID reader device if the transaction authentication data matches the transaction verification data.

13. The system of claim 12, wherein the computer readable medium is configured to store a unit identifier (UI) and at least one one-time-password (OTP) therein, the UI and the at least one OTP comprising the transaction authentication data.

14. The system of claim 12, wherein the transaction verification data comprises at least one server OTP related to at least one unit identifier.

15. The system of claim 12, wherein the contactless RFID reader includes a jammer coupler disposed proximate a reader coupler such that the RFID reader includes a sensing zone wherein the RFID reader interrogates the contactless payment unit and a jamming zone wherein the RFID reader transmits a jamming signal substantially outside of the sensing zone.

16. The system of claim 12, wherein the predetermined distance is less than or equal to approximately eight (8) inches.

17. A system comprising:

a transaction unit including an RFID assembly disposed therein, the RFID assembly including an RFID coupler and a microchip having a computer readable medium configured to store transaction authentication data, the transaction unit being configured to transmit the transaction authentication data in response to receiving the predetermined signal;

IPR2025-01150
Apple EX1071 Page 1102

an RFID reader device configured to transmit the predetermined signal when the transaction unit is disposed within a predetermined distance from the RFID reader device to thereby interrogate the transaction unit and read the transaction authentication data, the RFID reader includes a jammer coupler disposed proximate a reader coupler such that the RFID reader device includes a sensing zone wherein the RFID reader device interrogates the transaction unit and a jamming zone wherein the RFID reader device transmits a jamming signal substantially outside of the sensing zone, the RFID reader device being configured to generate at least one authentication indicia in response to receiving an authentication signal; and

a server coupled to the RFID reader device, the server including a database having transaction verification data stored therein, the server being configured to compare the transaction authentication data with the transaction verification data, the server being configured to transmit the authentication signal to the RFID reader device if the transaction authentication data matches the transaction verification data.

18. The system of claim 17, wherein the RFID coupler includes a detuned inlay, the detuned inlay including an LC circuit having a resonant frequency calculated to correspond to a sub-harmonic of the main frequency of the predetermined signal.

19. The system of claim 17, wherein the predetermined distance is less than or equal to approximately eight (8) inches.

20. The system of claim 17, wherein the computer readable medium is configured to store a unit identifier (UI) and at least one one-time-password (OTP) therein, the UI and the at least one OTP comprising the transaction authentication data, and wherein the transaction verification data is comprised of at least one server OTP related to at least one unit identifier.

IPR2025-01150
Apple EX1071 Page 1103

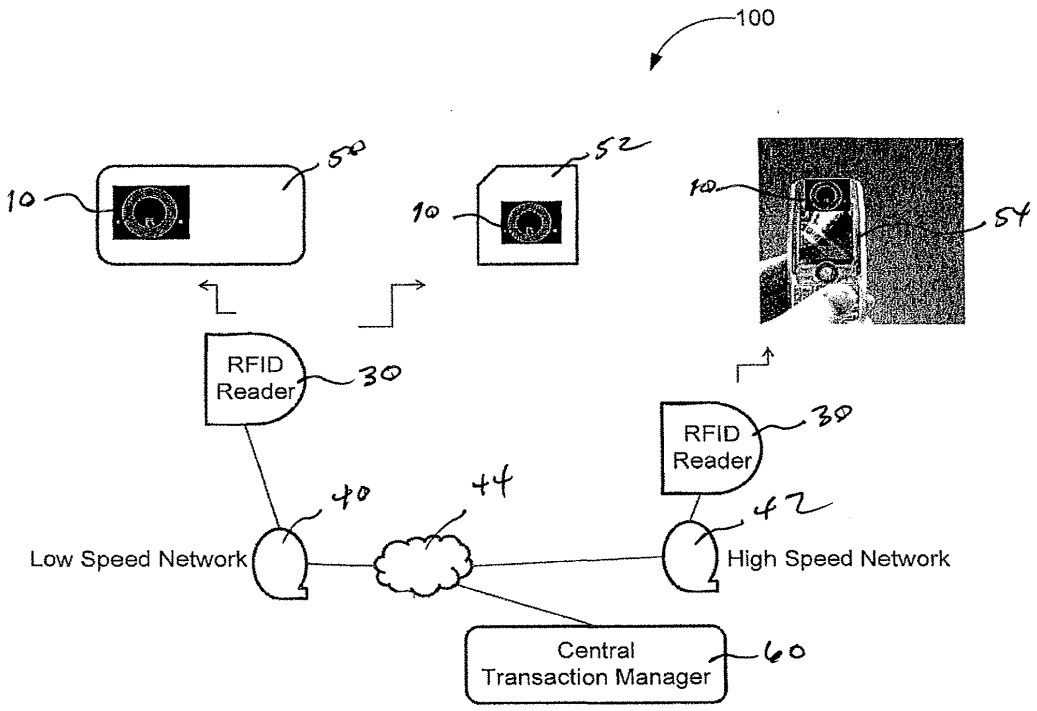

100
10
50
10
52
10
54
RFID Reader
30
RFID Reader
30
40
44
42
Low Speed Network
High Speed Network
Central Transaction Manager
60

Figure 1

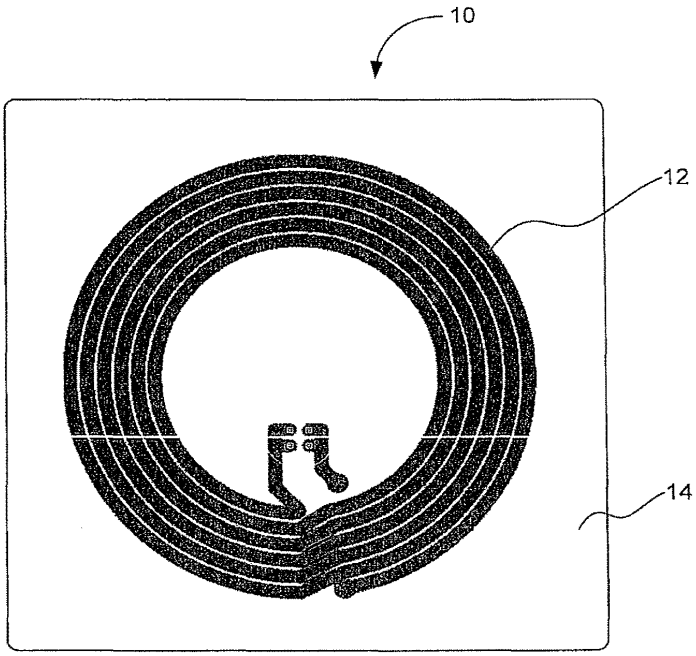


Figure 2

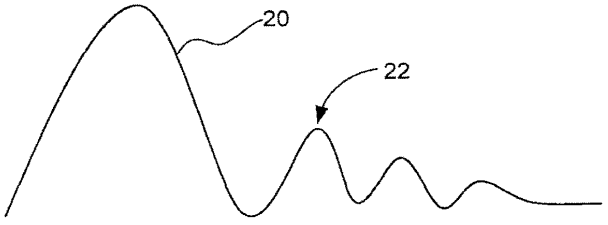


Figure 3

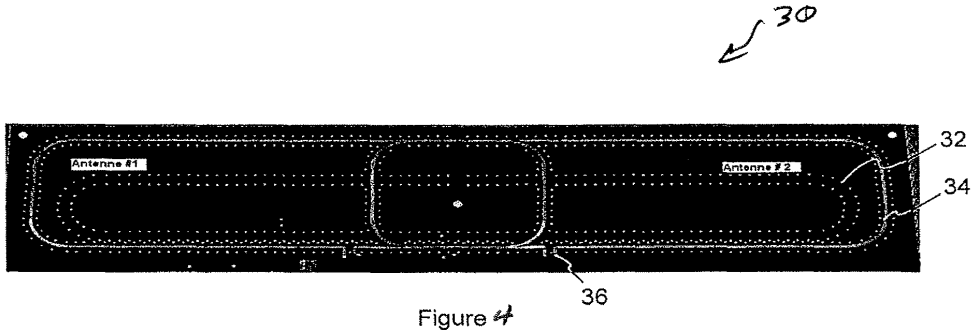


Figure 4

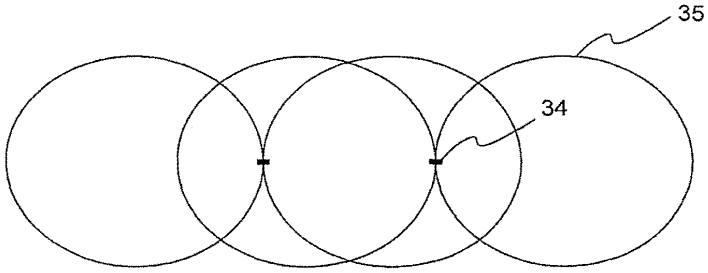


Figure 5A

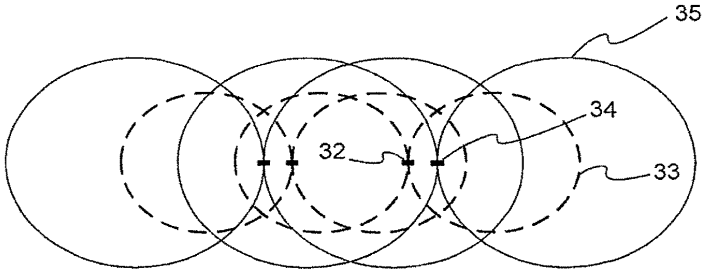


Figure 5B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2009/007364

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***G06Q 20/00*** (2006.01) , ***G06K 7/10*** (2006.01) , ***H04L 9/32*** (2006.01) , ***H04K 3/00*** (2006.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC: ***G06Q*** (2006.01) , ***G06F*** (2006.01), ***G06K*** (2006.01), ***H04B*** (2006.01), ***H04L*** (2006.01), ***H04Q*** (2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
EPOQUE, DELPHION, Canadian Patent Database, Google™, Google™ Scholar,
& keywords: RFID reader, one-time password*, authentication, jammer, LC, sub-harmonic* and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/037220 A1 (RICHARD, C.) 13 April 2006 (13-04-2006) * pages 1, 3, 4, 6, 8, 9 and 11 *	1 - 3, 10, 11
Y		4 - 9, 12 - 20
X	US 2007/0194889 A1 (BAILEY, D.V. et al.) 23 August 2007 (23-08-2007) * paragraphs [0030] to [0037], [0040] to [0047], [0053] to [0060] and [0075] *	1 - 3, 7
Y		4 - 6, 8 - 20
Y	US 2007/0194931 A1 (MILLER, R.N. et al.) 23 August 2007 (23-08-2007) * paragraphs [0012] to [0016] *	5, 15, 17 - 20
Y	US 2002/0140215 A1 (BREED, D.S.) 3 October 2002 (03-10-2002) * paragraph [0275] *	6, 12 - 16, 18
Y	US 2008/0014867 A1 (FINN, D.) 17 January 2008 (17-01-2008) * paragraphs [0018], [0057], [0058], [0063], [0082] to [0084] and [0095] *	6, 8, 9, 16, 19
A	* paragraphs [0118], [0145], [0146] and [0184] to [0185] *	1 - 5, 7, 10 - 18, 20

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

*	Special categories of cited documents :	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier application or patent but published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
25 February 2010 (25-02-2010)	4 March 2010 (04-03-2010)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Jennifer Guerra (819) 934-2628

IPR2025-01150
Apple EX1071 Page 1107

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2007/057786 A2 (FINN, D.) 24 May 2007 (24-05-2007) * pages 2, 8, 14, 15, 32, 37, 39, 43, 44, 46, 47, 48, 61, 62 and 67 *	4, 9
A	* pages 77 and 79 *	1 - 3, 5 - 8, 10 - 20
Y	WO 2005/125078 A1 (KAMENDJE, G) 29 December 2005 (29-12-2005) * pages 3 and 9 *	11
P, X	WO 2009/075434 A1 (CHOI, D.H.) 18 June 2009 * entire document *	1 - 3, 10
P, Y		4 - 9, 11 - 20
P, X	US 2009/0200371 A1 (KEAN, B.) 13 August 2009 (13-08-2009) * paragraphs [0009], [0012], [0017], [0055] and [0059] *	1 - 3
P, Y		4 - 20
P, Y	US 7,387,260 B1 (MACKENZIE, J.D.) 17 June 2008 (17-06-2008) * column 1, lines 56 to 65 and column 22, lines 57 to 62 *	6, 12, 18
P, Y	US 2009/0224058 A1 (SAVRY, O.) 10 September 2009 (10-09-2009) * paragraph [0032] *	6, 12, 18
A	WO 2007/123895 A2 (HALLAM-BAKER, P.M.) 1 November 2007 (01-11-2007) * paragraphs [0020] to [0039] and [0050] to [0067] *	1 - 20
A	US 2008/0238676 A1 (DHILLON, P.S. et al.) 2 October 2008 (02-10-2008) * paragraphs [0019] and [0025] *	1 - 20
A	WO 2007/149775 A2 (HAMMAD, A. et al.) 27 December 2007 (27-12-2007) * pages 2, 6 to 8, 12, 14, 20 and 21 *	1 - 20
A	WO 2007/073609 A1 (ROLLIER, A. et al.) 5 July 2007 (05-07-2007) * pages 3 to 5, 8, 9, 12 and 13 *	1 - 20

IPR2025-01150
Apple EX1071 Page 1108

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2009/007364

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
WO2006037220A1	13-04-2006	AU2005291797A1	13-04-2006
		CA2578983A1	13-04-2006
		CN101031940A	05-09-2007
		EP1805735A1	11-07-2007
		US2008214312A1	04-09-2008
US2007194889A1	23-08-2007	NONE	
US2007194931A1	23-08-2007	CA2678423A1	23-08-2007
		US7612675B2	03-11-2009
		WO2007093038A1	23-08-2007
US2002140215A1	03-10-2002	US6820897B2	23-11-2004
US2008014867A1	17-01-2008	NONE	
WO2007057786A2	24-05-2007	EP1883892A2	06-02-2008
		US2006219776A1	05-10-2006
		US7597250B2	06-10-2009
WO2005125078A1	29-12-2005	CA2471055A1	16-12-2005
		CA2570878A1	29-12-2005
		CN101015163A	08-08-2007
		EP1759479A1	07-03-2007
		US2008172713A1	17-07-2008
WO2009075434A1	18-06-2009	KR20090061118A	16-06-2009
US2009200371A1	13-08-2009	US2009104888A1	23-04-2009
		WO2009052196A1	23-04-2009
US7387260B1	17-06-2008	US7152804B1	26-12-2006
US2009224058A1	10-09-2009	EP2098981A1	09-09-2009
		FR2928475A1	11-09-2009
		JP2009211696A	17-09-2009
WO2007123895A2	01-11-2007	AU2007240903A1	01-11-2007
		CA2649584A1	01-11-2007
		CN101569130A	28-10-2009
		EP2016699A2	21-01-2009
		GB0707939D0	30-05-2007
		GB2437639A	31-10-2007
		JP2009535900T	01-10-2009
		KR20080112395A	24-12-2008
		US2007250704A1	25-10-2007
US2008238676A1	02-10-2008	NONE	

(Continued on extra sheet, page 6)

IPR2025-01150
Apple EX1071 Page 1109

(Continued from patent family annex, page 5)

WO2007149775A2	27-12-2007	AU2007261072A1	27-12-2007
		CA2655015A1	27-12-2007
		CN101473344A	01-07-2009
		EP2041714A2	01-04-2009
		KR20090023491A	04-03-2009
		MX2008016173A	26-01-2009
		US2008005037A1	03-01-2008
WO2007073609A1	05-07-2007	AU2006331310A1	05-07-2007
		CA2650063A1	05-07-2007
		CN101336436A	31-12-2008
		EA200870122A1	27-02-2009
		EA012094B1	28-08-2009
		EP1811421A1	25-07-2007
		EP1966737A1	10-09-2008
		KR20080087021A	29-09-2008
		US2009320118A1	24-12-2009

IPR2025-01150
Apple EX1071 Page 1110

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2009/007364

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of the first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons :

1. [ ] Claim Nos. :
because they relate to subject matter not required to be searched by this Authority, namely :

2. [ ] Claim Nos. :
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically :

3. [ ] Claim Nos. :
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows :

see extra sheet, page 7

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [X] As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claim Nos. :

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim Nos. :

Remark on Protest
[ ] The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
[ ] The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
[ ] No protest accompanied the payment of additional search fees.

IPR2025-01150
Apple EX1071 Page 1111

Continued from Box III, page 2

The international application relates to multiple inventions not linked to form a single general inventive concept. The multiple inventions are as follows:

Group A: Claims 1 to 11 are directed to a system comprising a transaction unit, a reader device, and a server wherein the reader transmits an authentication signal to the transaction unit, which in turn transmits a unit identifier (UI) and one-time-password (OTP) to the reader for authentication purposes. The reader communicates with a server to verify the authentication information.

Group B: Claims 12 to 16 are directed to a system comprising a transaction unit having an RFID assembly with LC circuit thereon, a contactless reader device and a server. The reader transmits an authentication signal to the transaction unit, which in turn transmits authentication data to the reader for authentication purposes. The reader communicates with a server to verify the authentication.

Group C: Claims 17 to 20 are directed to a system comprising a transaction unit having an RFID assembly, a RFID reader device and a server, wherein the RFID reader includes a jammer. The reader transmits a signal to the transaction unit when it is within a predetermined distance from the RFID reader, which in turn transmits authentication data to the reader. The reader communicates with a server to verify the authentication data.

The common features between the groups of claims are known. Specifically, WO 2006/037220 (D1) and US 2007/0194889 (D2) teach the following features:

- a transaction unit (D1 - tag 302, page 8; D2 - Tag, paragraph [0053]), a reader device (D1 - reader 301, page 8; D2 - Reader, paragraph [0053]) and a server (D1 - host 305 and security server, page 8; D2 - paragraph [0036]);
- the reader device sends an authentication signal to the transaction unit (D1 - page 8, lines 22 to 25; D2 - paragraph [0054]);
- the transaction unit responds with authentication data (D1 - page 8, lines 25 to 27; D2 - paragraph [0055]);
- the reader verifies the authentication data with a server (D1 - page 8, line 27 to page 9, line 1; D2 - paragraph [0036]).

As the common features between the groups of claims are known, the claims are considered to lack unity.

IPR2025-01150
Apple EX1071 Page 1112

UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 12:46:29 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424590	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 10

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form.pdf	12	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
WYAT-0002-13C12US_RCE_transmittal_sb0030efs.pdf	3	Request for Continued Examination (RCE)	1628 KB
WO0062214A1.pdf	50	Foreign Reference	3712 KB
WO0157620A2.pdf	165	Foreign Reference	13790 KB
GB2478712A.pdf	33	Foreign Reference	1829 KB

GB2485442A.pdf	55	Foreign Reference	3691 KB
WO2010043974A1.pdf	32	Foreign Reference	1935 KB
WO2005119607A2.pdf	52	Foreign Reference	2732 KB
WO2007145687A1.pdf	116	Foreign Reference	8227 KB
WO2012154915A1.pdf	292	Foreign Reference	14237 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form.pdf	A1DCCC49E010C972B8DA039B97AD768C924D75104D82341DD15D00514387B5428A82E16EDB5E46FDE9AF4B0C121A9C4444C3AAB4AF212CF19698B3F2F74535F0
WYAT-0002-13C12US_RCE_transmittal_sb0030efs.pdf	5A47D147BF3F4D153AB91045FBEC5786F3DCE68AE5ECD2BA94EE2B394BC27BF0C53EE5FF3AE6D7BCB0C6EFBA5CA373654D02B0B7CCD985C94F1918670777F806
WO0062214A1.pdf	DDABC100FBD99C5C2F1307B97ADAFDC42462C2F8E0A9EC08BF4DB93A3284DB009B21554EB4E4075C1982C64BCDA34ABABD069F983983ADB16719B4102F372C9C
WO0157620A2.pdf	180EBC78F4CC75B078186E3A497C95A442BC876B63C20EA5B2ACD32EF886AEEF91E5D3D51D1601CAAC89E00E66B25CB04122092207BEB9E98658F0C35EC9CA2B
GB2478712A.pdf	8FEF0EF3995674C591E9DF1668886F0633A19CF86756C6E406A54250C819993EEA54B56D8A7747698A55352B0C83FDE463BE4283E73E89340EC72BEC1C5A80F9
GB2485442A.pdf	1A2A993084C17AD07871B330FC849EF279D41D3ADD1533B418BC28A5AA9F71F623C8B1A672A909C468E9EACFBF5A704E7EA064390D0EEEF17B6F1448EFECD140

WO2010043974A1.pdf	1286E404C4D2D6FADECD924104DEFAEC9E36C84A8D2A2EA EB2BF8D92C0FF78FC7C1E94943BAB2B5068D741F166D7D90A 0B78EB3110238CF343F754C6383CA509
WO2005119607A2.pdf	F8CB44647999039A2B9B267DDA24D9B1C602EF693973B5F94 ADE9EB117CC0A6490CA09551374E915889481A8AB1ABAF5DF 22962178D89D90E69C7E5CA52A3E95
WO2007145687A1.pdf	A2ADDB624C035AAC00F247824B6AD54B06A15A36EE4B1B5E FA1BE459D3DE0BC5E781ECF631EF543EB85D53AE13B902697 CA72D63A3334618B25123D2FDE04363
WO2012154915A1.pdf	A734A15C2B5EA2E2E7A65BBDFED9D06E720BA873F1E1958B 33B89AC6941E2D48D9775F93B3FDCEE3B6CAE6AC75862E8A 0E05E1D0728AC941EE393B2FEBEA7BAF

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	01/12/2023 12:46:29 AM ET	WYAT-0002.USD1C1C1C1C1C

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424590	AUTHORIZED BY	-
CUSTOMER #	136197	FILING DATE	11/16/2021
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	David WYATT

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
EFT / 9055	E20231B147333454	Jose Garcia

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2801	REQUEST FOR CONTINUED EXAMINATION (RCE) - 1ST REQUEST (SEE 37 CFR 1.114)	544.00	1	544.00
			TOTAL AMOUNT:	$544.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(12) UK Patent Application (19) GB (11) 2478712 (13) A

(43) Date of A Publication 21.09.2011

(21) Application No: 1004246.3

(22) Date of Filing: 15.03.2010

(51) INT CL:
G06Q 20/00 (2006.01) *G07C 9/00* (2006.01)
G07F 7/08 (2006.01)

(56) Documents Cited:
US 20080222048 A US 20080210754 A1
US 20050211771 A1

(58) Field of Search:
INT CL G06Q, G07C, G07F
Other: Online: WPI & EPODOC

(71) Applicant(s):
David Jackson
18 Feltham Avenue, EAST MOLESEY, KT8 9BL, United Kingdom

(72) Inventor(s):
David Jackson

(74) Agent and/or Address for Service:
Mathys & Squire LLP
120 Holborn, LONDON, EC1N 2SQ, United Kingdom

(54) Title of the Invention: **Authorisation system**
Abstract Title: **Authorisation system**

(57) An authorisation system 1 which comprises a transaction processing terminal 20 for processing transactions; and a mobile user device 10, the user device 10 comprising means for receiving information relating to a particular transaction from the processing terminal 20, and means for generating a user code to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal 20 thereby to enable the processing terminal 20 to process the transaction. The invention extends to a corresponding method, a point-of-sale terminal POS, and a mobile device. The process for card holder present transactions comprises the merchant scanning goods and presenting via a barcode the transaction reference, merchant id and amount. The customer scans the barcode and depending on the amount enters a PIN into the smart phone. The smartphone generates a one time activation code and card number via an on screen barcode and the merchant scans the barcode and processes the transaction. A dynamic activation code may be generated based on a clock signal and a preinstalled random seed key. The system may also be used to control access or authorize provision of service.

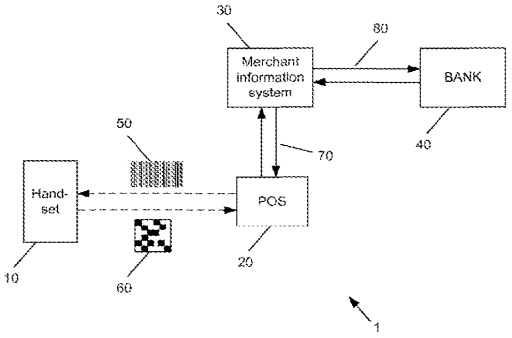


Fig. 1

GB 2478712 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

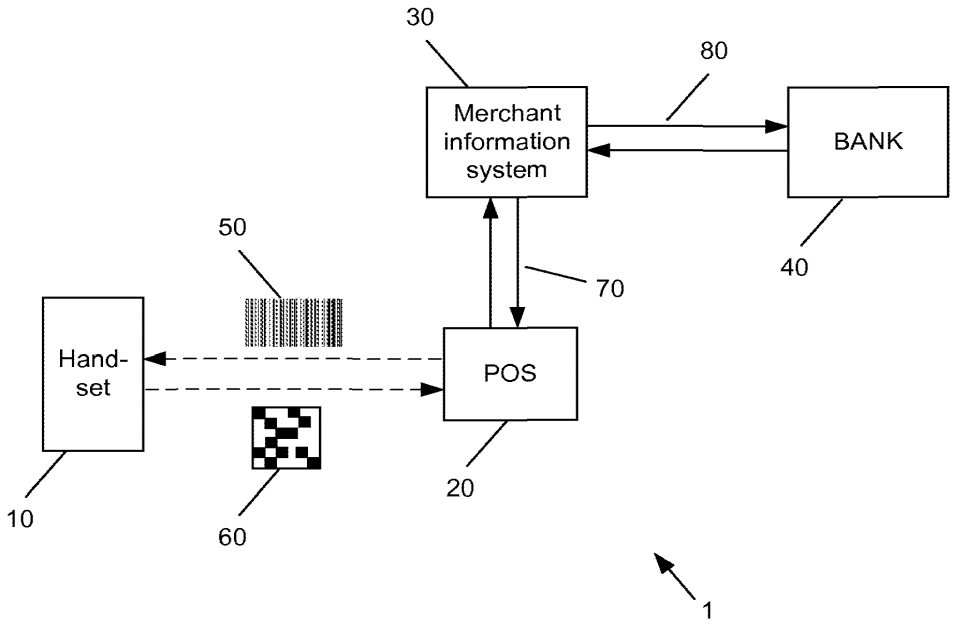

30
80
Merchant information system
BANK
40
50
70
Hand-set
POS
10
60
20
1

Fig. 1

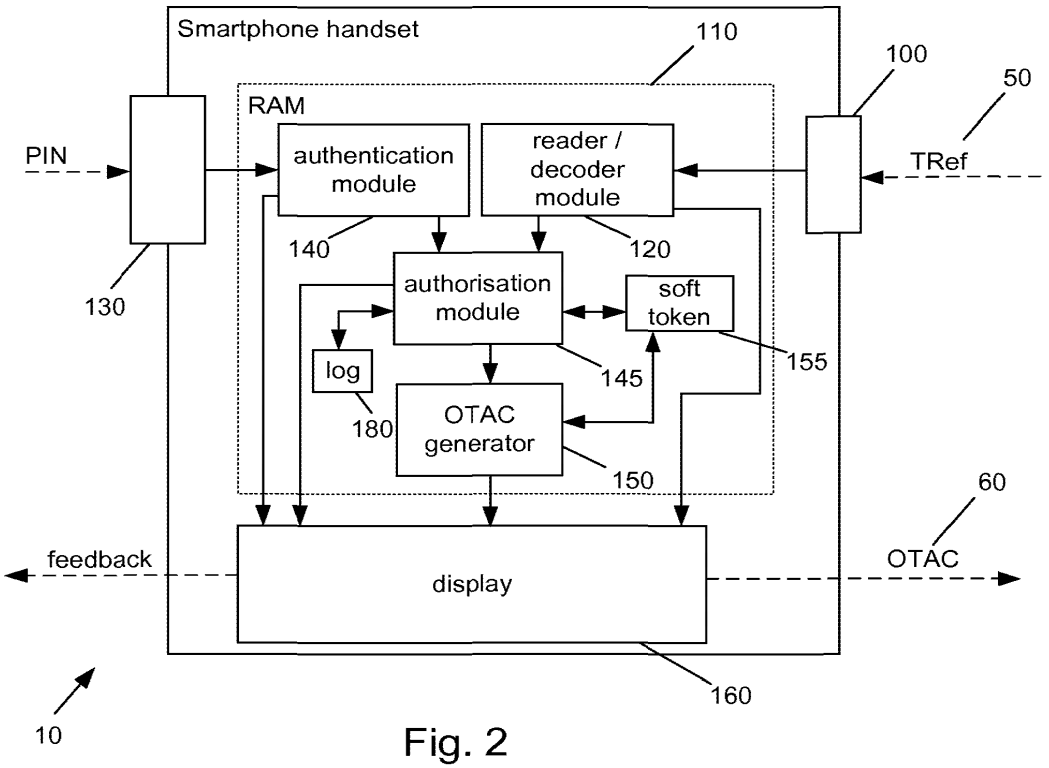

Smartphone handset
110
100
50
RAM
PIN
authentication module
reader / decoder module
TRef
140
120
130
authorisation module
soft token
log
155
145
180
OTAC generator
150
60
feedback
display
OTAC
160
10

Fig. 2

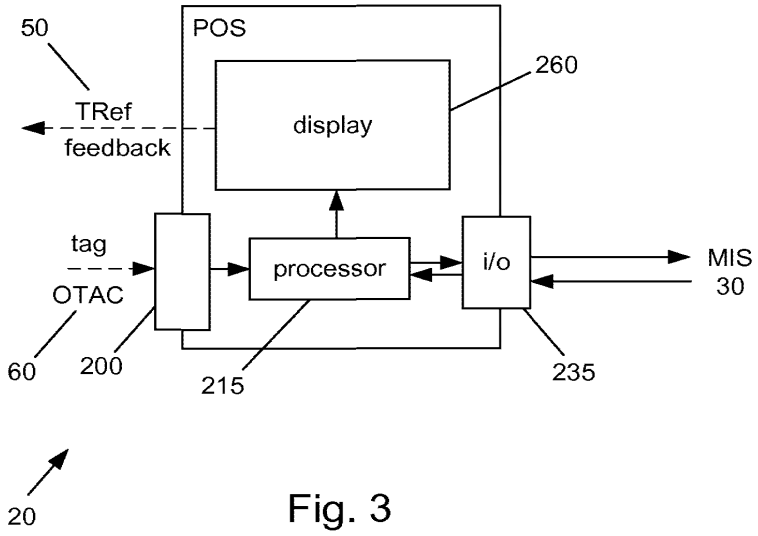

50
POS
260
TRef
feedback
display
tag
processor
i/o
MIS
30
OTAC
60
200
215
235
20

Fig. 3

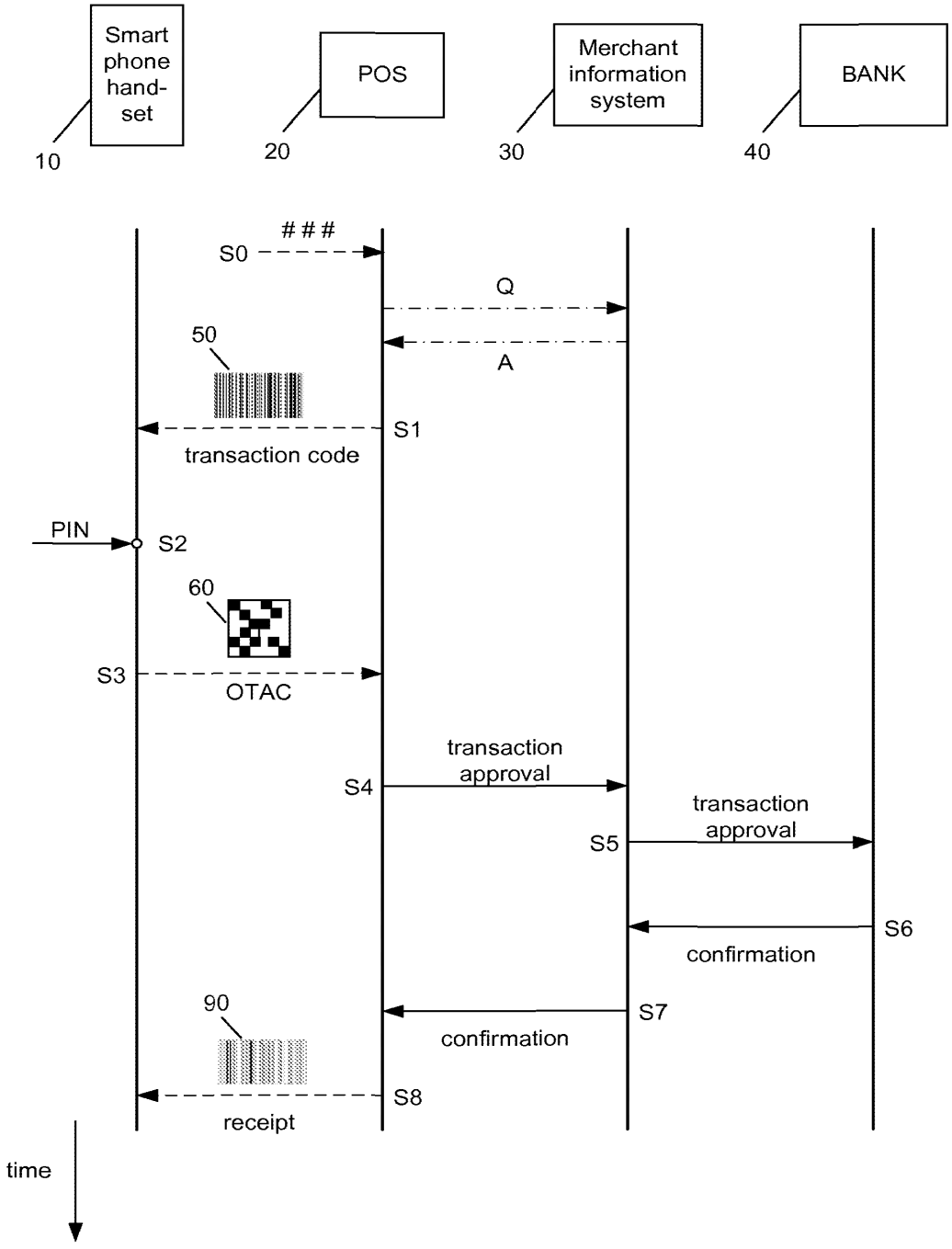
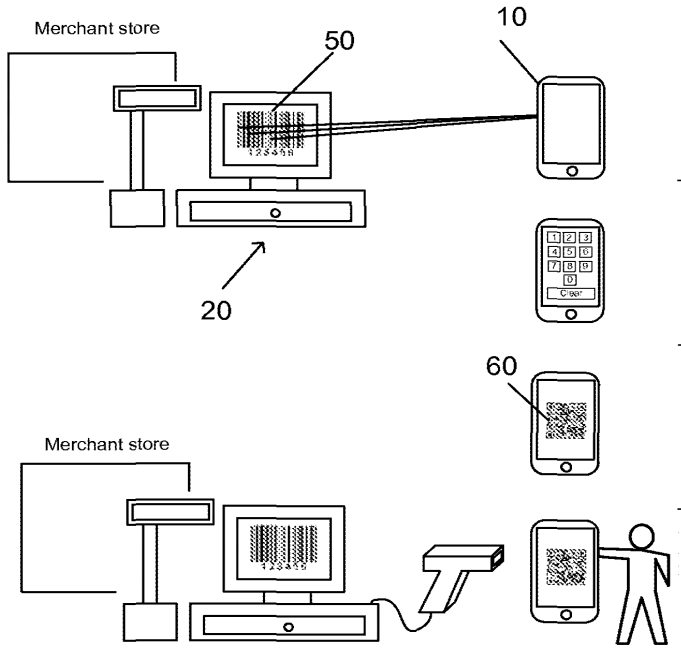

Smart phone hand-set
10
POS
20
Merchant information system
30
BANK
40
###
S0
Q
A
50
S1
transaction code
PIN
S2
60
S3
OTAC
transaction approval
S4
transaction approval
S5
S6
confirmation
90
S7
confirmation
S8
receipt
time

Fig. 4



Process for card holder present transactions

1. Merchant scans good(s) and presents via barcode the transaction ref, merchant ID and amount.

2. Customer scans barcode and depending on amount enters their PIN in to smart phone.

3. Smart phone generates a one time transaction authorisation code and card number via on screen barcode

4. Merchant scans barcode and processes payment.

14 06 11

Fig. 5

Authorisation system

The present invention relates to an authorisation system. This invention also relates to a method of authorising a transaction, and to a mobile device and a point-of-sale (POS) terminal.

Authorisation systems for enabling users to carry out transactions that make use of tokens (such as credit cards) containing RFID tags are known, for example, the MasterCard ™ PayPass ™ system. Such systems enable a user to swipe a credit card equipped with an RFID tag over a reader located at a point-of-sale (POS) terminal in order to effect a payment transaction. However, such systems may be vulnerable to eavesdropping, and the information contained on the RFID tag cannot be altered dynamically, for example, in an effort to improve security. Furthermore, since no user authentication is required, such transactions are limited in value so as to limit the financial exposure to a user and the card issuer should a card be lost or stolen.

For larger value transactions, chip and pin systems are frequently employed. However, there may be security flaws in chip and pin systems. It is known to use separate card readers, into which a credit card is inserted, to generate dynamic pass codes, such as the Visa ™ Dynamic Passcode Authentication Scheme. These systems do enhance the security of existing chip and pin systems. However, the requirement for a user to carry around a card reader, in addition to their credit card, may be inconvenient in certain circumstances.

The present invention aims to alleviate at least some of these problems.

According to one aspect of the invention, there is provided an authorisation system which comprises a transaction processing terminal for processing transactions; and a mobile user device, the user device comprising means for receiving information relating to a particular transaction from the processing terminal, and means for generating a user code to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

The generation of a user code on the basis of the received transaction information may enhance the security of the system.

Preferably, the user code generating means is adapted to generate a user code which is in the form of a machine readable code.

Preferably, the user code generating means is further adapted to generate a user code which is in the form of an optical indicator. More preferably, the code is in the form of a bar code, and yet more preferably a two-dimensional bar code.

Preferably, the terminal comprises means for reading the code.

Preferably, the reading means comprises an optical scanner.

Alternatively, or in addition, the user code generating means is further adapted to generate the user code in the form of a series of audible tones, and preferably a series of dual-tone multi-frequency (DTMF) signalling tones. In this case, the terminal may be adapted to receive audible tones.

Preferably, the user code generating means is adapted to generate a unique code for each transaction. Hence, the user code is referred to herein as a one-time authorisation code (OTAC).

Preferably, the user code generating means is adapted to incorporate the information relating to a particular transaction within the user code.

Preferably, the user code generating means is adapted to incorporate at least one of the following pieces of information relating to the transaction within the user code: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

Preferably, the user code generating means is adapted to incorporate bank details relating to the user of the mobile device into said code.

Preferably, the bank details are stored on the mobile device, preferably in encrypted form.

Alternatively, or in addition, the bank details may be stored on a remote server, preferably a secure server connectable to the internet. Preferably, the mobile device further comprises means for accessing the server thereby to obtain the bank details from the remote server. Preferably, the mobile device comprises means for connecting the mobile device to the internet.

Alternatively, or in addition, the bank details may be provided in a physical form on an outer surface of the mobile phone. Preferably, the bank details are displayed on an outer surface of the mobile device. More preferably, the bank details are etched onto the outer surface and/or cover of the mobile device. In one example, a card number may be etched onto the rear cover of the mobile device. In an alternative example, an optical indictor, preferably in the form of a bar code, may be provided on the outer surface of the device.

Preferably, the bank details comprise at least one of the following: a credit card number; a bank account number; a Card Verification Value (CVV) code; bank and/or credit card validity dates; and a bank and/or credit card issue number.

Preferably, the user code generating means is adapted to incorporate a dynamically generated authentication code within the user code.

Preferably, the mobile device comprises means for generating a dynamic authentication code based on a clock signal of the user device and a preinstalled random seed key.

Preferably, the means for generating the dynamic authentication code is adapted to generate the code on the basis of the bank details stored on the mobile device.

In the case where the bank details are stored on a remote server, the user code generating means may be adapted to request a dynamically generated authentication

code from the server, in which case the server further comprises means for generating a dynamic authentication code.

Preferably, the mobile device further comprises means for encrypting the user code.

Preferably, the mobile device further comprised means for storing a log of all generated user codes.

Preferably, the mobile device further comprises means for authenticating a user prior to generating the user code.

Preferably, the authentication means comprises means for interrogating a user.

Preferably, the interrogating means comprises means for presenting a user with an authentication screen adapted to be displayed on a display means of the mobile device.

Preferably, the authenticating means is adapted to make use of a Personal Identification Number (PIN) code corresponding to the user's bank account and/or credit card to authenticate the user.

Preferably, the PIN code is stored in an encrypted form on the mobile device.

Preferably, the authentication means is adapted to authenticate the user using a set of images.

Preferably, the set of images includes a selection of random images and at least one image that is known to the user.

Preferably, the authentication means is adapted to authenticate a user on the basis of information relating to the user available via the user's online profile.

Preferably, the authentication means is adapted to access the online profile of a user thereby to obtain information relating to the user to form the basis of the authentication.

Preferably, the processing terminal comprises means for decoding the user code to extract information relating to the user authorisation of the transaction.

Preferably, the terminal comprises means for decrypting the user code.

Preferably, the terminal is connectable to a transaction approval system for approving transactions.

Preferably, the terminal is adapted to transmit information relating to the user authorisation of the transaction to the approval system.

Preferably, the approval system includes a banking institution.

Preferably, the processing terminal further comprises means for displaying transaction information to a user thereby to enable a user to input manually the transaction information relating to a particular transaction into the mobile device.

Preferably, the transaction information comprises at least one of the following: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

Preferably, the processing terminal comprises means for generating a transaction code relating to a particular transaction, said code being adapted to be read by the mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

According to a further aspect of the invention, there is provided an authorisation system which comprises a processing terminal for processing transactions; and a mobile user device, wherein the processing terminal comprising means for generating a transaction code relating to a particular transaction, said code being adapted to be read by the mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

Preferably, the processing terminal further comprises means for displaying the transaction code.

Preferably, the processing terminal is adapted to display the transaction code in the form of an optical indictor.

Preferably, the transaction code generating means is adapted to generate the transaction code in the form of an optical indictor, and preferably in the form of a bar code.

Alternatively, or in addition, the transaction code generating means is further adapted to generate the user code in the form of a series of audible tones, and preferably a series of dual-tone multi-frequency (DTMF) signalling tones. In this case, the mobile device may be adapted to receive audible tones.

Preferably, the truncation code incorporates at least one of the following: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

Preferably, the mobile device further comprises means for reading the transaction code.

Preferably, the reading means is adapted to scan the transaction code.

Preferably, the mobile device further comprises a camera adapted to photograph the transaction code. More preferably, the camera is adapted to operate as an optical scanner.

Preferably, the mobile device further comprises means for decoding the transaction code thereby to extract transaction information from the transaction code.

Preferably, the processing terminal comprises means for displaying a confirmation receipt relating to a completed transaction.

Preferably, the processing terminal comprises a user interface for enabling a user to manually enter a user code into the terminal.

Preferably, the mobile user device is in the form of a mobile telephone and/or a personal digital assistant, and preferably a smartphone.

Preferably, the processing terminal is in the form of a point-of-sale (POS) terminal.

Preferably, the processing terminal is in the form of an internet-based or online merchant.

Preferably, the system is in the form of a payment system.

According to a further aspect of the invention, there is provided a mobile device which is adapted to form part of the system as herein described.

According to another aspect of the invention, there is provided a point-of-sale (POS) device adapted to form part of the system as herein described.

According to another aspect of the invention, there is provided a method of authorising a transaction using a mobile device, the method comprising: receiving information relating to a particular transaction from a transaction processing terminal; and generating a user code on the mobile device to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

According to yet another aspect of the invention, there is provided a method of processing a transaction using a point-of-sale (POS) terminal, which comprises: generating a transaction code relating to a particular transaction, said code being adapted to be read by a mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

According to a further aspect of the invention, there is provided a mobile device (preferably in the form of a mobile telephone) which comprises software code adapted to carry out the various method steps as described herein.

According to a further aspect of the invention, there is provided a point-of-sale terminal which comprises software code adapted to carry out the various method steps as described herein.

According to another aspect of the invention, there is provided a mobile device, which comprises means for receiving information relating to a particular transaction from a transaction processing terminal; and means for generating a user code on the mobile device to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

According to a further aspect of the invention, there is provided a point-of-sale (POS) terminal, which comprises means for generating a transaction code relating to a particular transaction, said code being adapted to be read by a mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

In another aspect the invention provides a method of authorising payment transactions by exchanging dynamically generated optical indicators, preferably in the form of bar codes, between a mobile user device and a transaction processing terminal.

The invention also provides a computer program and a computer program product comprising software code adapted, when executed on a data processing apparatus, such as the processing terminal and/or mobile device to perform any of the methods described herein, including any or all of their component steps.

The invention also provides a computer program and a computer program product comprising software code which, when executed on a data processing apparatus, such as the processing terminal and/or mobile device, comprises any of the apparatus

features described herein.

The invention also provides a computer program and a computer program product having an operating system which supports a computer program for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein.

The invention also provides a computer readable medium having stored thereon the computer program as aforesaid.

The invention also provides a signal carrying the computer program as aforesaid, and a method of transmitting such a signal.

The invention extends to methods and/or apparatus substantially as herein described with reference to the accompanying drawings.

Any feature in one aspect of the invention may be applied to other aspects of the invention, in any appropriate combination. In particular, method aspects may be applied to apparatus aspects, and vice versa.

Furthermore, features implemented in hardware may be implemented in software, and vice versa. Any reference to software and hardware features herein should be construed accordingly.

Each feature disclosed in the description, and (where appropriate) the claims and drawings may be provided independently or in any appropriate combination.

The invention is now described, purely by way of example, with reference to the accompanying drawings, in which:-

Figure 1 shows an authorisation system;
Figure 2 is a block diagram of a smartphone;
Figure 3 is a block diagram of a point-of-sale (POS) terminal;

Figure 4 shows a time-sequence chart of the information exchange steps involved in making a payment for an item using the system of Figure 1; and
Figure 5 shows another embodiment of the authorisation system of Figure 1.

Figure 1 shows an authorisation system, in the form of a smartphone-based payment system 1, as may be located in a department store or shopping mall (or, in principle, in many other commercial premises). The system 1 includes a mobile user device in the form of a smartphone handset or PDA 10 which interacts with a transaction processing terminal in the form of a point-of-sale (POS) terminal 20 by means of an exchange of machine-readable codes 50, 60. The exchange of these codes 50, 60 allows the user of the smartphone 10 to authorise the purchase of an item in the department store; the authorisation is subsequently passed by the POS terminal 20 to a merchant information system (MIS) 30 and thereby used to approve the transaction and effect the appropriate transfer of funds at the bank 40 to make the payment for the item.

The exchanged codes 50, 60 comprise a transaction reference code (TRef) 50 and a one-time authorisation code (OTAC) 60.

Transaction reference code (TRef) 50 is generated dynamically by the POS terminal 20 to be read by the smartphone 10 and comprises information on the product being purchased. TRef 50 includes one or more of the following: an item description, the item price, a merchant identifier, and a time stamp. In this example, TRef 50 is in the form of an optical indicator such as a barcode, which can be readily captured by a built-in camera 100 of the smartphone 10.

The one-time authorisation code (OTAC) 60 is generated by the smartphone 10 in dependence on the received transaction reference code (TRef) 50 and also in dependence on the user's bank account and/or credit card details (which may be stored on the smartphone 10). The user of the smartphone 10 must first be authenticated thereby to authorise the transaction, for example, by entering a security PIN associated with their bank account and/or credit card, before the OTAC 60 is generated for sending on to the POS terminal 20. In this embodiment, the OTAC 60 is also an optical indicator such as a 2D barcode (1D barcodes are possible alternatives).

Also shown in Figure 1 are the transaction approval / confirmation messages 70 (exchanged by the POS terminal 20 and the merchant information system 30) and 80 (exchanged by the merchant information system 30 and the bank 40) to approve, complete, and provide feedback regarding the transaction.

Figure 2 is a block diagram of the smartphone 10, comprising a user interface 130 such as a touchscreen (for example, the Apple iPhone and various models made by Nokia, Samsung, LG and HTC amongst others) or a keypad / keyboard (for example, the Blackberry made by Research In Motion, and various models by Nokia and Sony, amongst others), a display 160 and a camera 100.

The smartphone 10 has been adapted by software to capture or scan (by means of the camera 100) and process (by means of the software modules described below) optical indicators such as barcodes used to represent transaction reference codes (TRef) 50. In operation, random-access memory (RAM) 110 of the smartphone 10 comprises a number of software modules including a reader/decoder module 120, an authentication module 140, an authorisation module 145 and a one-time authorisation code (OTAC) generator 150. Together these modules form a smartphone purchasing application. The software modules are written in a suitable programming language for the suitable software platform for the particular smartphone operating system, for example Java MIDP, C++ or Python on the S60 platform for smartphones running Symbian OS.

The reader/decoder module 120 processes optical indicator details (such as barcodes) captured by the smartphone camera 100 and representing transaction reference codes (TRef) 50. The reader/decoder module 120 decodes the captured TRef 50 into its constituent pieces of information, such as the item description, the item price, and a merchant identifier, and passes this information on to the authorisation module 145. The reader/decoder module 120 sends feedback regarding progress in capturing the TRef data and information regarding the item to the user via display 160.

The authentication module 140 assesses whether the correct security PIN has been entered by the user via the user interface 130 to authenticate the user to allow

authorisation of the purchase of the item. In this embodiment, details of the user's bank (or for example credit or debit card details) and corresponding PIN are stored (in encrypted form) within the authentication module 140. The PIN entered by the user via user interface 130 is compared to the stored PIN and if the values match, a positive authentication is sent to the authorisation module 145; if the values do not match, standard security measures are employed (for example, only a limited number of re-tries are permitted before the smartphone purchasing application is locked). The authentication module 140 sends feedback regarding PIN input and authentication to the user via the display 160.

The authorisation module 145 correlates the item information received from the reader/decoder module 120 with the result of the authentication received from the authentication module 140, recording in log 180 whether the purchase of the item has been approved by the user, providing feedback to the user via the display 160 and instructing the OTAC generator 160 to generate a OTAC to send to the POS terminal 20.

OTAC generator 150 generates a one-time authorisation code (OTAC) 60 to send to the POS terminal 20 to authorise the purchase of the item.

The One-Time Authorisation Code (OTAC) 60 is generated in dependence on data which includes information obtained from the received transaction reference code (TRef) 50 (which, as described previously, may comprise a item description, item price, and a merchant identifier) and the user's bank account details (for example, the user's account number, credit/debit card number, card valid-from/expiry date, issue number and card verification value CVV) stored on the smartphone by the authentication module 140. Additional details encoded in the OTAC may include data specific to the smartphone 10, such as the IMEI (International Mobile Equipment Identity) number, or to the user such as the IMSI (international mobile subscriber identity) stored on the SIM (subscriber identity module) card. A time-stamp is also included.

A hashing algorithm is used to combine the data (or the appropriate subset, as acceptable to authorise payment transactions by the merchant information system 30

and bank 40) and generate the OTAC 60 in the form of an optical indicator such as a 2D barcode (for example, according to an open-standard such as Data Matrix or Semacode) which is displayed on the screen 160, and is readable by the POS terminal 20.

The uniqueness of the OTAC therefore results from the particular data used in its generation. The system therefore allows for the use of a combination of "something you have" (the smartphone 10, which has encoded data specific to a user's bank account and/or credit card) with "something you know" (the PIN) as required by a two-factor authentication scheme.

The "one-time" or unique aspect of the one-time authorisation code (OTAC) 60 is further enhanced by providing the smartphone 10 with a dynamic authentication code generating means, in the form of a soft token 155, which is used to generate dynamic authentication codes which are then embedded within the OTAC 60. In one example, the system uses an authentication scheme based on RSA SecurID, which can be used to generate a series of secretly-seeded random numbers at regular time intervals. In this case, the secret seed will have been previously securely transmitted (potentially encrypted by a public-key of the user or assigned to the smartphone 10) or installed directly at the smartphone 10, and is otherwise known only to the bank 40 (or a certification authority) which therefore knows what authentication code to expect at any given time. RSA SecurID is available as a software module and executes from the smartphone 10 RAM 110.

Figure 3 is a block diagram of a point-of-sale (POS) terminal 20, comprising an optical scanner 200, a processor 215, an input / output (i/o) port 235 (to connect the POS terminal 20 to the merchant information system 30, for example by a network connection or telephone line) and a display 260.

Figure 4 shows a time-sequence chart of the information exchange steps involved in making a payment for an item using the smartphone-based payment system 1.

In a preliminary step (S0), the customer / smartphone user having taken the item to be

purchased to the POS terminal 20, the POS terminal 20 determines the item details by, for example, reading the price-tag attached to the item (this may be a barcode, a magnetic strip an RFID tag or some other form of price tag) by means of scanner 200, processing the resulting data using processor 215 (optionally, if the POS terminal 20 does not have this information stored, enquiring via the i/o port 235 of the merchant information system (MIS) 30 as to the item details, shown as exchange Q-A) and displaying on display 260 a machine-readable transaction code 50. Optionally, POS terminal 20 may also display human-readable details regarding the item on the display 260 for the convenience of (and as feedback for) the customer.

In step S1, the user scans transaction code 50 displayed by POS terminal 20 with the camera 100 of smartphone 10, that is, the camera 100 of the smartphone 10 is used as a barcode scanner.

In step S2, the user authorises the transaction by entering the PIN associated with the bank account or credit card. If the entered PIN is correct (as determined by the authentication module 140), smartphone 10 generates (by means of the OTAC generator module 150) a one-time authorisation code (OTAC) 60.

In step S3, smartphone 10 sends the OTAC code 60 authorising payment to the POS terminal 20. In practice, this means smartphone 10 displays the 2D barcode representing the OTAC code 60 on its display screen 160, and the POS terminal 20 scans the code with its scanner 200. As mentioned above, the OTAC 60 typically includes the user's bank card data (possibly including a dynamic authentication code) together with certain transaction information.

In step S4, POS terminal 20 sends the transaction approval message to merchant information system 30. Depending on the encryption scheme in use (if any), processor 215 of the POS terminal 20 may be able to decode the OTAC 60 and send pertinent transaction details to the merchant information system 30; alternatively, if processor 215 of the POS terminal 20 cannot decode the OTAC 60, POS terminal 20 acts merely as a relay and forwards the OTAC 60 to the merchant information system 30.

In step S5, merchant information system 30 (potentially having first decoded the OTAC 60) sends a transaction approval message and user bank details to bank 40. Bank 40 makes the payment, transferring money from the user's bank account to that of the merchant.

In step S6, bank 40 sends a confirmation message to merchant information system 30, confirming the payment has been made.

In step S7, merchant information system 30 sends a confirmation message to POS terminal 20, which then displays a confirmation message to the customer / smartphone user.

Optionally, in step S8, POS terminal 20 issues a receipt 90 in the form of further optical indicator, such as barcode. This is scanned by the user with the camera 100 of smartphone 10, which then stores the receipt as evidence of the purchase having been made. Alternatively, a traditional paper receipt may be issued.

Figure 5 shows another embodiment of the smartphone-based payment system 1, showing the process for card-holder present transactions, comprising the steps of:

1. Merchant scans good(s) and presents via barcode the transaction reference, merchant ID and amount;
2. Customer scans barcode with a smartphone or handset and depending on amount enters their PIN in to smartphone (low value transactions may be processed and authorised without the need to enter a pin);
3. Smartphone generates a one-time transaction authorisation code and card number via an onscreen barcode; and
4. Merchant scans barcode and then processes payment.

Further features

- Additional security

For additional security, the data may be encrypted before or during generation of the

OTAC to prevent user information being obtained surreptitiously by those obtaining the unencrypted OTAC (for example by intercepting its transmission to the POS terminal 20) and reversing the hashing algorithm. An encryption key is stored as a further software token on the smartphone handset 10. In a symmetric-key scheme, the further software token is one of identical shared secret keys; the other shared secret key is stored at the bank 40. In an asymmetric-key (or public-key) scheme, the further software token is the public key issued by the bank; the bank's private key is stored at the bank 40.

As a further alternative, the PIN needing to be entered by the user need not be the same one as used to access the user's bank account directly, but merely one to access the smartphone payment system on that particular smartphone 10.

- Remote storage of bank account details

In an example, instead of storing the user bank account details, such as a credit card number, on the smartphone 10, the bank account details are instead stored on a secure remote server that is typically connected to the banking institution's communication network infrastructure. In this case, the smartphone 10 is adapted to access the bank account details by establishing a secure connection to this server, for example via a Secure Sockets Layer (SSL) internet connection. In particular, after the user has been authenticated, for example by entering the correct security PIN, the authorisation module 145 then establishes a secure communications channel with the remote server to extract the user's bank account details from the remote server. These details are then used by the OTAC generator 150 to generate the OTAC 60.

In another example, the remote server is capable of generating a dynamic authentication code, for example, based on the user bank account details which are stored on the remote server, and when the authorisation module connects to the remote server, instead of extracting or downloading the full user bank account details or card number, the server instead generates a dynamic authentication code which is then transmitted to the smartphone for use by the OTAC generator 150 in creating the OTAC 60.

- PIN-less payments

For the convenient purchase of items of low monetary value, such as newspapers, step S2, in which the user authorises the transaction by entering the security PIN associated with the user's bank account, is optional and the payment may be termed 'PIN-less'. In this case, the user would merely click an "accept button" to authorise the transaction.

In order to limit the financial exposure were the smartphone to be stolen, PIN-less payments are restricted in that they may only be made for individual purchases not exceeding a predetermined maximum monetary value per purchase. Optionally, the total value for PIN-less payments made in total and/or during a predetermined time period may also be restricted to a predetermined maximum monetary value (reaching this value then requires the user to re-set the PIN-less payment system, which necessitates entering the requisite PIN).

- Manual entry systems

In certain examples, instead of the POS terminal 20 presenting the user with a barcode for scanning with the camera 100 of smartphone handset 10, POS terminal 20 presents transaction reference code (TRef) 50 in the form of an alphanumeric string which the user keys into the smartphone 10 manually via user interface 130. The subsequent steps S2 to S8 proceed as described above. Step S3, wherein POS terminal 20 scans the OTAC 60 displayed on the display screen 160 of smartphone 10 may also be replaced by the manual entry of an alphanumeric string by the user on the POS terminal 20. In this case the OTAC is presented in the form of an alphanumeric string which the user then enters into a keypad of the POS terminal 20.

- Telephone based transactions

The described payment system may also be adapted for the payment of goods or services over a telephone communications system. In this case, the transaction reference code (TRef) 50 and/or the OTAC 60 are generated in the form of a series of audible DTMF signalling tones. In particular, the POS terminal 20 generates the TRef code 50 in the form of a sequence of DTMF tones, which are then received by the smartphone 10, for example, via a microphone of the smartphone 10. The smartphone 10 then extracts the transaction information from the sequence of DTMF tones and then

generates the OTAC 60 in dependence on the received transaction information. In this case, the generated OTAC 60 is also in the form of a sequence of DTMF tones, which are then played to the POS terminal 20, which then receives and decodes these tones to process the transaction.

In certain examples, the payment system might use a combination of audible, visual or other OTAC 60 and TRef 50 codes. Thus, for example, the smartphone 10 might receive a TRef code 50 in the form of a sequence of DTMF tones, and then generate the OTAC 60 in the form of a 2D barcode.

- Internet based transactions

The described smartphone payment system may also be adapted for payment of goods and services over the internet. In one example, the merchant information system 30 provides a web-site which displays optical indicators such as barcodes to relate information such as item descriptions, item prices, and a merchant identifier. In an analogous way to that of the above-described POS-based embodiment, the user scans the requisite barcode with the smartphone handset 10 and enters a PIN to authorise the transaction (steps S1 and S2).

In one example, based on the manual entry systems described above, the OTAC 60 generated by smartphone 10 is in the form of an alphanumerical string which the user enters manually into a text box on the website to approve payment.

In an alternative embodiment, the user generates an OTAC 60 via smartphone 10 and merchant information system 30 uses the user's webcam to read the OTAC 60.

- Further authentication schemes

Instead of authenticating the user by having them input a PIN directly via the user interface 130 (which may require bank account or credit card information and PIN being stored on the smartphone handset 10), alternative authentication schemes may be used.

- ***Picture password authentication***

In one example, the user is shown a selection of random photographs, one of which is a 'key' photograph for the user, for example, a photograph of a person that is related to user. The user is then authenticated by selecting the correct 'key' photograph. The user might also be required to select more than one photograph displayed on the screen, or might be required to select particular photographs from successively displayed selections of photographs. 'Key' photographs are typically preselected by the user or authorising system.

- ***Online profile authentication***

In another example, items specific to the user and obtainable from the user's recent on-line activity (for example, a recent posting to a social networking website or a twitter 'tweet') are presented amongst other items of a similar form; the user authenticates by correcting identifying their own contributions.

This form of authentication might be used in combination with the above described picture password authentication, since 'key' photographs might be sourced from a user's online profile, for example, the system might make use of an image that has recently been uploaded to a user's page on a social networking site.

- ***Voice authentication***

Another possible authentication scheme is to use a speech recognition system to identify the user.

- Dynamic credit card numbers

In an example, the smartphone 10 is provided with a series of credit card numbers to be used for a successive series of transactions. In this case, each credit card number is only valid for a particular time period (for example for one day or one week) or for a particular number of transactions. After the specified time period, or after a particular number of transactions, the card number expires and the next card number in the sequence is then used for subsequent transactions. The series of credit card numbers are securely delivered to the smartphone in a similar manner to that described above

with respect to the delivery of a secret seed code. In this case, when the user carries out a payment transaction using the smartphone 10, the OTAC 60 would be generated based on the currently valid credit card number in a particular series.

- Physical card details

In one example, the user's bank account details are provided on an outer surface of the smartphone 10 itself. In particular, the user's card number, or a coded representation of the user's card number (such as a barcode), is etched onto the rear surface of the smartphone 10. In an example, the card number or barcode is etched or displayed on a removable cover of the smartphone 10. Alternatively, the card number or barcode could be provided in the form of a (removable) sticker which is stuck onto the rear surface of the smartphone 10. In this case, the OTAC generator is used to generate an OTAC which includes a dynamic authentication code, but which does not include the user's card number. The user's card number is then either manually inputted by the user into the POS terminal 20, or scanned by the POS terminal 20 from the rear surface of the smartphone 10 at the time that the user scans the transaction reference code (TRef) 50 from the POS terminal 20. In the case where the user's card number itself is provided on the surface of the smartphone, the card would be of the type that would only operate if it is used in combination with a dynamic authentication code.

While, the authorisation system has been described above mainly with reference to a payment system 1, it is also envisaged that the present authorisation system could be used in many other similar situations in which it is necessary to control access and/or authorise the provision of goods or services. For example, the system could be employed to control access to a particular controlled area, like a music concert or a public transportation system.

It will be understood that the present invention has been described above purely by way of example, and modifications of detail can be made within the scope of the invention.

Claims:

1. An authorisation system which comprises a transaction processing terminal for processing transactions; and a mobile user device, the user device comprising means for receiving information relating to a particular transaction from the processing terminal, and means for generating a user code to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

2. The system of Claim 1, wherein the user code is in the form of a machine readable code.

3. The system of Claim 1 or 2, wherein the user code is in the form of an optical indicator.

4. The system of Claim 3, wherein the code is in the form of a bar code, and more preferably a two-dimensional bar code.

5. The system according to any of the preceding claims, wherein the terminal comprises means for reading the code.

6. The system according to Claim 5, wherein the reading means comprises an optical scanner.

7. The system according to any of the preceding claims, wherein the user code generating means is adapted to generate a unique code for each transaction.

8. The system according to Claim 7, wherein the user code generating means is adapted to incorporate the information relating to a particular transaction within the user code.

9. The system according to Claim 8, wherein the user code generating means is

adapted to incorporate at least one of the following pieces of information relating to the transaction within the user code: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

10. The system according to any of the preceding claims, wherein the user code generating means is adapted to incorporate bank details relating to the user of the mobile device into said code.

11. The system according to Claim 10, wherein the bank details are stored on the mobile device.

12. The system according to Claim 10 or 11, wherein the bank details comprise at least one of the following: a credit card number; a bank account number; a Card Verification Value (CVV) code; bank and/or credit card validity dates; and a bank and/or credit card issue number.

13. The system according to any of the preceding claims, wherein the user code generating means is adapted to incorporate a dynamically generated authentication code within the user code.

14. The system according to Claim 13, further comprising means for generating a dynamic authentication code based on a clock signal of the user device and a preinstalled random seed key.

15. The system according to any of the preceding claims, further comprising means for encrypting the user code.

16. The system according to any of the preceding claims, further comprising means for storing a log of all generated user codes.

17. The system according to any of the preceding claims, wherein the mobile device further comprises means for authenticating a user prior to generating the user code.

18. The system according to Claim 17, wherein the authentication means comprises means for interrogating a user.

19. The system according to Claim 18, wherein the interrogating means comprises means for presenting a user with an authentication screen adapted to be displayed on a display means of the mobile device.

20. The system according to any of the preceding Claims 17 to 19, wherein the authenticating means is adapted to make use of a Personal Identification Number (PIN) code corresponding to the user's bank account and/or credit card to authenticate the user.

21. The system according to Claim 20, wherein the PIN code is stored in an encrypted form on the mobile device.

22. The system according to any of the preceding Claims 17 to 19, wherein the authentication means is adapted to authenticate the user using a set of images.

23. The system according to Claim 22, wherein the set of images includes a selection of random images and at least one image that is known to the user.

24. The system according to any of the preceding Claims 17 to 19 and 22 or 23, wherein the authentication means is adapted to authenticate a user on the basis of information relating to the user available via the user's online profile.

25. The system according to Claim 24, wherein the authentication means is adapted to access the online profile of a user thereby to obtain information relating to the user to form the basis of the authentication.

26. The system according to any of the preceding claims, wherein the terminal comprises means for decoding the user code to extract information relating to the user authorisation of the transaction.

27. The system according to any of the preceding claims, wherein the terminal comprises means for decrypting the user code.

28. The system according to any of the preceding claims, wherein the terminal is connectable to a transaction approval system for approving transactions.

29. The system according to Claim 28, wherein the terminal is adapted to transmit information relating to the user authorisation of the transaction to the approval system.

30. The system according to Claim 28 or 29, wherein the approval system includes a banking institution.

31. The system according to any of the preceding claims, wherein the processing terminal further comprises means for displaying transaction information to a user thereby to enable a user to input manually the transaction information relating to a particular transaction into the mobile device.

32. The system according to Claim 31, wherein the transaction information comprises at least one of the following: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

33. The system according to any of the preceding claims, wherein the processing terminal comprises means for generating a transaction code relating to a particular transaction, said code being adapted to be read by the mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

34. An authorisation system which comprises a processing terminal for processing transactions; and a mobile user device, wherein the processing terminal comprising means for generating a transaction code relating to a particular transaction, said code being adapted to be read by the mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

35. A system according to Claim 33 or 34, wherein the processing terminal further

comprises means for displaying the transaction code.

36. A system according to Claim 35, wherein the processing terminal is adapted to display the transaction code in the form of an optical indictor.

37. A system according to Claim 35 or 36, wherein the transaction code generating means is adapted to generate the transaction code in the form of an optical indictor, and preferably in the form of a bar code.

38. A system according to any of the preceding Claims 33 to 37, wherein the truncation code incorporates at least one of the following: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

39. A system according to any of the preceding Claims 35 to 38, wherein the mobile device further comprises means for reading the transaction code.

40. A system according to Claim 39, wherein the reading means is adapted to scan the transaction code.

41. A system according to Claim 39 or 40, wherein the mobile device further comprises a camera adapted to photograph the transaction code.

42. A system according to any of the preceding Claims 35 to 41, wherein the mobile device further comprises means for decoding the transaction code thereby to extract transaction information from the transaction code.

43. A system according to any of the preceding claims, wherein the processing terminal comprises means for displaying a confirmation receipt relating to a completed transaction.

44. A system according to any of the preceding claims, wherein the processing terminal comprises a user interface for enabling a user to manually enter a user code

into the terminal.

45. A system according to any of the preceding claims, wherein the mobile user device is in the form of a mobile telephone and/or a personal digital assistant, and preferably a smartphone.

46. A system according to any of the preceding claims, wherein the processing terminal is in the form of a point-of-sale (POS) terminal.

47. A system according to any of the preceding Claims 1 to 45, wherein the processing terminal is in the form of an internet-based or online merchant.

48. A system according to any of the preceding claims, wherein the system is in the form of a payment system.

49. A mobile device which is adapted to form part of the system according to any of the preceding claims.

50. A point-of-sale (POS) device adapted to form part of the system according to any of the preceding Claims 1 to 49.

51. A method of authorising a transaction using a mobile device, the method comprising: receiving information relating to a particular transaction from a transaction processing terminal; and generating a user code on the mobile device to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

52. A method of processing a transaction using a point-of-sale (POS) terminal, which comprises: generating a transaction code relating to a particular transaction, said code being adapted to be read by a mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

53. A mobile device (preferably in the form of a mobile telephone) which comprises software code adapted to carry out the method of Claim 51.

54. A point-of-sale terminal which comprises software code adapted to carry out the method of Claim 52.

55. A mobile device, which comprises means for receiving information relating to a particular transaction from a transaction processing terminal; and means for generating a user code on the mobile device to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

56. A point-of-sale (POS) terminal, which comprises means for generating a transaction code relating to a particular transaction, said code being adapted to be read by a mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

57. A method of authorising payment transactions by exchanging dynamically generated optical indicators, preferably in the form of bar codes, between a mobile user device and a transaction processing terminal.

58. A system substantially as herein described and/or as illustrated with reference to the accompanying drawings.

59. A method substantially as herein described and/or as illustrated with reference to the accompanying drawings.

60. A mobile device substantially as herein described and/or as illustrated with reference to the accompanying drawings.

61. A point-of-sale (POS) terminal substantially as herein described and/or as illustrated with reference to the accompanying drawings.

Application No:	GB1004246.3	**Examiner:**	Mr Stuart Purdy
Claims searched:	1-33, 35-48, 51, 53, 55, 58-61	**Date of search:**	20 June 2011

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-9, 15, 26, 27-29, 31-33, 35-51, 53, 55	US 2005/211771 A1 (ONOZU) See whole document and note in particular paras 18-24, 26, 29, 31, 41, 44, 144, 146:
X	1-33, 35-48, 51, 53, 55	US 2008/210754 A1 US 2008210754 A1 (LOVETT) See whole document and note in particular paras 8, 36-40, 53, 102, 103, 106, 108 and 111;
A	-	US 2008/222048 A (HIGGINS) See whole document;

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[X] :

Worldwide search of patent documents classified in the following areas of the IPC

G06Q; G07C; G07F

The following online and other databases have been used in the preparation of this search report

WPI & EPODOC

International Classification:

Subclass	Subgroup	Valid From
G06Q	0020/00	01/01/2006
G07C	0009/00	01/01/2006
G07F	0007/08	01/01/2006

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2007 (21.12.2007)

PCT

(10) International Publication Number
WO 2007/145687 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/US2007/004646

(22) International Filing Date:
21 February 2007 (21.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/812,279	9 June 2006 (09.06.2006)	US
60/775,046	21 February 2006 (21.02.2006)	US
60/859,235	15 November 2006 (15.11.2006)	US

(71) Applicant and
(72) Inventor: **WEISS, Kenneth, P.** [US/US]; 59 Sargent Street, Newton, MA 02458 (US).

(74) Agent: **DONAHOE, Robert, V.**; Lowrie, Lando & Anastasi, Llp, One Main Street, Suite 1100, Cambridge, MA 02142 (US).

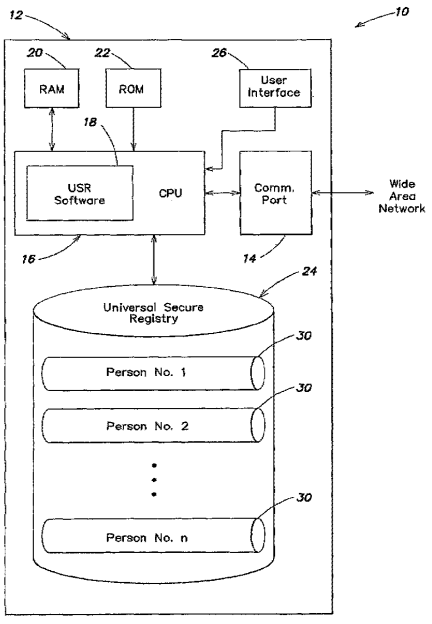
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) **Title:** METHOD AND APPARATUS FOR SECURE ACCESS PAYMENT AND IDENTIFICATION



(57) **Abstract:** According to one aspect, the invention provides a system for validating an identity of a user to enable or prevent an occurrence of an event. In one embodiment, the system includes a first device including a wireless transmitter which is configured to transmit validation information, a second device including a wireless receiver, where the second device is configured to receive the validation information and further transmit the validation information; and a secure system in communication with the second device. According to one embodiment, the secure system includes a database. In a further embodiment, the secure system is configured to receive the validation information transmitted from the second device, and to transmit additional information to the second device following a receipt of the validation information to assist the second device in either enabling or preventing the occurrence of the event.

WO 2007/145687 A1

IPR2025-01150
Apple EX1071 Page 1151

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR SECURE ACCESS PAYMENT AND IDENTIFICATION

BACKGROUND OF INVENTION

1. Field of Invention

Embodiments of the invention generally relate to systems, methods, and apparatus for authenticating identity or verifying the identity of individuals and other entities seeking access to certain privileges and for selectively granting privileges and providing other services in response to such identifications/verifications. In addition, embodiments of the invention relate generally to systems and methods for obtaining information from and/or transmitting information to a user device and, in particular, to systems, methods, and apparatus that provide for contactless information transmission.

2. Discussion of Related Art

Control of access to secure systems presents a problem related to the identification of a person. An individual may be provided access to the secure system after their identity is authorized. Generally, access control to secure computer networks is presently provided by an authentication scheme implemented, at least partly, in software located on a device being employed to access the secure computer network and on a server within the secure computer network. For example, if a corporation chooses to provide access control for their computer network, they may purchase authentication software that includes server-side software installed on a server in their computer system and corresponding client-side software that is installed on the devices that are used by employees to access the system. The devices may include desktop computers, laptop computers, and handheld computers (e.g., PDAs and the like).

In practice, the preceding approach has a number of disadvantages including both the difficulty and cost of maintaining the authentication system and the difficulty and cost of maintaining the security of the authentication system. More specifically, the software resides in the corporation's computers where it may be subject to tampering/unauthorized use by company employees. That is, the information technology team that manages the authentication system has access to the private keys associated with each of the authorized users. As a result, these individuals have an

opportunity to compromise the security of the system. Further, any modification and/or upgrade to the authentication system software is likely to require an update to at least the server-side software and may also require an update of the software located on each user/client device. In addition, where the company's computer systems are geographically distributed, software upgrades/updates may be required on a plurality of geographically distributed servers.

There is also a need, especially in this post September 11 environment, for secure and valid identification of an individual before allowing the individual access to highly secure areas. For example, an FBI agent or an air marshal may need to identify themselves to airport security or a gate agent, without compromising security. Typically such identification may comprise the air marshal or FBI agent showing identification indicia to appropriate personnel. However, there are inherent flaws in this process that allow for security to be compromised, including falsification of identification information and failure of the airport security or other personnel to not recognize the situation. Of course this process could be automated, for example, by equipping airport personnel or security with access to a database and requiring the FBI agent or air marshal to appropriately identify themselves to the database, for example, by again providing identification which airport personnel can then enter into the database to verify the identity of the person seeking access to a secure area. However, this process also has the inherent flaws in it as described above. In addition, there may be times when airport security or personnel may not be able to communicate with the database to check the identity of the person seeking access, for example, when they are not near a computer terminal with access to a database or are carrying a hand-held device that does not have an appropriate wireless signal to access the database. In addition, there is a need to ensure that if such a hand-held device ends up the wrong hands, that security is not compromised.

Systems capable of effectively performing all or some of these functions do not currently exist.

Further, both commercial (e.g., banking networks) and non-commercial (e.g., security systems) information systems often rely on magnetic card readers to collect information specific to a user (e.g., a security code, a credit card number, etc.) from a user device (e.g., a transaction card). Credit card purchases made in person provide an

example of the most common transaction-type that relies on a user device, the credit or debit card, which is read by a magnetic card reader. User devices that rely on magnetic-stripe based technology magnetically store information (e.g., binary information) in the magnetic stripe. The magnetic stripe reader provides an interface to a larger computerized network that receives the user's information to determine, for example, whether to authorize a transaction, to allow the user access to a secure area, etc.

Recently, such devices have seen technological advances that increase their capabilities and improve their security. For example, such devices may now include embedded processors, integral biometric sensors that sense one or more biometric feature (e.g., a fingerprint) of the user, and magnetic stripe emulators. As one result, today's user devices may provide greater security by dynamically generating the necessary information, for example, generating the credit card number at the time of a transaction. Improved security can also be provided by such devices because more sophisticated authentication schemes can be implemented with the devices.

In addition, user devices such as transaction cards may now also provide for one or more modes of information transmission other than transmission via a magnetic stripe/card reader combination. For example, user devices that may transmit information optically or via radio frequency ("RF") signal transmission to a compatible system interface are now available. Further, the architecture of a user device that includes a processor is generally compatible with both the improved security features described above and the contactless transmission modes such as optical and RF signal transmission. As a result of the improved security and greater functionality of some current user devices, there is a desire to replace magnetic-stripe based user devices with devices that include forms of information transmission other than the reading of a magnetic-stripe.

There is, however, a substantial installed base of interfaces (for example, at points of sale, at automatic teller machines ("ATM"), and the like) that include magnetic card readers which are not equipped to receive information from a user device in any other format other than from a magnetic stripe. As a result of the cost to replace or retrofit the installed base, efforts to more-widely introduce user devices that do not employ magnetic stripe devices have not been developed. Because of the potential to

substantially reduce fraud, however, the further implementation of such devices is of great interest to financial institutions among others. RF devices that transmit information wirelessly are expected to become much more prevalent and at some point, the predominant form of information transmission for user authentication based on a hand-held device, for example, credit card, debit card, drivers license, passport, social security card, personal identification, etc. Thus, new and improved methods for transitioning from a purely magnetic based form of communication to a wireless form of communication are desired.

One current approach that is intended to "transform" a smart card for use with a magnetic stripe card reader employs a "bridge" device. The bridge device requires that the smart card be inserted within it. The bridge device includes a slot for receiving the smart card, a key pad whereby the user may enter information (e.g., a PIN number), and a credit card sized extension member. Operation of the bridge device requires that the smart card be inserted within it and that an electrical contact surface of the smart card engage a similar surface within the bridge device before the bridge device (i.e., the extension member) can be used with a magnetic card reader. Thus, the contactless nature of more advanced information transmission systems is lost with the bridge device because it does not support wireless signal transmission.

SUMMARY OF INVENTION

There is thus a need for an identification system that will enable a person to be accurately identified ("identification" sometimes being used hereinafter to mean either identified or verified) and/or authenticated without compromising security, to gain access to secure systems and/or areas. Likewise, there is a need for an identification system that will enable a person to be identified universally without requiring the person to carry multiple forms of identification.

Accordingly, this invention relates, in one embodiment, to an information system that may be used as a universal identification system and/or used to selectively provide information about a person to authorized users. Transactions to and from a secure database may take place using a public key/private key security system to enable users of the system and the system itself to encrypt transaction information during the

transactions. Additionally, the private key/public key security system may be used to allow users to validate their identity. For example, in one embodiment, a smart card such as the Secure ID™ card from RSI Security, Inc. may be provided with the user's private key and the USR system's public key to enable the card to encrypt messages being sent to the USR system and to decrypt messages from the USR system 10.

The system or database of the invention may be used to identify the person in many situations, and thus may take the place of multiple conventional forms of identification. Additionally, the system may enable the user's identity to be confirmed or verified without providing any identifying information about the person to the entity requiring identification. This can be advantageous where the person suspects that providing identifying information may subject the identifying information to usurpation.

Access to the system may be by smart card, such as a Secure ID™ card, or any other secure access device. The technology enabling the user to present their identity information may be physically embodied as a separate identification device such as a smart ID card, or may be incorporated into another electronic device, such as a cell phone, pager, wrist watch, computer, personal digital assistant such as a Palm Pilot™, key fob, or other commonly available electronic device. The identity of the user possessing the identifying device may be verified at the point of use via any combination of a memorized PIN number or code, biometric identification such as a fingerprint, voice print, signature, iris or facial scan, or DNA analysis, or any other method of identifying the person possessing the device. If desired, the identifying device may also be provided with a picture of the person authorized to use the device to enhance security.

According to one embodiment of the invention, a method of controlling access to a plurality of secure computer networks using a secure registry system located remotely from the secure computer networks is disclosed. The secure registry system includes a database containing selected data of a plurality of users each authorized to access at least one of the plurality of secure computer networks. The method comprises acts of receiving authentication information from an entity at a secure computer network, communicating the authentication information to the secure registry system, and validating the authentication information at the secure registry system. The method

also includes receiving from the secure registry system an indication of whether the entity is authorized to access the secure computer network, granting the entity access to the secure computer network when the authentication information of the entity corresponds to one of the plurality of users, and denying the entity access to the secure computer network when the authentication information of the user does not correspond to one of the plurality of users.

Another embodiment of the invention comprises a method of controlling access to a secure computer network using a secure registry system. The secure registry system includes a database containing selected data of a plurality of users authorized to access the secure computer network and selected data identifying the secure computer network. The method comprises receiving an access request including authentication information and a computer network ID from an entity, determining whether the authentication information is valid for any of the plurality of users, accessing data when the authentication information of the entity is valid for one of the plurality of users to determine whether the entity is authorized to access the computer network identified by the computer network ID, and allowing the entity to access the secure computer network when the authentication information of the entity is valid for one of the plurality of users authorized to access the computer network identified by the computer network ID.

Another embodiment of the invention comprises a method of authenticating an identity of a first entity. The method comprises the acts of wirelessly transmitting from a first device, first encrypted authentication information of the first entity, receiving with a second device the wirelessly transmitted first encrypted authentication information, decrypting with the second device, the first wirelessly encrypted authentication information to provide the first authentication information of the first entity to the second device; and authenticating the identity of the first entity based upon the first authentication information; and acting based on the assessed identity of the first entity.

Another embodiment of the invention comprises a system for authenticating an identity of a first entity, comprising a first wireless device comprising a first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted authentication information, a first processor configured to compare stored

biometric data with detected biometric data of the first entity and configured to enable or disable use of the first device based on a result of the comparison, and configured to encrypt first authentication information with a first private key of the first entity into the first encrypted authentication information, a first biometric detector for detecting biometric data of the first entity, and a first memory for storing biometric data of the first entity, a private key of the first entity authorized to use the first device, and the first authentication information.

According to some embodiments, the system further comprises a second wireless device comprising a second wireless transmitter and receiver configured to receive the first wireless signal and to process the first wireless signal, a second processor configured to compare detected biometric data of a second entity with stored biometric data and configured to enable or disable use of the second device based upon a result of the comparison, and configured to decrypt the first authentication information received in the first wireless signal, a biometric detector for detecting biometric data of a second entity, and a second memory storing biometric data of the second entity and a plurality of public keys of a plurality of first entities.

Another embodiment of the invention provides a first wireless device comprising a processor configured to enable operation of the first wireless device if it receives an enablement signal validating first biometric information of a first entity and configured to generate a non-predictable signal from the biometric information, a first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted biometric information of the first entity and to receive the enablement signal, and a first biometric detector for detecting the first biometric information of the first entity.

In one aspect of the invention, a device converts a wireless transaction device to a magnetic-stripe emulator device. In one embodiment, the device includes a wireless signal receiver that is configured to receive a wireless signal and provide information from the wireless signal. In addition, the device may include a magnetic-stripe emulator which is communicatively coupled to the wireless signal receiver and adapted to provide a time-varying signal which emulates data provided by a magnetic-stripe card to a magnetic card reader in response to receiving the information from the wireless signal. In one embodiment, the device includes a processor communicatively

coupled to the wireless signal receiver and to the magnetic-stripe emulator. The device may also include an LED. In a version of this embodiment, the processor is configured to control the LED to indicate that the device is properly aligned with the magnetic card reader. In another embodiment, the device includes an output device that can provide information to a network or to a network device. In a version of this embodiment, the output device is a wireless transmitter device.

Further embodiments of the invention may include additional features, for example, in one embodiment the output device is a data port to which the device can provide data to a network or to a network device. In a version of this embodiment, the data port is also configured to receive data from the network or the network's device. In a further embodiment, the device is configured to communicate with the magnetic card reader via the data port.

In a further embodiment, the wireless receiver and/or processors configure, decrypt and encrypt the wireless signal. In a further embodiment, the processor is configured to determine whether a user is authorized to provide the information contained within the wireless signal from data within the wireless signal. In a version of this embodiment, the data contained within the wireless signal includes user ID information. In yet another embodiment, the data contained within the wireless signal includes biometric information of the user.

According to another aspect, the invention provides a system for validating an identity of a user to enable or prevent an occurrence of an event. In one embodiment, the system includes a first device including a wireless transmitter which is configured to transmit validation information, a second device including a wireless receiver, where the second device is configured to receive the validation information and further transmit the validation information; and a secure system in communication with the second device. According to one embodiment, the secure system includes a database. In a further embodiment, the secure system is configured to receive the validation information transmitted from the second device, and to transmit additional information to the second device following a receipt of the validation information to assist the second device in either enabling or preventing the occurrence of the event. In various embodiments, the event that is enabled or prevented may be a transaction (e.g., a

financial transaction), access control (e.g., physical or electronic access) or other action that is either enabled or prevented.

According to a further aspect, the invention provides a method employing a system to validate an identity of a user to enable or prevent an occurrence of an event. In one embodiment, the system includes a first device, a second device and a secure system including a database. According to one embodiment, the method includes acts of receiving at the second device validation information wirelessly transmitted from the first device, communicating the validation information from the second device to the secure system, and receiving at the second device additional information from the secure system. In a further embodiment, the additional information assists the second device in either enabling or preventing the occurrence of the event. In various embodiments, the event that is enabled or prevented may be a transaction (e.g., a financial transaction), access control (e.g., physical or electronic access) or other action that is either enabled or prevented.

BRIEF DESCRIPTION OF DRAWINGS

This invention is pointed out with particularity in the appended claims. The above and further advantages of this invention may be better understood by referring to the following description when taken in conjunction with the accompanying drawings. The accompanying drawings are not intended to be drawn to scale. In the drawings, each identical or nearly identical component that is illustrated in various figures is represented by a like numeral. For purposes of clarity, not every component may be labeled in every thawing. In the drawings:

FIG. 1 is a functional block diagram of a computer system configured to implement the universal secure registry ("USR"), including a USR database, according to one embodiment of the invention;

FIG. 2 is a functional block diagram of a first embodiment of a networked environment including the computer system of FIG. 1;

FIG. 3 is a functional block diagram of an entry of a database forming the USR database of FIG. 1;

FIG. 4 is a functional block diagram of a second embodiment of a networked environment including the computer system of FIG. 1;

FIG. 5 is a flow chart illustrating steps in a process of inputting data into the USR database;

FIG. 6 is a flow chart illustrating steps in a process of retrieving data from the USR database;

FIG. 7 is a flow chart illustrating a first protocol for purchasing goods from a merchant via the USR database without transmitting credit card information to the merchant;

FIG. 8 is a flow chart illustrating a second protocol for purchasing goods from a merchant via the USR database without transmitting credit card information to the merchant;

FIG. 9 is a flow chart illustrating a protocol for purchasing goods from a merchant via the USR database by validating the user's check;

FIG. 10 is a flow chart illustrating a protocol for purchasing goods from an on-line merchant via the USR database without transmitting credit card information to the on-line merchant, and enabling the on-line merchant to ship the goods to a virtual address;

FIG. 11 is a flow chart illustrating a protocol for shipping goods to a virtual address via the USR database;

FIG. 12 is a flow chart illustrating a protocol for telephoning a virtual phone number via the USR database;

FIG. 13 is a flow chart illustrating a protocol for identifying a person via the USR database;

FIG. 14 is a flow chart illustrating a protocol for identifying a person to a policeman via the USR database;

FIG. 15 is a flow chart illustrating a protocol for providing information to an authorized recipient of the information via the USR database;

FIG. 16 is a flow chart illustrating a protocol for providing application information to an authorized recipient of the information via the USR database;

FIG. 17 is a functional block diagram of an embodiment configured to use information in the USR system to activate or keep active property secured through the USR system; and

FIG. 18A is a functional block diagram of an embodiment configured to use the USR system to control access to a secure computer network;

FIG. 18B is a functional block diagram of another embodiment configured to use the USR system to control access to a secure computer network;

FIG. 19 is a flow diagram of a process for controlling access to a secure computer network with the USR system in accordance with an embodiment of the invention;

FIG. 20 is a flow diagram of a process for controlling access to a secure computer network with the USR system in accordance with another embodiment of the invention;

FIG. 21 illustrates an embodiment of a system for validating the identity of an individual;

FIGS. 22A and 22B illustrate one embodiment of a process for validating the identity of an individual;

FIG. 23 illustrates one embodiment of various fields included within a first wireless signal and a second wireless signal as transmitted by the system of FIG. 21;

FIG. 24 illustrates one embodiment of a process for verifying or authenticating the identity of a first user of a first wireless transmission device;

FIG. 25 illustrates another embodiment of a process for authenticating the identity of a first user of a wireless transmission device;

FIG. 26 illustrates still another embodiment of a process for authenticating the identity of a first user of a wireless transmission device; and

FIG. 27 illustrates one embodiment of a data structure that can be used by any wireless device of the system of FIG. 21;

FIG. 28 illustrates a system in accordance with one embodiment of the invention;

FIG. 29 illustrates a process in accordance with an embodiment of the invention; and

FIGS. 30A-30D illustrate a converter device in accordance with one embodiment of the invention.

DETAILED DESCRIPTION

This invention is not limited in its application to the details of construction and the arrangement of components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced or of being carried out in various ways. Also, the phraseology and terminology used herein is for the purpose of description and should not be regarded as limiting. The use of "including," "comprising," or "having," "containing", "involving", and variations thereof herein, is meant to encompass the items listed thereafter and equivalents thereof as well as additional items.

In one embodiment, an information system is formed as a computer program running on a computer or group of computers configured to provide a universal secure registry (USR) system. The computer, in this instance, may be configured to run autonomously (without the intervention of a human operator), or may require intervention or approval for all, a selected subset, or particular classes of transactions. The invention is not limited to the disclosed embodiments, and may take on many different forms depending on the particular requirements of the information system, the type of information being exchanged, and the type of computer equipment employed. An information system according to this invention, may optionally, but need not necessarily, perform functions additional to those described herein, and the invention is not limited to a computer system performing solely the described functions.

In the embodiment shown in FIG. 1, a computer system 10 for implementing a USR system according to the invention includes at least one main unit 12 connected to a wide area network, such as the Internet, via a communications port 14. The main unit 12 may include one or more processors (CPU 16) running USR software 18 configured to implement the USR system functionality discussed in greater detail below. The CPU 16 may be connected to a memory system including one or more memory devices, such as a random access memory system RAM 20, a read only memory system ROM 22, and one or more databases 24. In the illustrated embodiment, the database 24 contains a universal secure registry database. The invention is not limited to this particular manner of storing the USR database. Rather, the USR database may be included in any aspect of the memory system, such as in RAM 20, ROM 22 or disc, and may also be separately stored on one or more dedicated data servers.

The computer system may be a general purpose computer system which is programmable using a computer programming language, such as C, C++, Java, or other language, such as a scripting language or even assembly language. The computer system may also be specially programmed, special purpose hardware, an application specific integrated circuit (ASIC) or a hybrid system including both special purpose components and programmed general purpose components.

In a general purpose computer system, the processor is typically a commercially available microprocessor, such as Pentium series processor available from Intel, or other similar commercially available device. Such a microprocessor executes a program called an operating system, such as UNIX, Linux, Windows NT, Windows 95, 98, or 2000, or any other commercially available operating system, which controls the execution of other computer programs and provides scheduling, debugging, input/output control, accounting, compilation, storage assignment, data management, memory management, communication control and related services, and many other functions. The processor and operating system defines a computer platform for which application programs in high-level programming languages are written.

The database 24 may be any kind of database, including a relational database, object-oriented database, unstructured database, or other database. Example relational databases include Oracle 81 from Oracle Corporation of Redwood City, California; Informix Dynamic Server from Informix Software, Inc. of Menlo Park, California; DB2 from International Business Machines of Armonk, New York; and Access from Microsoft Corporation of Redmond, Washington. An example object-oriented database is ObjectStore from Object Design of Burlington, Massachusetts. An example of an unstructured database is Notes from the Lotus Corporation, of Cambridge, Massachusetts. A database also may be constructed using a flat file system, for example by using files with character-delimited fields, such as in early versions of dBASE, now known as Visual dBASE from Inprise Corp. of Scotts Valley, California, formerly Borland International Corp.

The main unit 12 may optionally include or be connected to an user interface 26 containing, for example, one or more input and output devices to enable an operator to interface with the USR system 10. Illustrative input devices include a keyboard, keypad, track ball, mouse, pen and tablet, communication device, and data input

devices such as voice and other audio and video capture devices. Illustrative output devices include cathode ray tube (CRT) displays, liquid crystal displays (LCD) and other video output devices, printers, communication devices such as modems, storage devices such as a disk or tape, and audio or video output devices. Optionally, the user interface 26 may be omitted, in which case the operator may communicate with the USR system 10 in a networked fashion via the communication port 14. It should be understood that the invention is not limited to any particular manner of interfacing an operator with the USR system.

It also should be understood that the invention is not limited to a particular computer platform, particular processor, or particular high-level programming language. Additionally, the computer system may be a multiprocessor computer system or may include multiple computers connected over a computer network. It further should be understood that each module or step shown in the accompanying figures and the substeps or subparts shown in the remaining figures may correspond to separate modules of a computer program, or may be separate computer programs. Such modules may be operable on separate computers. The data produced by these components may be stored in a memory system or transmitted between computer systems.

Such a system may be implemented in software, hardware, or firmware, or any combination thereof. The various elements of the information system disclosed herein, either individually or in combination, may be implemented as a computer program product, such as USR software 18, tangibly embodied in a machine-readable storage device for execution by the computer processor 16. Various steps of the process may be performed by the computer processor 16 executing the program 18 tangibly embodied on a computer-readable medium to perform functions by operating on input and generating output. Computer programming languages suitable for implementing such a system include procedural programming languages, object-oriented programming languages, and combinations of the two.

As shown in FIG. 2, the computer system 10 may be connected to a plurality of interface centers 27 over a wide area network 28. The wide area network 28 may be formed from a plurality of dedicated connections between the interface centers 27 and the computer system 10, or may take place, in whole or in part, over a public network

such as the Internet. Communication between the interface centers 27 and the computer system 10 may take place according to any protocol, such as TCP/IP, ftp, OFX, or XML, and may include any desired level of interaction between the interface centers 27 and the computer system 10. To enhance security, especially where communication takes place over a publicly accessible network such as the Internet, communications facilitating or relating to transmission of data from/to the USR database 24 or the computer system 10 may be encrypted using an encryption algorithm, such as PGP, DES, or other conventional symmetric or asymmetric encryption algorithm.

In one embodiment, the USR system 10 or USR database 24 may be able to authenticate its identity to a user or other entity accessing the system by providing an appropriate code which may be displayed on the user's smart card, for example a SecurID™ card or its equivalent, or other code generator, for example a single use code generator, being employed by the user. A comparison by the user or the code generator between the provided number and an expected number can validate, to the user (or other entity) or the code generator, that communication is with the database and not an imposter. In another embodiment, a challenge-response protocol is employed to authenticate the identity of the USR system and/or the user to the other.

The database 24 shown in FIG. 1 has a USR database containing entries related to persons 1-n. The data in the USR database may also be segregated, as shown in FIG. 4, according to data type to enable individual computer modules to handle discrete applications on discrete data types. Segregating the data, as illustrated in FIG. 4, may make access to the database more robust by enabling portions of the data in the USR database 24 to be accessible even when it is necessary to perform maintenance on a portion of the database. However, storing the data in the USR database 24 according to the scheme illustrated in FIG. 1 may make it easier for a user of the database to make changes to multiple types of data simultaneously or in a single session. There are advantages and disadvantages to each data structure, and the invention is not limited to a particular manner of organizing the data within the database 24, data structures other than the two shown also being possible.

As shown in FIG. 3, each entry 30 in the database 24 may contain multiple types of information. For example, in the embodiment shown in FIG. 3, the entry

contains validation information 32, access information 34, publicly available information 36, address information 38, credit card and other financial information 40, medical information 42, job application information 44, and tax information 46. The invention is not limited to a USR containing entries with all of this information or only this particular information, as any information on a person or other entity such as a company, institution, etc. may be stored in USR database 24.

If the database information is split between multiple databases, each database will typically include at least the validation and access information to enable the USR software to correlate a validation attempt with a verified validation, and to enable the USR software to determine access privileges to the requested data. Alternatively, databases may be linked to permit information not in a main USR database to be retrieved, with validation/identification for all databases accessed being done at the USR system.

In FIG. 3, the validation information is information about the user of the database to whom the data pertains and is to be used by the USR software 18 to validate that the person attempting to access the information is the person to whom the data pertains or is otherwise authorized to receive it. The validation information may be any type of information that will reliably authenticate the identity of the individual. For example, in some embodiments, the information may include any of a secret known by the user (e.g., a pin, a phrase, a password, etc.), a token possessed by the user that is difficult to counterfeit (e.g., a secure discrete microchip), and/or a measurement such as a biometric (e.g., a voiceprint, a fingerprint, DNA, a retinal image, a photograph, etc.).

The user's identifying information may be manually entered or scanned at the interface center. However, a variety of types of communication may be employed to communicate the user's identifying information from the identification card or token to the computer system. For example, near field signal may be employed to communicate information between the identification card or token and the computer system 10. According to one embodiment, the user's identifying information is included in (or entered via) the user's cell phone where it is then communicated to the computer system 10. In one embodiment, the cell phone is also configured to receive information from the computer system 10 at the interface center 27.

In one embodiment, the user of the database will carry a SecurID™ card available from RSA Security, formerly Security Dynamics Technologies, Inc., of Cambridge, MA. Use of this card enables secure access to the USR database without requiring the user to transmit any personal information. Specifically, to access the USR database, the card retrieves a secret user code and/or time varying value from memory and obtains from the user a secret personal identification code. The card mathematically combines these three numbers using a predetermined algorithm to generate a one-time nonpredictable code which is transmitted to the computer system 10. The computer system, specifically USR software 18, utilizes the received one-time nonpredictable code to determine if the user is authorized access to the USR database and grants access to the USR database if the user is determined to be authorized. The verification information 32 in the database entry in the embodiment of the invention illustrated in FIG. 3 contains information to enable the USR software 18 to validate the user using such a card in this manner.

Alternative types of identification cards or tokens may likewise be used. For example, other smart cards may be used which generate non-predictable single use codes, which may or may not be time varying, or other access code generators may be used. An algorithm generating such non-predictable codes may also be programmed onto a processor on a smart card or other computing device, such as a cell phone, pager, ID badge, wrist watch, computer, personal digital assistant, key fob, or other commonly available electronic device. For convenience, the term "electronic ID device" will be used generically to refer to any type of electronic device that may be used to obtain access to the USR database.

Likewise, various types of biometric information may be stored in the verification area of the database entry to enable the identity of the user possessing the identifying device to be verified at the point of use. Examples of the type of biometric information that may be used in this situation includes a personal identification number (PIN), fingerprint, voice print, signature, iris or facial scan, or DNA analysis. If desired, the verifying section of the database may contain a picture to be transmitted back to the person seeking to validate the device to ensure the person using the device is the correct person. Optionally, the identifying device itself may also be provided

with a picture of the person authorized to use the card to provide a facial confirmation of the person's right to use the card.

Further, a challenge-response protocol may be employed in combination with or as an alternative to the preceding to validate the person attempting to access the information. Various embodiments may employ a challenge-response protocol with or without an identification card.

In FIG. 3, the Access information 34 is provided to enable different levels of security to attach to different types of information stored in the entry 30 in the USR database 14. For example, the person may desire that their address information be made available only to certain classes of people, for example colleagues, friends, family, Federal Express, U.P.S., and the U.S. mail service. The names or universal identifiers for those selected individuals, companies, organizations and/or agencies may be entered into appropriate fields in the Access information to specify to the USR software 18 those individuals to whom the address information may be released. Likewise, access fields may be specified for the other types of information. For example, the individual may specify that only particular individuals and/or companies have access to the credit card and other financial information 40, medical information 42, job application information 44 and tax information 46. Additionally, the individual may specify that no one have access to that information unless the individual participates in the transaction (see FIG. 6).

As shown in FIG. 1, the USR software 18 contains algorithms for execution by the CPU 16 that enables the CPU 16 to perform the methods and functions of the USR software described below in connection with Figs. 5-16. The USR software 18, in this embodiment, performs all functions associated with validating an electronic ID card. If desired, a separate validation software module may be provided to validate electronic ID devices outside of a firewall segregating the validation information from other user information.

This algorithm comprising the USR software 18 may be used to implement, in one exemplary embodiment, a USR system configured to enable selected information to be disseminated to selected individuals in a secure and dynamic fashion. This information may be used for numerous purposes, several of which are set forth below and discussed in greater detail in connection with Figs. 5-16.

For example, the USR system may be used to identify the person, enable the person to be contacted by telephone or mail anonymously, enable the person to be contacted by telephone or by mail without revealing the person's telephone number or present location, enable the person to purchase items over the Internet or in a store without revealing to the merchant any personal identification information or credit card information, enable the person to complete a job application without completing a job application form, enable the police to discern the person's identity and any outstanding warrants on the individual, and numerous other uses. The invention is not limited to these several enumerated uses, but rather extends to any use of the USR database. The methods of using the USR database 24 will now be discussed in connection with Figs. 5-16.

FIG. 5 illustrates a method of training the USR database 24. As shown in FIG. 5, the USR software 18 first validates the person's identification (500). The initial validation of the person's identification (500) may take place at the point of sale of an electronic ID device (for example, a smart card). This may be done in any conventional manner, such as by requiring the person to show a government issued identification card, passport, birth certificate, etc. Once the person's electronic ID device has been issued and initially validated, the validation process proceeds as discussed above.

After the validation process (500), the USR software 18 determines if the person has rights to enter data into the system (502). This step enables the system to charge persons for maintaining information in the USR database 24. For example, the USR software 18 may poll a database of current accounts or a database of accounts that are currently in default to determine if the person has paid the access fee to enter data into the database. A similar account status inquiry process may be performed by the USR software 18 in connection with each of the other methods set forth in Figs. 6-16. If the person is not authorized to enter data into the USR database 24, the person is notified of the status of their account and the process returns (512) to wait for further input from another person. Alternatively, a person may be permitted to enter some classes of data into the system and update such classes of data at no charge, with a fee possibly being required for other classes of data, for example medical records. This would facilitate a more robust database.

If the person is authorized, the USR software 18 then enables the person to enter basic personal data into the USR database 24 (504). Optionally, personal data may be one class of data the USR software 18 allows the person to enter into the USR database 18 regardless of account status, i.e., for free.

The USR software 18 will then check to see if the person has additional rights to enter additional data (506), such as data to be entered into one of the other categories of data in FIG. 3. Optionally, this step of checking the person's rights to enter data (506) may be combined with the initial check (502). If the person does not have rights to enter any further data, the USR software 18 notifies the user and returns (512).

If the USR software 18 determines that the person has the right to enter additional data into the USR database 24, the person is prompted through the use of appropriate prompts, provided with forms, and otherwise enabled to enter advanced personal data into the USR database 24 (508). For each type of data entered, the person is asked to specify the type of access restrictions and/or whom should be allowed to access the advanced personal data (510). When the person has completed entering data into the database, the process returns (512) and commits the data to the database.

In the situation where only one person has access to enter and/or modify data for a given person in the database, there should be no conflict with committing data to the database. If, however, multiple people have access to a given account to modify data, the database may perform an integrity check to ensure the absence of conflict in the data before committing the new data to the database.

Enabling access to the information in the database will be explained in greater detail in connection with FIG. 6. As shown in FIG. 6, the database will generally allow anyone to access basic personal data on anyone without performing any authorization check (600).

If information beyond that specified in the basic personal information area is requested, the USR software 18 queries whether the requestor has the right to access the type of requested data (602). The process of determining the requestor's rights (602) typically involves validating the requestor's identity and correlating the identity, the requested information and the access information 34 provided by the person to the USR database during the training process described above with respect to FIG. 5.

If the USR software 18 determines that the requestor has rights to access the type of requested data (604), the USR software 18 instructs the USR database 24 to enable access to the type of requested data (606). The actual step of enabling access to the type of requested data may involve multiple steps of formulating a database query, querying the USR database 24, retrieving the results, assembling the results into a user friendly or user readable format, and transmitting the information to the user.

If the USR software 18 determines that the requestor does not have the appropriate rights to access the type of requested data (604), the USR software 18 checks to see if the person is participating in the transaction (608). Checking to see if the person is participating in the transaction enables the user to authorize access to the requested data in real time. For example, a person may wish to participate in a transaction to give a potential employer one-time access to job application information 44 (see FIG. 3). If the person is not participating in the transaction, the USR software 18 determines that the requestor is not authorized to have access to the requested data, notifies the requestor of this determination, and ends (610).

If the person is participating in the transaction (608), however, the USR software 18 validates the person's identity (612) and enables the person to change access rights to the data (614). If the USR software 18 is not able to validate the person's identity, the USR software 18 refuses to allow the person to update the database, notifies the person and/or requestor of this determination, and returns (610).

It is also possible that a person may be required to grant access to certain data, for example financial data such as account numbers, under duress. The system may provide the person with the ability to safely signal this when accessing the system by using a selected access code or by making a known modification to the access code provided by the electronic ID device. On receiving such code, the system would take appropriate steps to protect the person, including for example alerting the police, tracking the person's location to the extent possible, providing traceable data, and the like.

Once the person has had the opportunity to change access rights to the data (614), the USR software 18 again checks to see if the requestor has rights to access the type of requested data (616). Although step 616 may seem redundant, given the fact that the person is participating in the transaction and has just previously changed access

rights to the database to enable the requestor to have access to the data, step 616 is actually useful at preventing a different type of fraud. Specifically, the requestor may not be forthright with the person regarding the type of information they are requesting. If step 616 were omitted, the USR software 18 may inadvertently allow access to an unauthorized type of information in the situation where the requestor has surreptitiously requested multiple types of data.

If the USR software 18 determines that the requestor has rights to the type of data requested (616), it causes the USR database to enable access to the type of requested data (606). Otherwise, it notifies the requestor of the decision to deny access to the requested data and returns (610).

Various applications of the USR database 24 and USR software 18 will now be discussed in connection with Figs. 7-16. These applications are merely exemplary of the types of applications enabled by the USR software 18 and USR database 24, and the invention is not limited to these particular applications.

Figure 7 illustrates one embodiment of a method of using the USR software 18 and USR database 24 to purchase goods or services from a merchant without revealing to the merchant account information relating to the person's bank or credit card.

As shown in FIG. 7, when a user initiates a purchase (700), the user enters a secret code in the user's electronic ID device (702) to cause the ID device to generate a onetime code or other appropriate code, and presents the electronic ID device with the code to the merchant or otherwise presents the code to the merchant. The merchant transmits to the credit card company (1) the code from the electronic ID device, (2) the store number, (3) the amount of the purchase (704), and the time of receipt of the code. The credit card company takes this information and passes the code from the electronic ID device to the USR software 18 (706). The USR software 18 determines if the code is valid, or was valid at the time offered, and if valid accesses the user's credit card information and transmits the appropriate credit card number to the credit card company (708). While the link between the USR system and the credit card system is a secure link, there is always a danger that the link may be penetrated and credit card numbers obtained. This may be avoided by instead transmitting, on approval, a multidigit public ID code for the credit card holder which the credit card company can map to the correct credit card number. Even if the link is violated, the public ID code is

of no value and the secure link prevents this code from being improperly sent to the credit card company. The credit card company checks the credit worthiness of the user and declines the card or debits the user's account in accordance with its standard transaction processing system (710). The credit card company then notifies the merchant of the result of the transaction (712). In this embodiment, the user has been able to purchase goods or services from a merchant without ever providing to the merchant the credit card number. Since the electronic ID device generates a time variant code or otherwise generates a code that can for example only be used for a single transaction, the merchant retains no information from the transaction that may be fraudulently used in subsequent transactions.

Another embodiment of a system for facilitating purchase of goods or services without providing financial information to the merchant is set forth in FIG. 8. In FIG. 8, like FIG. 7, the user initiates a purchase (800), enters a secret code in the electronic ID device (802) and presents the resultant code to the merchant. The merchant, in this embodiment, transmits to the USR software 18, (1) the code from the electronic ID, (2) the store number, and (3) the amount of the purchase (804). The USR software 18 determines if the code is valid (806) and, if valid, accesses from the USR database 24 the user's credit card information (808). The USR software then transmits to the credit card company (1) the credit card number, (2) the store number, and (3) the amount of purchase (808). The information in this embodiment transmitted to the credit card company is intended to be in a format recognizable to the credit card company. Accordingly, the invention is not limited to transferring from the USR system 10 to the credit card company the enumerated information, but rather encompasses any transfer of information that will enable the use of the USR system 10 to appear transparent to the credit card company.

The credit card company then processes the transaction in a standard fashion, such as by checking the credit worthiness of the person, declining the card or debiting the user's account and transferring money to the merchant's account (810). The credit card company then notifies the USR system 10 the result of the transaction (812) and the USR software 18 in turn notifies the merchant of the result of the transaction (814).

In this embodiment, like the embodiment of FIG. 7, the user can use the USR system 10 to purchase goods or services from a merchant without providing the

merchant with the user's credit card number. In the embodiment of FIG. 8, the interposition of the USR system 10 between the merchant and the credit card company is transparent to the credit card company and thus requires no or minimal cooperation from the credit card company to implement.

FIG. 9 illustrates one embodiment of a method of using the USR system 10 to verify funds when using a check to purchase goods or services from a merchant. In the embodiment of FIG. 9, the user initiates a purchase and writes a check to the merchant (900). The check may be a conventional check containing identifying information, or may be a check bearing a unique serial number and no identifying information to enable the check to be used anonymously.

In either situation, the user enters a secret code into the electronic ID card and presents the resulting code to the merchant along with the check (902). The merchant transmits to the USR software 18 (1) the code from the electronic ID card, (2) the store number, and (3) the amount of the purchase (904). Where the check is an anonymous check, the merchant also transmits to the USR software 18 the check number.

The USR software 18 then determines if the code from the electronic ID is valid (906), and if valid accesses the user's bank information and transmits to the bank: (1) the user's bank account number, (2) the store number, and (3) the amount of the purchase (908). Optionally, the USR software 18 may additionally inform the bank of the check number.

The bank polls its own database to determine if there are sufficient funds in the user's account (910) and notifies the USR software 18 of the result (912). The USR software 18 then, in turn, notifies the merchant of the result of the verification (914).

This check verification system may take place over an unsecured connection between the merchant and the USR system 10 since the user's bank account information is not sent over the connection between the merchant and the USR system 10. Moreover, where an anonymous check is used, the merchant is not even provided with the person's name or account information in written form. This provides additional security against unauthorized persons writing subsequent checks.

The check verification system may be conducted over a telephone network, such as by having the merchant call a toll free number or over a network connection such as over the Internet.

FIG. 10 illustrates a method of conducting a transaction with a merchant without requiring the user to provide to the merchant the user's name, address, or other identifying information, while enabling the merchant to ship the goods to the user. This may be beneficially employed, for example, in connection with transactions that take place between remote parties in a networked environment, such as the Internet.

As shown in FIG. 10, the user initiates an anonymous purchase by entering a secret code into the electronic ID device and transmitting the result to the on-line merchant (1000). The merchant transmits this information to the USR software 18, along with the store number and the amount of the purchase (1002). Optionally, the merchant may provide the store number and purchase price to the user and the user may send this information directly to the USR software 18 along with the code from the electronic ID. Where the number from the electronic ID device is a time varying number, the merchant may also need to input the time the number was received. Alternatively, the electronic ID device may encode or encrypt the time with the number, the USR software being able to extract time when receiving the number from the merchant. This may not be required where the time varying number varies slowly, for example changing every hour rather then every minute as for some existing such devices.

In either event, the USR software 18 determines if the code is valid (1004) and, if valid, accesses the user's credit card information from the USR database 24 (1006). The USR software 18 then contacts the user's credit card company, as described above in connection with FIG. 8 (1008) and notifies the USR software 18 of the result (1010).

If the user's credit is declined, the USR software 18 notifies the on-line merchant and the transaction is terminated (1012). If the user's credit is honored, the USR software 18 polls the USR database 24 for the user's address and/or address code (1014). Address codes are discussed below in greater detail with reference to FIG. 11. The merchant then packages the goods into a parcel, labels the parcel with the appropriate address and/or address code and ships the parcel to the user (1016). Having the USR system 10 provide the address and/or address code to the on-line merchant enables the user to purchase items in a networked environment without requiring the user to input address information in connection with every sale.

RECTIFIED SHEET (RULE 91)
ISA/EP

IPR2025-01150
Apple EX1071 Page 1177

FIG. 11 illustrates a use of the USR database 24 to deliver mail to a user without requiring the user to provide address information to the sender. This may be useful in many contexts. For example, the user may wish that the address information be known only by the post office. In this instance, using the USR database 24 according to the method of the invention described below, will enable the user to receive parcels without requiring the user to provide the merchant with the address information. Additionally, the user's address may change, temporarily, permanently, or frequently. Enabling the sender to send mail by entering a code instead of an address enables the post office to effectively deliver the coded mail to the corresponding address regardless of the frequency with which the address changes or the duration in which the address will remain valid.

In FIG. 11, the user provides an address code on a public area of the USR database 24 that is available to all persons to see (1100). This code may for example be six alpha characters, which should be adequate for currently anticipated system populations. Optionally, the user may provide this code directly to a merchant or other person desirous of sending the person one or more parcels.

The user also provides address information to the address information area 38 of the user's entry in the USR database 24 (1102). Access to the address information 38 is restricted by a rule or other appropriate entry in the access information 34 of the user's entry to only permit mail, parcel or other material delivery services, such as the US mail, UPS and Fed Ex to access the address information.

When someone wishes to have a parcel or other items delivered to the user, the sender retrieves the user's address code from the USR database 24 or otherwise receives the address code from the user, and prints the address code on the parcel (1104).

The delivery service accesses the USR software 18, validates its identity, and queries the USR database 24 for address information corresponding to the address code (1106). The USR database 24 retrieves the appropriate address data and provides the address information to the delivery service. The delivery service then either prints out an address label, prints a machine readable bar code to be attached to the package, or correlates an entry in a delivery database between the address code and the user address (1110). The delivery service then uses this retrieved information to deliver the package

to the user while never supplying the merchant with the user's permanent or temporary address. A user may also assure that mail, parcels, etc. are delivered to a current location by providing only a single notice to the USR system, regardless of how frequently the person moves. The person can also automatically provide for address changes where the person moves according to a known schedule. Thus, deliveries to be made on a weekday could be directed to one address and deliveries on a weekend to another address; or deliveries during winter months to one address and during summer months to a different address.

FIG. 12 illustrates a method of enabling a person to telephone a user of the USR system 10 without providing the user's telephone number to the person. In the embodiment illustrated in FIG. 12, the user provides a telephone code on the publicly available area of his entry on the USR database 24 (1200). This code may be assigned by the USR software 18 or made up by the user. The user also provides the USR database 24 with actual telephone information to enable the USR system 10 to connect callers with the user (1202).

The person wishing to telephone the user of the USR system 10 calls a telephone number and enters the telephone code of the user (1204). The USR software 18, optionally, may require the person to identify themselves to see if they are authorized to call the user. Assuming that the person is authorized to call the person, or if no authorization check is performed, the USR connects the person to the telephone number in the USR database 24 without providing the person with the telephone number.

Enabling the user to specify the telephone number may be advantageous for many reasons. First, the user may frequently be switching between telephone coverage areas and may wish to be reachable at all times. Simply by instructing the USR database 24 to connect incoming telephone calls to one of a myriad of numbers will facilitate connecting the incoming calls to, for example, the user's cell phone, work phone, pager, car phone or home phone, without necessitating the user to provide all these numbers to the caller. A similar system may be implemented for facsimile transmissions, e-mails or other communications.

The user also may have predefined rules to enable telephone calls to follow a set pattern. For example, the user may desire to receive telephone calls only from family

members during the night time at home, may wish to have all incoming calls routed to a car phone during commuting hours, and may wish to have all incoming calls routed to a cell phone during lunch. These time dependent rules may and/or caller specific rules may be entered into the USR database to specify accessibility and connectivity of incoming telephone calls.

The publicly available address code and telephone code and any other codes may be the same, or may be different, there being some advantages to having a single code usable for all such applications for each person on the system. The codes could be accessible through a variety of media including telephone and the Internet. Where two or more people on the system have the same name, which will frequently be the case, additional publicly available biographical data may be provided with the name to assure that the right code is selected. The system may similarly be used to provide public keys for use in a public key/private key encryption system, to provide other public codes for an individual or to provide other public information. Access to such information would typically be unrestricted.

Where the system is used to provide public keys, the public code used to obtain the key, or possibly the public key itself, may be used as above to obtain the e-mail address, telephone number or the like for the person to whom the message is being sent, and the USR system may also be used to perform the encryption. When the recipient receives the message, he deencrypts it using the recipient's private key in standard fashion, including deencrypting the name of the sender. However, this does not necessarily verify the sender and such verification may be desirable for important messages, particularly ones involving large financial transactions. The USR system may accomplish such verification by also storing private keys for people in the system. The sender first authenticates himself to the system, and the system then adds a second signature to the message which is encrypted with the sender's private key. The receiving party deencrypts this signature with the sender's public key. Since the system only sends such signatures for authenticated users, the message is thus verified.

FIG. 13 illustrates a general method of using the USR database 24 to authenticate a user's identification. This may be used in connection with any of the other methods disclosed herein to ensure that the electronic ID device has not been stolen and/or hacked by an unauthorized holder.

Specifically, in the embodiment illustrated in FIG. 13, the user attempts to prove identification to a validator, such as to prove that the possessor of the electronic ID device is of sufficient age to purchase alcohol (1300). In connection with this attempt, the user enters a secret code into the electronic ID (1302). The validator transmits to the USR software 18 the code from the electronic ID (1304). If the USR software 18 determines that the code is valid (1306), it accesses the user's photograph, age information, or any other desired information, and transmits that information to the validator (1308). By transmitting back to the validator a picture of the person to whom the electronic ID card was issued, the validator can ensure that the person using the electronic ID card is the proper person. Likewise, the validator can ensure, based on the information provided by the USR system 10, that the person is as old as the person claims to be.

A specific embodiment of this identification validation procedure is illustrated in FIG. 14. In FIG. 14, a policeman takes the place of the validator. In this scenario, however, instead of simply transmitting to the policeman a validation of the user's identity, such as their picture, the policeman may also receive additional information, such as the user's police records, records of any arrests, outstanding warrants, and other similar information that may be of use to the policeman when determining how to handle a particular individual.

FIG. 15 illustrates a process for enabling the user to provide specific information to a party, such as medical staff in an emergency room. As shown in FIG. 15, if the user desires to provide information to a party (1500), the user enters a secret code in the electronic ID device and provides the electronic ID code to the party (1502). The party transmits to the USR software 18 the ID code and the party code (1504). The party code may be a code from for example an electronic device which identifies the party, may be a status code which identifies the class of users to which the party belongs, for example policeman, emergency room personnel, doctor, etc. or may be a combination of both, the status code for example being encrypted into the ID code. The USR software 18 determines if the code is valid (1506), accesses the user's information in the USR database 24 and transmits available information to the party (1508). In this scenario, the user may be provided with a plurality of different codes to enter into the electronic ID device depending on the type of information to be released

to the party. For example, the user's basic code may be 1234. The fifth digit of the electronic code may specify the type of information to be provided, i.e., 1 = address information, 2 = medical information; 3 = telephone information, 4 = job application information, etc. Using multiple codes eliminates any ambiguity about the authority provided by the user to the party, but requires the user to remember additional information.

The above assumes the user is able to provide an ID code when the information is required. However, in for example an emergency room situation, the user may not be in a position to provide the ID code, but would still want medical records provided. The release authorization for certain portions of the user's database could therefore specify that the information be released to certain class or classes of individuals and the USR system would release such information to individuals or organizations based only on status code. Thus, the status code of an emergency room could alone trigger release of medical data.

FIG. 16 illustrates one embodiment of a method of using the USR database 24 to complete a standard application, such as a job application or an application to rent an apartment. This embodiment is a specific example of the more generic method of enabling a party to retrieve information discussed above with respect to FIG. 15. In FIG. 16, however, the party may be provided with the opportunity to provide a form to the USR software 18, the fields of which may be automatically completed with information from the job application information section of the USR database 24.

As can be seen from the above, many of the users of the USR system are organizations or agencies such as carriers (post office, UPS, FedEx), communication companies, law enforcement organizations, hospitals and other medical facilities and the like. Each of these organizations can be provided with specialized software either on a disc or other suitable media or electronically, for example over the Internet, which performs a number of functions, for example automatically generating status codes for data access requests, controlling information received, and formatting data received in response to a request in a desired way. This can result in an access request from such organization for a given user causing all data on the user required to complete the form being retrieved and presented to the organization in the format of their form. A user may also authorize an organization for which a form has been completed using the USR

system to receive updates, either in response to a request from the organization or at selected intervals, for example once a year, so as to maintain information in the forms current. Since the user will be providing information to the system on a regular basis, this is a relatively easy and painless way for the user to maintain current information with many organizations the user deals with.

Another potential use of the system is to permit a person to be located where only limited biographical information on the person is known. Users of the USR system wishing to participate in this feature could be cued to provide non-confidential biographical data when they come on the system or at any time thereafter when they decide to participate. They can also indicate whether they wish their name given out in response to such an inquiry or to merely be alerted to an inquiry which might involve them and information on the requester. A person seeking to find another person or group of people can input appropriate biographical data, for example members of 1975 Harvard University hockey team, or information of a person's last known address plus school information, etc. The system will then provide a list of persons who meet the listed criteria from which the person making the inquiry can hopefully find the person they are looking for.

In the above application and others, when a person is located, the person may request that only the person's address code or general access code (i.e. a single code which is used to get current address, telephone, e-mail, etc. information) be provided when the person is located. This can further protect the individual from undesired contacts.

Further, although each of FIGS. 13-16 refer to the entry of a secret code for validation by the USR system, the processes illustrated for each of FIGS. 13-16 may include a challenge-response protocol by which the user's identity is authenticated.

FIG. 17 illustrates another embodiment of the invention. As shown in FIG. 17, the USR system 10 may be used to secure expensive personal equipment, such as stereos, televisions, laptop computers, cellular telephones, cars, boats, and other items of value to a person. In this embodiment, each item to be secured using the USR system is provided with a USR timer chip imbedded in the electronics. If the USR timer chip is not provided with a code within a predefined period of time, for example every 30 days, the equipment is deactivated. Thus, for example, a television, mobile

phone, laptop computer, automobile, heavy equipment, weapon or facility may be provided with a security chip having an internal timer that must be reset before expiration by provision of a particular code. When reset does not occur, the timer will disable the electronic device or other device using any one of a number of known disablement methods. Exemplary codes may be transmitted in the same manner as beeper signals are conventionally transmitted or may be transmitted to wired devices over the Internet or other public network.

The USR system 10 may be advantageously employed to automatically provide the secured property with the necessary codes at appropriate intervals, unless instructed by the user of the USR system 10 to cease doing so. Alternatively, the USR system 10 may require participation by the user prior to sending out the activation codes.

In this embodiment, the user may provide to the USR system 10, information indicative of the codes to be transmitted, timing information, and automation information -- i.e., whether the codes should be sent automatically or should require user intervention. Optionally, where the user opts to require user intervention, the USR system 10 may notify the user of the upcoming deadline via e-mail or another method.

This system may be useful to secure sensitive equipment other than personal equipment as well, such as military equipment, public equipment, school equipment and any other equipment that is subject to theft.

FIG. 18A illustrates another embodiment of the invention that can provide a centralized system to control access to a plurality of secure networks. As shown in FIG. 18A, for example, a system 1800 may employ the USR 10 to control access to a plurality of secure systems 1804 (e.g., a plurality of secure computer networks). The system 1800 may include one or more access devices 1802 that can be employed by a user to access a secure computer network included in the plurality of secure systems. In addition, the system 1800 may be employed to protect other secure systems such as secure communication networks and/or other resources that are accessed electronically. According to one embodiment, the system 1800 includes a first communication link 1801 that provides a communication path between the access device 1802 and the USR 10, and a second communication link 1803 that provides a communication path between the USR 10 and the plurality of secure system 1804. In one embodiment, each

IPR2025-01150
Apple EX1071 Page 1184

of the first communication link 1801 and the second communication link 1803 are wide area networks, for example, the Internet.

Each of the secure systems 1804 can be associated with an organization. An organization is any entity that employs a secure (e.g., restricted access) host system to provide resources to a plurality of users. For example, an organization may be a corporation (including a non-profit corporation), partnership, other business entity, an affiliation or individual that employs a secure host system to provide resources to a plurality of authorized users. As should be apparent to those of ordinary skill in the art, an organization is not restricted to any particular size, for example, as measured by the number of members or employees.

More specifically, each of the secure systems No. 1, No. 2, No. 3, etc. may be associated with a different organization and the USR 10 may control access to each of the secure systems. That is, the USR 10 can provide access control for a plurality of secure computer networks each associated with a different and unrelated organization. Further, each of the secure computer networks may have a different plurality of users who are authorized to access the network.

The access device may include any of a desktop computer, a laptop computer, and a handheld computer (e.g., a PDA, call phone and the like). Further, as shown in phantom, a plurality of access devices may communicate with the USR 10. Where a web-based system is employed, for example, each of a plurality of computers connected to the Internet may be individually employed as a separate access device to communicate (e.g., independently communicate) with the USR 10 to gain access to one or more of the secure systems 1804.

For example, the access device 1802 may be a computer employed with a client-server network. In this example, to access resources provided by one of the secure system 1804, the user initiates an access request for a secure system 1804 selected by the user. That is, the user may supply authentication information and a computer network ID to the USR. As is described in further detail below, the authentication information and the computer network ID are processed by the USR to authenticate the user and determine whether the user is authorized to access the secure system 1804 that is identified by the computer network ID. The USR then routes

communications between the user and the secure system provided that the user authentication is successfully completed.

According to one embodiment, the USR 10 connects the access device 1802 to one of the secure systems 1804 via a communication path that does not include the USR 10. In an alternate embodiment, the USR 10 connects the access device 1802 to one of the secure system 1804 via a communication path that does include the USR.

Referring now to FIG. 18B, a system 1810 employs a USR 10 to control access to a secure system (e.g., a secure computer network) according to another embodiment. In one embodiment, the system 1810 includes the USR 10, an access device 1802, and a plurality of secure system 1804. According to this embodiment, the user selects from the plurality of secure systems 1804 a secure system that the user would like to access. With the access device 1802, the user communicates authentication information directly to the selected secure system 1804, e.g., without gaining access to the system. The secure system then communicates the authentication information and/or information corresponding to the authentication information to the USR 10. The USR 10 processes the information received from the secure system and then communicates an indication of whether the authentication information corresponds to one of the plurality of users authorized to access the secure system. The secure system grants or denies access to the secure system (and the associated resources) based on the indication received from the USR 10.

As illustrated in Figs. 18A and 18B, the USR 10 can provide a centralized access control system (e.g., an authentication system) for a plurality of secure systems 1804 that are associated with independent organizations that may have no affiliation with one another. Referring to Figs. 18A and 18B, a first organization may be associated with (have resources located on and/or accessed by) the secure system no. 1, a second organization may be associated with the secure system no. 2, and so on. In addition, a single organization may also be associated with a plurality of the secure systems 1804. Thus, in one embodiment, the USR 10 provides access control to a plurality of secure systems for a single organization.

The systems 1800 and 1810 allow an organization to operate a secure system without hosting the authentication system software or at least without the need to host a substantial part of authentication system software. Thus, in one embodiment, software

upgrades/maintenance can be implemented at the USR 10 (e.g., centrally) for the plurality of secure systems 1804 and specialized authentication software is not required at the access device. In a further embodiment, specialized authentication software is also not required at the secure system. In versions of these embodiments, the USR 10 provides a web-based system in which the user employs a web-browser when communicating with the USR 10 and the secure system.

The USR 10 can also provide centralized administration and management for the plurality of secure systems 1804. The centralized administration can include routine tasks such as adding or removing authorized users for each of the plurality of secure systems 1804, for example, based on the hiring or resignation, respectively, of an employee. Additional administrative functions such as maintaining a secure database of private keys associated with each user, generating time varying codes, maintaining encryption software, maintaining audit trails and other functions may also be accomplished in a centralized fashion with the USR 10 for a plurality of organizations.

In one embodiment, following the connection of the access device 1802 to the secure system 1804, the USR 10 develops an audit trail by monitoring the communication path to capture information concerning the use of the secure system. For example, the USR 10 may collect and store information concerning the length of time during which the access device remains connected to the secure system, the type of resources accessed by the user, the type of data transmitted (including the identification of specific documents) during a login period and the volume of data transmitted.

According to one embodiment, the USR continuously monitors the communication between a plurality of access devices 1802 and a secure computer network and collects information to generate an audit trail for each device. According to another embodiment, the USR does not continuously monitor communications. Instead, the secure computer network intermittently (e.g., periodically) transmits audit information to the USR 10 where the audit information may concern one or a plurality of users connected to the network during a specific time period.

In each of the embodiments, described with reference to FIGS. 18A and 18B, the USR 10 may be located in an ultra-secure facility that employs heightened security

relative to the security provided by the organizations that it serves. The physical facility where the USR is located may meet requirements generally associated with critical military installations. For example, the USR 10 may be housed in a facility that is hardened against radiation, shielded against electromagnetic interference, and/or protected against earthquakes, hurricanes, etc. to allow operation of the USR during times of general emergency. Further, the personnel and hiring policies of the facility operating the USR 10 may also be more secure relative to the security measures taken by the organizations associated with the secure systems 1804. That is, the individuals operating the USR 10 may undergo more rigorous background checks that include a detailed investigation of their personal and employment histories.

The centralized approach described above can provide increased security because the administration of the access control system (e.g., authentication software) is in the hands of a highly trusted third party who has taken heightened security measures regarding the hiring of the administrative personnel, in particular, the personnel who have access to authentication data (e.g., private encryption keys, etc.).

In any of the preceding embodiments, the USR 10 may be geographically remote from the secure systems.

Further, in any of the preceding embodiments, there may be situations where a user employs the access device 1802 to connect to more than one of the plurality of secure systems 1804. In one embodiment, the user is independently authorized to access separate secure systems 1804 associated with independent organizations. In another embodiment, the user is authorized to access separate secure systems 1804 each associated with the same organization. In either situation, the user may employ one or more of the authentication procedures described herein before being allowed access to any one of the secure systems 1804.

Referring now to FIG. 19, a process 1900 that employs a USR to control access to a secure computer network is illustrated. In one embodiment, the process 1900 is employed with the system 1800 illustrated in FIG. 18A. At step 1902 an entity initiates an access request. In general, the access request will be initiated when the user or entity inputs information into an access device such as a computer. At stage 1904, the entity supplies authentication information and a computer network ID to the USR (e.g., the information is electronically transmitted from the access device to the USR).

According to one embodiment, the information is transmitted via the Internet from the access device to the USR. At stage 1906, the USR receives the access request which includes the authentication information and the computer network ID. At stage 1908, the USR determines whether the authentication information is valid for a user. According to one embodiment, the USR includes a database containing selected data of a plurality of users authorized to access a secure computer network, and may compare the authentication information supplied by the entity with authentication information included in the database to determine whether the authentication information corresponds or is valid for a user. If the authentication information is valid, the process 1900 moves to stage 1910 where the USR determines whether the entity is authorized to access the computer network identified by the computer network ID. If the entity is authorized to access the computer network then the USR may allow communication between the entity and the secure computer network at stage 1912. As previously indicated, the USR may route communications between the entity and the secure computer network and remain in the communication path employed by the access device to communicate with the secure computer network. Alternatively, the USR may simply provide a connection between the access device and the secure computer network where the communication path provided by the connection does not involve the USR.

Returning to stage 1908 if the authentication information supplied by the entity is not valid for any of the plurality of users then the process 1900 moves to stage 1914 where an indication is provided to the entity that access is denied. Similarly, if at stage 1910 the entity is not authorized to access the computer network identified by the computer network ID, an indication is provided that the entity is denied access at stage 1914. In various embodiments, the entity may be allowed additional opportunities to successfully access the system.

Referring now to FIG. 20, a process 2000 for controlling access to a secure computer network is illustrated in accordance with one embodiment. In one embodiment, the process 2000 is employed with the system 1810 illustrated in FIG. 18B.

In one embodiment the entity initiates an access request at stage 2002. As described above, the access request can be initiated using an access device and each

secure computer network may communicate with a plurality of access devices. At stage 2004, the entity supplies authentication information to the secure computer network, for example, by entering the information in a web browser and transmitting the authentication information over the Internet to the secure computer network. At stage 2006, the secure computer network receives the authentication information. At stage 2008, the secure computer network communicates authentication information to the USR (or information corresponding to the authentication information) to allow the USR to authenticate the access request. At stage 2010, the USR validates the authentication information to determine whether the entity is authorized to access the secure system, and at stage 2014, the secure system receives an indication from the USR concerning whether the entity is authorized to access the system. In one embodiment, the indication is transmitted from the USR to the secure system via the Internet. At stage 2016, the secure system grants or denies the entity access to the secure system based on the indication received from the USR.

As should be recognized by those of ordinary skill, the processes 1900 and 2000 can be accomplished in a variety of stages that may include any of the stages described above in various combinations and sequences including one or more of the stages described above in combination with one or more additional stages.

Various embodiments can be employed to control access to a physical facility. That is, an electronic device (e.g., a keypad, a card reader, a biometric scanner, etc.) or combination of electronic devices can be located at an access point to a secure area (e.g., a door, a gate, etc.). The entity initiates the request using the electronic device. In one embodiment, the physical facility includes all or a portion of the secure computer network. Thus, in one embodiment, the secure system receives an indication of whether an entity is authorized to access a physical facility. The secure system communicates authentication information to the USR. The USR validates the authentication information and communicates an indication of whether the entity is authorized to access the physical facility. The secure system receives the indication and grants or denies the entity access to the physical facility.

Each of the embodiments described with reference to any FIGS. 18-20, may include a challenge-response protocol, for example, to authenticate the identity of the entity and/or the USR system to the other.

FIG. 21 illustrates an embodiment of a system 2100 for validating the identity of an individual or an entity. The system includes a first wireless device 2110 and a second wireless device 2112. The first wireless device 2110 comprises a first wireless transmitter and receiver 2114, a first processor 2116 and a first memory 2118. Similarly, the second wireless device 2112 comprises a second wireless transmitter and receiver 2120, a second processor 2122 and a second memory 2124. According to aspects of the invention, the first wireless device and the second wireless device are configured to wirelessly communicate with each other so that the entity associated with the first wireless device can communicate his identity to the entity associated with the second wireless device. It is to be appreciated that the first wireless transmitter and the second wireless transmitter can be configured to communicate by any form of a wireless signal such as low power Bluetooth signal, infrared signals, RF signals and electromagnetic signals in general. In accordance with one embodiment, the first wireless device and the second wireless device communicate via near field signal.

The first wireless device can also comprise user interface 2126 that allows the first entity to interact with the first wireless device and can also comprise a display, such as a LCD display, 2128 that allows the first entity to further interact with the first wireless device. In accordance with some embodiments the invention, the first wireless device can be configured so that the first entity must enter a PIN identification number, for example, via the user interface to gain access to the wireless device. Alternatively, or in addition, the first wireless device may comprise a biometric sensor or detector 2130 that enable the first entity to present biometric data to the first wireless device to gain access to the first wireless device. For example, the biometric sensor can be configured to detect a fingerprint of the first entity. For such embodiment, the memory 2118 also comprises stored biometric data of the first entity, which is compared, for example, by the processor 2116 with the detected biometric data to determine whether the first entity is enabled or should be disabled from using the first wireless device. It is also to be appreciated that the biometric data need not be fingerprint data and can be any biometric data known to those of skill in the art, and that the biometric sensor need not be a fingerprint sensor and can be any biometric sensor known to those of skill in the art.

RECTIFIED SHEET (RULE 91)
ISA/EP

Similarly, the second wireless device 2112 can also be configured as discussed above with respect to the first wireless device, namely with any or all of a user interface 2132, a display 2134 and a biometric sensor 2136 and can be configured to require any and/or all of a second entity to provide a PIN number, or the second wireless device to match biometric information of the second entity with stored biometric information to enable or disable the second entity to gain access to the second wireless device. Each of the first wireless device 2110 and the second wireless device 2112 comprise a power source or a power source interface 2138, 2140 that can be coupled to a power source that provides power to respective devices. It is to be appreciated that the power source can be any power source, such as, alkaline batteries, rechargeable batteries, proprietary power sources, and interfaces to power sources such as standard 120 VAC, or an AC to DC conversion device, as well as any other type of power source known to those of skilled in the art. In addition, it is to be appreciated that each of the first wireless device 2110 and the second wireless device 2112 can also comprise an additional wireless transmitter and receiver device 2142, 2144, respectively, which enable each of these devices to communicate wirelessly via other wireless communication systems such as, via any cell phone standard, via satellite communications, over wireless area networks, local area networks, wide area networks, as well as any other wireless communication standard know to those of skill in the art.

According to some embodiments of the system 2100 of FIG. 21, either or both of the first wireless device 2110 and the second wireless device 2112 can be configured to communicate with a secure database 2146, as will be discussed in further detail herein. According to some embodiments, either of the first or second wireless devices may communicate with the secure database on a periodic basis to update it's corresponding data, or to stay alive as will be discussed herein, or to retrieve information in the secure database that is used in the communication protocol between the first and second wireless devices to verify the identity of at least the first entity. Accordingly, it is to be appreciated that communication with a secure database can be, for example, via the additional respective wireless transmitters and receivers 2142, 2144 of the first and second wireless devices, or can be via a network interface 2152, 2154 of the respective devices, that communicate with a network 2148 and to the secure database 2146.

Referring now to FIG. 22, there is illustrated one embodiment of an overall communication process that occurs with the system 2100 of FIG. 21. In particular, the process is effected by the system of FIG. 1 so as to identify and authenticate the identity of the first user associated with the first wireless device 2110 to the second user associated with the second wireless device 2112. For example, consider the situation where an air marshal or an FBI agent is carrying the first wireless device 2110 and airport security or security personnel generally want to ensure the identity of the user of the device 2110. The communication protocol 200 illustrated in FIG. 22 is one embodiment of a protocol that enables secure authentication of the first user of the wireless device 2110.

According to one embodiment of the process, the first user of the first wireless device 2110 first authenticates his or herself to the wireless device 2110, for example as has been discussed above, by either entering a PIN via the user interface 2126 of the first wireless device or by interacting with the biometric sensor of the first wireless device at step 202. In various embodiments, a challenge-response protocol is employed in which the first user supplies information (a biometric, a PIN or other information) to authenticate his or herself to the wireless device 2110. If the user of the device does not enter the correct PIN number or does not match the biometric data stored in memory 2118 of the first authorized user of the device, then the device at a minimum shuts down at step 204. However, according to some embodiments, the device 2110 can also be configured to automatically delete any portion of or all of the data stored in memory 2118 at step 206. In addition, as will be discussed in further detail herein, according to some aspects of the invention, the first wireless device can be configured to periodically communicate with the secure database 2146 to remain alive, for example, after the first user of the first device authenticates itself to the first device. If the first device does not communicate with the secure database at such periodic intervals at step 208, then the first device can be configured to delete any or a portion of the data stored in memory at step 206.

The communication protocol also comprises a second user of the second device to authenticate his or herself to the second device at step 210. It is to be appreciated that the authentication by the second device of the second user by any of the mechanisms discussed herein and above with respect to the first wireless device,

including entering a PIN number to the user interface 2132 of the second wireless device or by interacting with the biometric sensor 2136 of the second wireless device. In addition, it is to be appreciated that as discussed above with respect to the first wireless device, if such identification is not successful, the second wireless device will at a minimum shut itself down at step 212. However, it is also to be appreciated that the second wireless device can be configured to automatically delete a portion of or all of the data stored in the memory 2124 of the second wireless device, should such authentication not be successful at step 214. In addition, it is to be appreciated that the second wireless device can also be configured at step 216 to communicate with the secure database 2146 within defined periods of time, or even a periodic interval once the second user authenticates himself to the second wireless device, and to delete a portion of or all of the data in memory 2124 should such periodic communication not occur.

If both the first user and the second user are successful in authenticating themselves to the first and second wireless devices respectively, then a communication protocol is initiated between the first wireless device 2110 and the second wireless device 2112 at step 218. If the communication protocol is not a valid communication protocol between the devices, the devices wait until there is a valid communication protocol. If the communication protocol is a valid protocol (218 yes), then the first wireless device transmits a first wireless signal containing encrypted authentication information of the first user to the second wireless device 2112 at step 220. The details of the communication protocol and the encrypted authentication information will be discussed further herein.

The second wireless device 2112 receives the first wireless signal and processes the wireless signal to determine the identity of the first user. In particular, as will be discussed herein, according to some aspects of the invention, the authentication of the first user includes displaying a picture of the first user to the second user on the display 2134 of the second wireless device as a result of the communication from the first wireless device to the second wireless device. The user of the second wireless device can view the picture on the display and ascertain whether the first user of the first wireless device is who he or she purports to be. However, as will also be discussed herein, it is to be appreciated that the second wireless device need not be a device that

requires a user to interact with it and can be, for example, an unmanned detection system that receives the first encrypted authentication information and determines from the first authenticated encrypted information whether the first user is authorized to gain access to a secured place, a secure network, or a secure computer, to do whatever the first person is seeking to do. If the first user is not who they purport to be, the communication process goes back to looking for a valid communication protocol. In addition, the process allows the second user or the system associated with the second wireless device to take an appropriate action such as denying access to the secure site at step 224.

If the user of the first wireless device is authenticated (at step 222 yes), then according to some aspects of the invention, the communication process allows for the second wireless device to transmit a second wireless signal comprising encrypted authentication information of the second user to the first wireless device at step 226. In addition, according to such aspects, the communication protocol and the first wireless device are configured to authenticate the identity of the second user to the first user at step 228. It is to be appreciated that the authentication of the second user to the first user can be in any of the manners discussed above with respect to the authentication of the first user of the first device, such as by viewing a picture of the second user as provided on the display 2128 of the first wireless device, by matching one-time information contained in the encrypted authentication information or via a challenge-response protocol.

In addition, according to some embodiments of the protocol, either or both of the first wireless device 2110 and the second wireless device 2112 may communicate with the secure database 2146 to retrieve additional information at step 230. Such information, as will be discussed herein, can include for example, a portion of the biographic data of the first user of the first wireless device or of the second user of the second wireless device, or full biometric information of the first user or the second user, which can be communicated back to the respective device and used by the respective device to authenticate the user. In addition, the information can be periodic updates as provided the secure database to the respective device, such as will be described herein, including periodic updates of public keys of a plurality of first users as stored in memory on the second wireless device, or updates to public keys of a

plurality of second users as stored in memory on the first wireless device. In addition, such information may include periodic updates of the biometric information of a plurality of first users as stored on the second wireless device or a plurality of second users as stored on the first wireless device, which can comprise for example a portion of the biometric information or all of the biometric information.

Referring now to FIG. 23, there is illustrated one embodiment of various fields included within the first wireless signal and the second wireless signal as transmitted between the first wireless device and the second wireless device. According to some embodiments, the signal comprises a header field 302. The header field can be any header field known to those of skill in the art. In addition, the signal comprises a public ID field 304, which can comprise, for example, any of name information, a badge number, an employee number, an e-mail address, a social security number, and the like, of the first user. In addition, the first wireless signal may also include a digital signature field 306 containing a digital signature of the first user. For example, the digital signature may be generated with the user's private PKI key. Further, the first wireless signal may comprise a one-time time varying code field 308 that includes a random code as generated by the first wireless device. According to some embodiments, the digital signature field and the one-time code field can be used, for example by the second wireless device, to allow access to a secure place without the need for a user of the second wireless device to interact with the second wireless device to authenticate the first user. As an example, referring to FIG. 24, the digital signature and one time code can be encrypted with the private key of the first user and transmitted to the second wireless device. The second wireless device can decrypt the digital signature and one time code with the public key of the first user at steps 402-404 to authenticate or not the first user at step 406.

In addition, referring back to FIG. 23, the first wireless signal also comprises a PKI encrypted one-time DES key field 310 comprising a PKI encrypted one-time DES key. Further, the first wireless signal comprises a DES key encrypted biometric data field 312, which includes at least a portion of biometric data of the first user encrypted with the DES key. As will be discussed in further detail herein, according to some aspects of the invention, the public key of a first user, for example, stored in memory 24 of the second wireless device can be used to decrypt the DES key, and the DES key

can be used to decrypt at least a portion of the biometric data of the first user to use in the authentication of the identity of the first user. According to some embodiments, the first wireless signal can also comprise another ID data field 314, which can contain other information such as name, height, weight, eye color or anything else.

It is to be appreciated that although the embodiment of the wireless signal discussed in FIG. 23 has been discussed with reference to the first wireless signal transmitted from the first wireless device 2110 of FIG. 21 to the second wireless 2112, that the same protocol can be used when transmitting a second wireless signal from the second wireless device 2112 to the first wireless device 2110 to authenticate the identity of the user of the second wireless device to the user of the first wireless device. It is to be further appreciated that various fields of the signal can be used and not all of the fields of the wireless signal are needed to authenticate identity of the user.

Referring now to FIG. 24, there is illustrated one embodiment of a process 400 as identified by act 222 in FIG. 22 for verifying or authenticating the identity of the first user of the first device. According to this embodiment, which has been briefly discussed herein with respect to FIG. 23, the second wireless device can verify the identity of the respondent without necessarily interacting with a second user by decrypting the first user's digital signature from the digital signature field 306 at step 402 and verifying that it is the digital signature of the first user, decrypting the one-time code from the one-time code field 308 at step 404, and using this information at step 406 to authenticate the first user. If the first user is authenticated at 406, an appropriate action such as allowing access to the secure site, or computer, or network can be granted.

Referring now to FIG. 25 there is illustrated another embodiment of a process 520 for authenticating the identity of the first user at step 222 of the communication process of FIG. 22. According to aspects of the invention, the second wireless device at step 522 receives the first wireless signal and extracts the PKI encrypted DES key from field 310. The wireless device looks up the public key of the first user from memory 2124 [See FIG. 21] or from a secure server based on the information provided in the public ID field 304 at step 524. The second wireless device uses the first public key to decrypt the PKI encrypted DES key at step 526. The second wireless device acts on the DES key encrypted biometric information from the field 312 and uses the

IPR2025-01150
Apple EX1071 Page 1197

decrypted DES key to decrypt the at least a portion of the biometric information of the first user as included in the first wireless signal at step 528.

According to some embodiments, the biometric information included in the first wireless signal is a portion of the biometric information of the first user and the second wireless device is configured to store a remainder of the biometric information of the first user in memory. According to such embodiments, the process 520 also comprises looking up the remainder of the biometric information stored in the memory at step 530 and combining the remainder of the biometric information with the decrypted and extracted biometric information to provide complete biometric information of the first user at step 532. According to some aspects of the invention, the biometric information can comprise a digital image of the first user and for such aspects, the digital image can be displayed on display 2134 of the second wireless device so that the second user can ascertain whether the first user associated with the first device is who he or she purports to be. However, it is to also be appreciated that the biometric information can be fingerprint information, a voiceprint, DNA codes of the first user, or any other biometric information known and used by those of skill in the art. Accordingly, the processor 2122 of device 2112 can also be configured to process the combined biometric information to authenticate the first user at step 536.

Referring now to FIG. 26, there is illustrated another embodiment of a process 620 that can be used to authenticate the identity of the first user at step 222 of the process 200 of FIG. 22. According to this embodiment, some of the steps are similar to the steps of the process 520 illustrated in FIG. 25 and accordingly a full description of these steps will not be herein duplicated. It is to be appreciated that this embodiment can be used for example, where the biometric information of the plurality of first users is not stored on the second wireless device 2112 but is instead stored at the secure database 2146 as illustrated in FIG. 21. In particular, for highly secure applications, where there is a worry that the second wireless device can be compromised (even with the necessity to authenticate the second user to the second wireless device), the second wireless device can be configured to interact with the secure database to obtain at least a portion of the biometric information of the first user, rather than storing at least a portion of the biometric information of the first user in memory on the second wireless device.

According to such embodiments, the second wireless device can receive the first wireless signal including the fields discussed above in respect to FIG. 23, in particular, the public ID field 304 and optionally the PKI encrypted DES key. According to some embodiments, the PKI encrypted DES key may be used by this process. At step 624, the second wireless device accesses public key information of the first user from the public keys stored in memory on the second wireless device. However, it is to be appreciated that in some embodiments, the public keys may not be stored on the second wireless device and for such embodiments, the second wireless device will communicate with the secure database to obtain the public key of the first user also at step 624. According to some embodiments, at step 626 the second wireless device transmits a signal to the secure database comprising public identification number to identify the second device to the secure database, presumably after the second user of the second device has authenticated his or herself to the second device. For such embodiments, at step 628, the secure database determines whether the second device is authorized to access the secure database at step 628. It is to be appreciated that according to some embodiments, this communication between the second wireless device and the secure database can be accomplished with encrypted signals and in some embodiments the encrypted signals can include using time varying one time codes to further secure the communication. If the second device is authorized to interact with the secure database, the process also comprises transmitting the first public ID from the second wireless device 2112 to the secure database at step 630, and with this information, the secure database accesses the biometric or identification information of the first user at step 632. The biometric or the at least a portion of the biometric information can then be transmitted by the secure database to the second wireless device at step 634. Again, this transmission can be encrypted and further include time varying or one time codes to further secure the communication. The second wireless device can use the received portion of the first biometric information and combine it with portion of the first biometric information provided in the first wireless signal, or can receive all of the first biometric information as provided by the secure database and, for example, display it on the display 2134 of the second wireless device 2112 at step 636, or can process the biometric or identification information at step 638 to determine whether the first user is authenticated.

RECTIFIED SHEET (RULE 91)
ISA/EP

IPR2025-01150
Apple EX1071 Page 1199

Referring now to FIG. 27 there is illustrated one embodiment of a data structure 720 that can comprise memory 2124 of the second wireless device 2112. It is to be appreciated that any or all of the various portions of this data structure can be present in the memory 2124. According to some aspects of the invention, the memory will include the private key of the second user at field 722. The private key can be used, for example, when communicating by the second wireless device to the first wireless device to provide a digital signature of the second entity encrypted with the second user's private PKI key to the first user. In addition, the memory can also comprise a plurality of public keys of a plurality of first users at area 724. Such public keys of a plurality of first users can be used as has been discussed herein in combination with the private key of the first user to decrypt information of the first user. For example, the public and private key can be used to decrypt the DES key of the first user. In addition, the memory can also comprise at least a portion of biometric data of a plurality of first users, at area 726. As been discussed herein, the at least a portion of the biometric data of the plurality of first users can be combined with the portion of the biometric data provided in the first wireless signal or from the secure database, to create the complete biometric data of the first user for ascertaining or authenticating the identity of the first user as has been described herein. In addition, the memory can also comprise biometric data of the second user at field 728. The biometric information of the second user can be used, for example, as has been discussed herein to compare the biometric data detected by the biometric sensor 2136 of the second wireless device to determine whether the second user is authorized to have access to the second wireless device. It is to be appreciated that the data structure 720 of FIG. 27 can also comprise the memory 2118 of the first wireless device 2110, and that any or all of the fields of the data structure 720 can exist in the memory 2118 in the first wireless device. It is also to be appreciated that the first wireless device can access the data structure 720 and the various fields for the same purposes as discussed above with respect to the second wireless device, namely, to provide the first digital signature of the first entity encrypted with the first private key in the first wireless signal, to access the public keys of a plurality of second users for the purpose of decrypting information provided in the second wireless signal, to access at least a portion of biometric information of the second user stored in the field 726, as well as to compare biometric information of the

IPR2025-01150
Apple EX1071 Page 1200

first user with sensed biometric data provided by the biometric sensor 2130 of the first wireless device.

In one embodiment, the method comprises acts of receiving first authentication information about the first entity with the first device, transmitting the authentication information about the first entity to a secure database, determining whether or not the first entity is allowed to access the first device based on the first authentication information, and transmitting an enablement signal to the first device indicating to enable nor not enable the first entity to access the first device. According to a further embodiment, the method also includes an act of allowing or not allowing operation of the first device based on the enablement signal. In another embodiment, the act of receiving the first authentication information of the first entity comprises receiving biometric information of the first entity by detecting the biometric information with the first device.

In yet another embodiment, the act of transmitting the first authentication information about the first entity to a secure database comprises generating a non-predictable signal from the biometric information. In a further embodiment, the act of generating the non-predictable signal from the biometric information comprises generating a time varying non-predictable signal from the biometric information. In a still further embodiment, the act of receiving biometric information of the first entity comprises receiving a voice signature of the first entity with the first device and the act of generating the non-predictable signal from the biometric information comprises mixing the voice signature of the first entity with a random code to generate the non-predictable signal. In yet a further embodiment, the act of transmitting the enablement signal to the first device comprises sending the random code to the first device. In a still further embodiment, the act of receiving biometric information of the first entity comprises receiving fingerprint data of the first entity with the first device and the act of generating the non-predictable signal from the biometric information comprises mixing the fingerprint data of the first entity with a random code to generate the non-predictable signal. In another embodiment, the act of transmitting the enablement signal to the first device comprises sending the random code to the first device.

In a further embodiment, the act of authenticating the biometric of the first entity comprises authenticating a voice signature of the first entity. In another

embodiment, the act of authenticating the biometric information of the first entity comprises authenticating a finger print of the first entity.

In one embodiment, a first wireless device includes a biometric detector comprising a fingerprint detector that detects a fingerprint of the first entity. In an alternate embodiment, the biometric detector comprises a voice signature that detects a voice signature of the first entity.

According to one embodiment, the system comprises a first wireless device including a processor configured to enable operation of the first wireless device if it receives an enablement signal validating first biometric information of a first entity and configured to generate a non-predictable signal from the biometric information, a first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted biometric information of the first entity and to receive the enablement signal, a first biometric detector for detecting the first biometric information of the first entity and a secure database configured receive the first wireless signal, to authenticate or not authenticate the first biometric information of the first entity, and to provide the enablement signal validating or not validating the first biometric data of the first entity.

In a further embodiment, the secure database further comprises biometric data of a plurality of first entities. In another embodiment, the processor is configured to generate the non-predictable signal from the biometric information by generating a time varying non-predictable signal from the biometric information. In a still further embodiment, the processor is configured to generate the non-predictable signal from the biometric information by mixing the biometric information of the first entity with a random code to generate the non-predictable signal. In yet another embodiment, the secure database is configured to transmit the enablement signal to the first device including the random code so as to authenticate the secure database to the first device. In still another embodiment, the system includes a memory for storing a private key of the first entity authorized to use the first device.

It should be understood that various changes and modifications of the embodiments shown in the drawings and described in the specification may be made within the spirit and scope of the present invention. Accordingly, it is intended that all matter contained in the above description and shown in the accompanying drawings be

interpreted in an illustrative and not in a limiting sense. The invention is limited only as defined in the following claims and the equivalents thereto.

FIG. 28 illustrates an embodiment of a system 100 that employs a converter device 102 to provide an interface between a user device 104 (e.g., a transaction card, a cell phone, etc.) and a system interface 106 where, for example, the system interface 106 employs a magnetic card reader and the user device 104 is not equipped with a magnetic stripe. That is, in one embodiment, the converter device 102 provides a mode of information transmission between the user device 102 and the system interface 106 which would otherwise be unavailable to the user device 102. The converter device 102 provides a modified system 100 that provides compatibility with a greater variety of user devices, for example, user devices such as transaction cards, cell phones or PDAs that are not equipped with a magnetic stripe. For example, in one embodiment, the converter device 102 includes a magnetic stripe emulator 137 communicatively coupled to a wireless signal receiver 140 and adapted to provide a time-varying signal emulating data provided by a magnetic stripe card to a magnetic card reader 152.

The user device need not be a "card" and may, for example, take the form of a fob used as a key ring, a cell phone, a watch, a personal digital assistant or any device that can include a wireless transmitter, or a magnetic stripe emulator.

In various embodiments, the user device 104 employs near field signal to communicate with the converter device 102. In one embodiment, the near field communication is bi-directional such that the user device 104 may both send and receive wireless communication. That is, the user device includes a transceiver.

In general, the system interface 106 provides an interface to a larger information system (e.g., a financial system, an access control system, a medical records system, and the like) that in one embodiment includes a system processor or controller 110, a database 112, a network 114, other systems 116, such as a universal secure registry 118 as will be described further herein. Each of the preceding system elements may be placed in communication with any one or any combination of the system elements, for example, over communication links 120A, 120B, 120C, 120D. It should be recognized that the communication links 120 need not provide the communication paths shown in FIG. 28 and that other communication paths may be employed. For example, the database 112 may be connected to the network 114 via the communication link 120A

and to the system processor 110 via the communication link 120B instead of being connected as shown in FIG. 28.

The communication link may be a wireless communication link, a hardwired communication link, a fiber optic communication link, any communication link used in the art, as well as a combination of any of the preceding or any other any communication link capable of transmitting signals between the elements of the system 100. The system processor 110 allows information transfer of both data and instructions, for example, between the interface 106 and one or more databases which may be connected to the system or other network elements.

In general, the operation of the converter device 102 allows a user in possession of the user device 104 to wirelessly communicate information to the device so that the device can be employed to interface with a network system. For example, in one embodiment, the network system may provide a magnetic card reader interface and the converter device 102 provides a magnetic stripe emulator that can interface with the system. In general, the overall operation of the system 100 includes the communication of information between the user device 104 and the converter device 102, for example, RF communication. In one embodiment, the communication is bi-directional such that information can be communicated both to and from the user device 104. The converter device 102 provides an interface by which information derived from the information being transmitted to or from the user device 104 is transmitted between the converter device and the system interface 106. The system interface 106 provides the communication interface between it and the remainder of the system 100 (e.g., processor 110, database 112, network 114, etc.).

According to one embodiment, the user device 104 includes a processor 122, a user interface 124, a wireless transmitter 126 and device indicia 128. In another embodiment, the user device 104 includes a biometric sensor 130. In various embodiments, the processor 122 is communicatively coupled to each of the wireless transmitter 126, the user interface 124 and the biometric sensor 130.

The processor 122 may include a chip such as a general purpose processor, an application specific integrated circuit ("ASIC"), or a field programmable gate array ("FPGA") and the like that may execute various programs and/or provide logic inputs and outputs. For example, the processor 122 may process biometric information

received from the biometric sensor 130 to verify the identity of the user before the user can employ the user device 104. Exemplary details of a processor and biometric sensor which are configured to authenticate a fingerprint of a user are disclosed in U.S. published application 2004/0133787, published on July 8, 2004, which is herein incorporated by reference in its entirety. The processor 122 may also include or be coupled to driver circuitry to drive a display included in the user interface 124 and can be configured to process user input data entered via the user interface 124. In one embodiment, the user interface 124 includes one or more control inputs (for example, control buttons).

The wireless transmitter 126 can process information provided by the processor and convert the information to an RF signal and can also include an RF antenna that transmits the RF information wirelessly. In another embodiment, the user device may also include an RF receiver that receives a wireless RF signal from the RF antenna and converts the RF signal to an information signal provided to the processor. It is to be appreciated that the wireless transmitter and/or receiver need not be an RF device, it can also be any of a IR device, an optical device, a Bluetooth signal or any other wireless signal transmitter or receiver used in the art.

The user device may also include a power source such as a battery that fits within the device. In one alternative embodiment, the user device remains in a sleep mode until it is placed in the vicinity of an RF transmitter at which time the user device 104 converts received RF energy into electrical energy used to provide power to the processor 122 and the other components included in the user device 104.

According to one embodiment, the user device 104 can be a smart card configured for wireless signal transmission using RF signals. For example, the wireless transmitter 126 may be an RF transmitter device or any other wireless transmitter device configured to transmit the smart card information of the card. Alternatively, it is to be appreciated that the card can be many cards such as a debit card, a plurality of credit cards such as VISA, MasterCard, American Express, or any other card with the card indicia and relevant information being stored in card memory 129 and read out by processor 122 and provided to the wireless transmitter 126. However, the user device 104 need not be in the form of a card and may instead include a cell phone or PDA.

In the embodiment illustrated in FIG. 28, the converter device 102 includes a substrate 132 which may include a stripe 134 and a magnetic field generator 136 which together comprise the magnetic stripe emulator 137, a processor 138, a wireless receiver 140, a user interface 142, a memory 144, and a power source 146. In a further embodiment, the converter device 102 includes an indicating light 148 (e.g., an LED) and an output device 150.

According to one embodiment, the system interface 106 with which the converter device 132 is employed includes any of or all of a magnetic card reader 152, a wireless transceiver 154 and a data port 156.

In general, according to one embodiment, the converter device 102 receives a wireless signal from the user device 104, processes the information that is received and provides an output in the form of a time-varying signal provided to the stripe 134 (e.g., a magnetic stripe). The signal provided to the stripe 134 can then be provided to the system processor 110 by inserting the stripe and the associated substrate 132 or portion thereof in the magnetic card reader of the system interface 106. That is, in one embodiment, the stripe 134 and at least a portion of the substrate 132 can be either slid by the magnetic card reader 152 or inserted to sit statically in front of the read head of the card reader.

The processor 138 may be a general purpose processor, an application specific integrated circuit ("ASIC"), or a field programmable gate array ("FPGA") and may be implemented in hardware, software, firmware or any combination of the preceding. The processor 138 may be communicatively coupled with any of the magnetic field generator 136 the wireless receiver 140, the memory 144, the user interface 142, the light source 148, the power source 146 and the output device 150. In general, the processor can be configured to receive inputs from one or more of the preceding elements and may provide outputs to each of the elements included in converter device 138.

For example, according to one embodiment, the magnetic stripe 134 is a programmable magnetic stripe and the magnetic field generator 136 generates a magnetic signal that controls the information provided by the magnetic stripe 134. The U.S. Patent Application No. 10/680,050, filed October 7, 2003, entitled "System Method and Apparatus for Enabling Transactions Using a Biometrically Enabled

Programmable Magnetic Stripe which was published on July 8, 2004 as US2004/0133787 (the '050 application), provides further details concerning embodiments of the user device that emulates a magnetic stripe and may also include, for example, a biometric sensor. The '050 application is incorporated herein by reference in its entirety. In this embodiment, the processor 138 may control the operation of the magnetic field generator 136 to provide the desired information to the stripe 134. For example, the processor 138 may provide an output to the stripe 134 in response to receiving information from the wireless receiver 140, where the information from the wireless receiver is information transmitted from the user device 104.

Further, the processor 138 may be configured to provide signals to drive a display included in the user interface 142 and process user input data entered with the user interface 142. In one embodiment, the user interface 142 includes a display screen that can be used to display an image of the user to whom the user device 104 belongs, for security purposes. The image to be displayed by the UI can either be part of the information transmitted by the user device 104, for example, where the user device 104 also requires some authentication by the user before transmitting the device information and image, or can be provided, for example, by the USR system 118 through the system interface 106 as part of the user authentication process, as will be described in more detail herein. In further embodiments, the user interface 142 may include a plurality of control elements that allow the user and/or the transaction processor (e.g., store clerk, security guard, medical service provider, etc.) to enter information into the converter device 102. According to one embodiment, the user interface 142 includes an LCD display.

The processor 138 may also be configured to provide signals to operate the indicating light 148. The indicating light 148 may provide an indication of the operational status of the converter device 102, for example, the indicating light 148 may indicate any of the following: that the converter device 102 is receiving a transmission from a user device 104; that the converter device 102 has generated output data to the stripe 134; the status of the power source 146 is normal or conversely that the power source has a low power level; that the converter device 102 is transmitting information via the output device 150; that the converter device 102 is properly aligned

with the magnetic card reader 152; that the converter device 102 has received authorization for a transaction; and the like. It should be apparent to one of skill in the art that the indicating light may be a single lamp or a plurality of lamps and that the lamp or lamps may be a single color including white or may included a plurality of colors. Further, it should also be apparent that the lights may provide a plurality of status indications based on their color, intensity, rate of change of the preceding characteristics or any combination of these and other features.

The power source 146 may include a battery power source or other energy sources suitable for the form factor of the converter device 102. For example, in a form factor where the converter device 102 is a hand-held device the power source 146 may be any one of a standard size battery (e.g., a AA battery). In a further embodiment, the power source is a lithium battery. Alternatively, the power source can be any of an AC power source, an AC to DC converter device, or any other DC power source known to those skilled in the art.

According to one embodiment, the converter device 102 includes a power bus 158 that provides a path for the transmission of power to the various components included in the converter device 102.

In accordance with one embodiment, the converter device 102 includes the output device 150. It is to be appreciated that the output device can be any standard interface device to be coupled to a data bus such as a USB device, or the output device can be configured for contactless communication with the system interface 106. For example, in one embodiment, the output device is an optical transmitter device. In general, the communication between the converter device 102 and the system interface 106 is bi-directional such that information (e.g., information associated with the user's identity) may be transmitted to the system interface 106, the system processor 110 may generate a response (e.g., a transaction approval), and the response may transmitted to the converter device 102 via the system interface 106.

In one embodiment, the processor 138 is configured in combination with the output device 150 to provide an encrypted output signal. In a further embodiment, the processor 138 is configured in combination with the output device 150 to provide a time-varying encrypted output signal. In yet another embodiment, the processor 138 is configured in combination with the output device 150 to provide a time-varying

encrypted (or not) public and private key output signal. In addition, the processor can also be configured in combination with the wireless receiver to receive and decrypt any and all of an encrypted signal, a time-varying encrypted signal and a signal encrypted with a private key as provided by the user device 104. A challenge-response protocol may also be employed alternatively or in addition to any of the preceding.

For example, embodiments of the invention may employ a protocol that does not require synchronized clocks in each of the user device 104 and the converter device and/or elsewhere in the system 100 to complete a validation and/or authentication process. That is, according to one embodiment, an information exchange between the user device 104 and the converter device 102 includes a first piece of information transmitted from the user device 104 to the converter device 102 and a subsequent challenge (e.g., an encrypted challenge) generated by the converter device and transmitted from the converter device to the user device 104. According to one embodiment, the user employs the user device to respond to the challenge. In one embodiment, the user's response is at least in part based on information included in the challenge. An identity of a user who responds accurately to the challenge can be successfully validated. In various embodiments, a challenge-response protocol includes an information exchange whereby the identity of the converter 102 is also authenticated by the user with the user device 104.

In various embodiments, the above-described challenge-response protocol may not require any further action by the user than is required under current approaches that require synchronized clocks in disparate devices.

In some embodiments, the output device 150 need not transmit any personal information associated with the user. For example, commonly owned U.S. Patent Application No. 09/810,703, filed March 16, 2001, entitled "Universal Secure Registry" ("the '703 application") describes an approach that can improve security and reduce the need for multiple forms of identification. The '703 application is incorporated herein by reference in its entirety. The universal secure registry 118 included in the system 100 provides one example of the integration of such a registry into a system that employs a converter device 102. With the USR system, for example, the user device 104 can provide some information, e.g., such as a public code of the user, which can be authenticated by the user, for example by providing an ID through

the user interface 124 or through biometric sensor 130. The public code can be provided to the USR via the converter 102, system interface 104, and network 114. The USR can then provide back to any of the system interface and the converter device any or all of device information (e.g., transaction card information), authorization for a transaction, e.g., where the network or the USR also communicates with the relevant authority, and indicia about the holder of the user device.

The system 100 may include a variety of system interfaces 106 of different types such as the wireless transceiver 154 and the data port 156 in addition to the magnetic card reader 152. Although not illustrated, other system interfaces such as an optical interface, a smart card reader interface or any other system interface known to those of skill in the art can also be included. Further, the system interfaces may be either commonly located or may be geographically distributed such that some locations include a wireless transceiver 154, some locations include a data port 156, some locations include a magnetic card reader 152, and some locations include a plurality of types of system interfaces.

Thus, in some embodiments the output device 150 of the converter device 102 may include a data port via which the converter device 102 can provide data to a network or a networked device. In one embodiment, the data port is also configured to receive data from the network or a networked device.

Embodiments of the converter device 102 can be configured to provide communication to the system interface 106 via any of the preceding approaches including wireless signal transmission. In a version of this embodiment, the converter device 102 may receive wireless signals from the user device and transmit wireless signals to the system interface 106. Further, the converter device may include a transmitter that allows it to transmit information back to the user device.

Referring now to FIG. 29, a process 260 employing the converter device 102 is illustrated in accordance with one embodiment. The process begins at Stage 262 – START. Here, the converter device 102 is in a steady state in which it awaits receipt of a signal from a user device 104. At Stage 264, the converter device 102 receives data, for example, a wireless signal transmitted from the user device 104. At Stage 266, the converter device 266 extracts information from the wireless signal for processing. As one example, the converter device 102 may extract information corresponding to the

user's identity and/or the identity of the individual to whom the user device was issued. The extracted information is then provided to the system interface, for example, it is simulated as magnetic striped data to the magnetic card reader. At Stage 268, the system 100 authenticates the user. In one embodiment, if the authentication is successful, the process continues at Stage 270. In this embodiment, if the authentication is unsuccessful, the process returns to Stage 262 where, for example, the user may be prompted to attempt to authenticate again.

Various user authentication approaches may be implemented using the converter device 102. For example, the authentication may be performed locally, that is, without the need for communication between the converter device 102 and the system interface 106 and system processor 110. In one embodiment, the authentication process employs the universal secure registry 118. In further embodiments, the authentication process employs one or more authentication protocols such as public-key cryptography, key exchange protocols, protocols employing one-way functions, and the like that are well known by those of ordinary skill in the art. In other embodiments, however, the authentication may require an exchange of information between the converter device 102 and any of the system interface 106, the network 114, the USR 118 and another database 112. A challenge-response protocol may also be employed alternatively or in combination with any of the preceding authentication approaches.

At Stage 270, the completion of the transaction may be involve any of a wide variety of acts including: authorizing a withdrawal of money from a user's account, permitting the user access to a secure area, permitting a user to view medical information concerning themselves or a third party, or permitting the user to access other confidential information.

In addition, in some embodiments, the process 260 includes Stage 274 where following authentication the converter device 102 receives information associated with the user. The information may, for example, be necessary for the completion of the transaction. For example, where the system 100 is employed in conjunction with a check-authorization process, the converter device 102 may receive an indication that the user has sufficient funds to cover the amount of the check that is presented at a point of sale. Alternatively, or in addition, the information may include indicia related

to the authorized holder of the user device 104, such as a picture ID. The process 260 is completed at Stage 272 – END.

An embodiment, of the converter device 302 is illustrated in FIGS. 30A through 30D. As illustrated in the front view of FIG. 30A, in one embodiment, the converter device 302 includes a housing 380, a substrate 332, and a magnetic stripe 334. In one embodiment, the housing 380 is manufactured from a rigid material, for example, metal or plastic and the converter device 302 is designed to be a hand-held device. FIG. 30B illustrates a side view perspective of an embodiment of the converter device 302, showing an indicating light 348 (e.g., an LED). As described in greater detail above, the indicating light 348 can include a single indicating light or a plurality of indicating lights.

FIGS. 30A-30D illustrate an embodiment where the substrate extends substantially perpendicular from a side of the housing 380, however, the specific angle at which the substrate extends from the housing may vary so long as the housing does not interfere with the insertion of the substrate into, for example, the magnetic card reader 152.

FIG. 30D illustrates a top view of an embodiment of the converter device 302 which includes a display screen (e.g., an LCD display screen) that may provide the user interface 342 or a portion of the user interface of the converter device 302. In one embodiment, the user interface 342 includes a display screen that displays either a black and white or a color image of the individual to whom the user device 104 was issued. It should be recognized that the display screen may provide a wide range of functionality, for example, the display screen may display a variety of data received by the converter device 302 including data represented in alpha numeric format.

The magnetic stripe 334 may be a programmable magnetic stripe such that the converter device 302 provides a magnetic stripe emulator. In one embodiment, as has been described herein, the converter device 302 receives a wireless signal from a user device 104 and provides a time varying signal which emulates data provided by a magnetic-stripe card to a magnetic card reader in response to receiving the information from the wireless signal. In a further embodiment, the information is provided to the magnetic card reader by inserting the magnetic stripe 334 into the magnetic card reader.

IPR2025-01150
Apple EX1071 Page 1212

The various embodiments of a system and method for converting a wireless transaction device to a magnetic stripe emulator device may include any of the following or any combination of the following: a converter device with a processor communicatively coupled to a wireless signal receiver and to a magnetic stripe emulator. The converter device may optionally include an LED. Further the processor may be configured for any combination of the following: control of the LED to indicate that the device is properly aligned with the magnetic card reader, control of the LED to indicate that the device has received authorization for a transaction, and where the converter device includes a power supply, a processor configured to control the LED to indicate that the device has power.

In one embodiment, the information received from the wireless signal by the converter device may include any of a name, a card number, user identification, a device code, amount of credit available, and an expiration date of the card for a transaction.

Further, in various embodiments, the converter device may include an output device that can provide information to a network or to a networked device. In various embodiments, the output device can be configured as a wireless transmitter device, such as an optical transmitter device.

In various embodiments the wireless transmitter device where the wireless transmitter may generally be configured as an RF transmitter device, and in particular, as a Bluetooth transmitter device.

In addition, in various embodiments, the processor can be configured in combination with the output device to provide any of an encrypted output signal, a time-varying encrypted output signal, and in particular, a time-varying public and private key output signal.

In further embodiments, the converter device may include an output device configured as a data port via which the converter device can provide data to a network or a networked device and to receive data from the network or a networked device.

In one embodiment, the converter device may also include an LCD screen for displaying at least some of the data received by the converter device, and a processor configured in combination with the LCD device to display indicia corresponding to the

authorization of a transaction, and in particular, indicia that includes picture information of the cardholder.

In addition to the above described features, the various embodiments of a system and method for converting a wireless transaction device to a magnetic stripe emulator device may include any combination of the following or any combination of the following and the above listed features: the converter device can be configured to communicate with the magnetic card reader via the data port; the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal; the converter device is configured to decrypt a time-varying encrypted wireless signal; the converter device configured to decrypt time-varying public and private key information contained within the wireless signal; the converter device includes a user interface communicatively coupled to the processor; the converter device processor is configured to determine whether the user is authorized to provide the information contained within the wireless signal from data provided through the user interface.

In addition, the following further additional features may be combined alone or in combination with the preceding: the data contained within the wireless signal received by the converter device may include any combination of the following: user I.D. information, biometric information of the user, secret information, (for example, a PIN, a password, or a passcode of the user), or information about an uncounterfeitable token of the user.

In various embodiments, the converter device may include a substrate housing the magnetic stripe emulator, and the substrate may include a programmable magnetic stripe.

In various embodiments, the system employed with the converter device may also include a system interface coupled to a network where the system interface includes a magnetic stripe reading device configured to read a time-varying signal. In a further embodiments, the system interface may be configured to transmit data received from the wireless transaction device to a networked credit card authentication entity also coupled to the network. The system may also include any of a keyboard, a printer, an (LCD) display, and an audio signal transducer.

Although the preceding description is primarily directed to an embodiment of the user device 104 that does not include a magnetic stripe, it should be recognized that

some embodiments of the user device 104 may include a magnetic stripe. In these various embodiments, the converter device 102 may be employed to convert information coded on the magnetic stripe for transmission via another mode of information transmission.

What is claimed is:

CLAIMS

1. A system for validating an identity of a user to enable or prevent an occurrence of an event, the system comprising:

a first device including a wireless transmitter configured to transmit validation information;

a second device including a wireless receiver, the second device configured to receive the validation information and further transmit the validation information; and

a secure system in communication with the second device, the secure system including a database,

wherein the secure system is configured to receive the validation information transmitted from the second device, and

wherein the secure system is further configured to transmit additional information to the second device following a receipt of the validation information to assist the second device in either enabling or preventing the occurrence of the event.

2. The system of claim 1 wherein the second device includes a magnetic stripe emulator communicatively coupled to the wireless receiver and adapted to provide a time-varying signal emulating data provided by a magnetic stripe card to a magnetic card reader, in response to receiving the validation information from the first device.

3. The system of claim 2, wherein the second device includes a processor communicatively coupled to the wireless receiver and to the magnetic stripe emulator.

4. The system of claim 3, wherein the information includes any of a name, a card number, user identification, a device code, an amount of credit available, and an expiration date of the card for a transaction.

5. The system of claim 3, wherein the second device includes a LCD screen for displaying at least some of the information received by the second device.

6. The system of claim 5, wherein the processor is configured in combination with the LCD device to display indicia corresponding to the authorization of a transaction.

7. The system of claim 6, wherein the indicia includes picture information of a user of the first device.

8. The system of claim 2, wherein the second device includes an output device configured to transmit the validation information.

9. The system of claim 8, wherein the second device is configured to communicate with the magnetic card reader via the output device.

10. The system of claim 1, wherein the second device is configured to decrypt an encrypted wireless signal transmitted from the first device.

11. The system of claim 10, wherein the second device is configured to decrypt a time-varying encrypted wireless signal transmitted from the first device.

12. The system of claim 11, wherein the second device is configured to decrypt time-varying public and private key information contained within the wireless signal.

13. The system of claim 3, wherein the second device includes a user interface communicatively coupled to the processor.

14. The system of claim 13, wherein the processor is configured to determine whether the user is authorized to provide the information transmitted from the first device from data provided through the user interface.

15. The system of claim 1, wherein the second device is configured to determine whether the user is authorized to provide the validation information from the validation information transmitted from the first device.

16. The system of claim 15, wherein the validation information transmitted from the first device comprises user I.D. information.

17. The system of claim 15, wherein the validation information transmitted from the first device comprises biometric information of the user.

18. The system of claim 15, wherein the validation information transmitted from the first device comprises any of secret information, a PIN, a password, or a passcode of the user.

19. The system of claim 15, wherein the data transmitted from the first device comprises information about an uncounterfeitable token of the user.

20. The system of claim 2, wherein the second device includes a substrate housing the magnetic stripe emulator.

21. The system of claim 20, wherein the substrate comprises a programmable magnetic stripe.

22. The system of claim 3, wherein the processor is configured to provide binary data to the magnetic stripe emulator.

23. The system of claim 1, further wherein the secure system is configured to transmit data received from the second device to a networked credit card validation entity coupled to the secure system.

24, The system of claim 1, wherein the first device is configured to receive authentication information of the user.

25. The system of claim 24, wherein the authentication information includes biometric information of the user.

26. The system of claim 25, wherein the first device is configured to generate a non-predictable signal from the biometric information.

27. The system of claim 26, wherein the first device is further configured to generate a time varying non-predictable signal from the biometric information.

28. The system of claim 24, wherein the first device is configured to authenticate the authentication information of the user and to allow or not allow operation of the first device based on the authentication information.

29. The system of claim 28, wherein the authentication information includes biometric information of the user.

30. The system of claim 29, wherein the biometric information of the user comprises a voice signature of the user.

31. The system of claim 30, wherein the biometric information of the user comprises a fingerprint of the user.

32. The system of claim 31, wherein the authentication information of the user comprises a PIN.

33. The system of claim 1, wherein the secure system is configured to access authenticating indicia of the user; and to transmit the authenticating indicia from the secure database to the second device.

34. The system of claim 33, further comprising an act of generating a non-predictable code at the second device from the first authentication information.

35. The system of claim 34, wherein the non-predictable code is a time-varying code.

36. The system of claim 35, wherein the second device is configured to transmit the time-varying code to the secure system; and wherein the secure system is configured to determine from the time-varying code the authentication information.

37. The system of claim 36, wherein communication between the second device and the secure system is over any of a wide area network, the Internet, and a wireless network.

38. The system of claim 1, wherein the second device includes a processor, wherein the second device includes a memory configured to store public keys of a plurality of users, and wherein the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal transmitted from the first device.

39. The system of claim 38, wherein the second device is configured to look up a public key of the user and to decrypt the authentication information with the public key of the user.

40. The system of claim 39, wherein the authentication information includes any of a name, an identification number, an e-mail address, and at least a portion of a picture of the user.

41. The system of claim 38, wherein the second device is configured to periodically update the public keys of the plurality of users.

42. The system of claim 1, wherein the second device includes a processor, wherein the second device includes a memory configured to store picture data, wherein the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal transmitted from the first device, and wherein the second device is configured to access the picture data based on the decrypted authentication information.

43. The system of claim 42, wherein picture information of the user may be viewed with the second device.

44. The system of claim 42, wherein the encrypted wireless signal transmitted from the first device includes a first portion of the picture information of the user. .

45. The system of claim 44, wherein the second device is configured to access a second portion of the picture information of the user and to combine the first portion of the picture and the second portion of the picture.

46. The system of claim 1, wherein the second device includes a processor, wherein the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal transmitted from the first device, and wherein the encrypted wireless signal includes encrypted authentication information which has been encrypted with a first private key of the user.

47. The system of claim 1, wherein the second device includes a processor, wherein the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal transmitted from the first device, and wherein the second device is configured to request the encrypted wireless signal from the first device.

48. The system of claim 1, wherein the first device is configured to transmit a first wireless signal including first encrypted authentication information.

49. The system of claim 48, wherein the first device includes a first processor, a first biometric detector and a first memory,

wherein the first processor is configured to compare stored biometric data with detected biometric data of the user and configured to enable or disable use of the first device based on a result of the comparison and configured to encrypt first authentication information with a first private key into first encrypted authentication information,

wherein the first biometric detector is configured for detecting biometric data of the user, and

wherein the first memory is configured to store biometric data of the user, a private key of the user authorized to use the first device, and the first authentication information.

50. The system of claim 49, wherein the second device includes a second processor, a second biometric detector and a second memory,

wherein the second biometric detector configured to detect biometric data of a user of the second device, and

wherein, the second memory configured to store biometric data of the user of the second device and a plurality of public keys of a plurality of users associated with a plurality of devices configured to transmit authentication information to the second device.

51. The system of claim 50, wherein the biometric data is fingerprint data and each biometric detector is a fingerprint sensor.

52. The system of claim 50, wherein the second processor is configured to use the public key of the user to decrypt the encrypted first authentication information.

53. The system of claim 49, wherein the first encrypted authentication information includes an encrypted DES key of the user.

54. The system of claim 53, wherein the first encrypted authentication information also includes a DES key encrypted portion of biometric data of the user.

55. The system of claim 54, wherein the portion of biometric data is a portion of a digital image of the user.

56. The system of claim 49, wherein the first encrypted authentication information comprises a digital signature of the user.

57. The system of claim 49, wherein the first encrypted authentication information comprises a one-time random code of the user.

58. The system of claim 50, wherein the second memory also comprises a portion of authentication data of a plurality of first users.

59. The system of claim 58, wherein the biometric data of the plurality of first users comprises at least a portion of a digital image of the plurality of first users.

60. The system of claim 50, wherein the first device can be any of a handheld device, a cell phone, a PDA, a PC, a credit card sized device, an ID badge, a key FOB, a passport, and a wrist watch.

61. The system of claim 50, wherein the database comprises biometric information of a plurality of users.

62. The system of claim 61, wherein the biometric information of the plurality of users includes at least a portion of digital image data of the plurality of users.

63. A method employing a system to validate an identity of a user to enable or prevent an occurrence of an event, the system including a first device, a second device and a secure system including a database, the method comprising acts of:

receiving at the second device validation information wirelessly transmitted from the first device;

communicating the validation information from the second device to the secure system; and

receiving at the second device additional information from the secure system, wherein the additional information assists the second device in either enabling or preventing the occurrence of the event.

64. The method of claim 63 wherein the second device includes a magnetic stripe emulator communicatively coupled to the wireless receiver, and wherein the method

IPR2025-01150
Apple EX1071 Page 1223

further comprises an act of providing a time-varying signal emulating data provided by a magnetic stripe card to a magnetic card reader, in response to receiving the validation information from the first device.

65. The method of claim 64, wherein the second device includes a processor communicatively coupled to the wireless receiver and to the magnetic stripe emulator.

66. The method of claim 65, wherein the information includes any of a name, a card number, user identification, a device code, an amount of credit available, and an expiration date of the card for a transaction.

67. The method of claim 65, wherein the second device includes a LCD screen, and wherein the method further comprises an act of displaying at least some of the information received by the second device on the LCD screen.

68. The method of claim 67, wherein the processor is configured in combination with the LCD device to display indicia corresponding to the authorization of a transaction.

69. The method of claim 68, further comprising an act of including picture information of a user of the first device in the indicia.

70. The method of claim 64, wherein the second device includes an output device, and wherein the method further comprises an act of transmitting the validation information from the second device with the output device.

71. The method of claim 70, further comprising an act of communicating with the magnetic card reader via the output device.

72. The method of claim 65, further comprising an act of decrypting an encrypted wireless signal transmitted from the first device with the second device.

IPR2025-01150
Apple EX1071 Page 1224

73. The method of claim 72 further comprising an act of decrypting, with the second device, a time-varying encrypted wireless signal transmitted from the first device.

74. The method of claim 73, further comprising an act of decrypting, with the second device, information encrypted with a private key contained within the wireless signal.

75. The method of claim 65, wherein the second device includes a user interface communicatively coupled to the processor.

76. The method of claim 75, further comprising an act of determining with the processor whether the user is authorized to provide the validation information transmitted from the first device from data provided through the user interface.

77. The method of claim 65, further comprising an act of determining with the processor whether the user is authorized to provide the validation information from the validation information transmitted from the first device.

78. The method of claim 77, further comprising an act of including user I.D. information in the validation information transmitted from the first device.

79. The method of claim 77, further comprising an act of including biometric information of the user in the validation information transmitted from the first device.

80. The method of claim 77, further comprising an act of including any of secret information, a PIN, a password, or a passcode of the user in the validation information transmitted from the first device.

81. The method of claim 77, further comprising an act of including information about an uncounterfeitable token of the user in the data transmitted from the first device.

IPR2025-01150
Apple EX1071 Page 1225

82. The method of claim 64, wherein the second device includes a substrate housing the magnetic stripe emulator.

83. The method of claim 82, wherein the substrate comprises a programmable magnetic stripe.

84. The method of claim 65, further comprising an act of providing binary data to the magnetic stripe emulator with the processor.

85. The method of claim 63, further comprising an act of, with the secure system, transmitting data received from the second device to a networked credit card validation-information entity coupled to the secure system.

86. The method of claim 63, further comprising an act of receiving, with the first device, authentication information of the user.

87. The method of claim 86, further comprising an act of including the biometric information of the user in the authentication information.

88. The method of claim 87, further comprising an act of generating, with the first device, a non-predictable signal from the biometric information.

89. The method of claim 88, further comprising an act of generating, with the first device, a time varying non-predictable signal from the biometric information.

90. The method of claim 86, further comprising acts of:

authenticating, with the first device, the authentication information of the user; and

allowing or not allowing operation of the first device based on the authentication information.

IPR2025-01150
Apple EX1071 Page 1226

91. The method of claim 90, further comprising an act of including biometric information of the user in the authentication information.

92. The method of claim 91, wherein the biometric information of the user comprises a voice signature of the user.

93. The method of claim 92, wherein the biometric information of the user comprises a fingerprint of the user.

94. The method of claim 93, wherein the authentication information of the user comprises a PIN.

95. The method of claim 63, wherein the secure system is configured to accessing, with the secure system, authenticating indicia of the user; and to transmit the authenticating indicia from the secure database to the second device.

96. The method of claim 95, further comprising an act of generating a non-predictable code at the second device from the first authentication information.

97. The method of claim 96, wherein the non-predictable code is a time-varying code.

98. The method of claim 97, further comprising an act of transmitting the time-varying code to the secure system with the second device; and determining from the time-varying code the authentication information with the secure system.

99. The method of claim 98, further comprising an act of communicating between the second device and the secure system over any of a wide area network, the Internet, and a wireless network.

100. The method of claim 63, wherein the second device includes a processor and a memory, and wherein the method further comprises acts of:

IPR2025-01150
Apple EX1071 Page 1227

storing public keys of a plurality of users in the memory; and

decrypting an encrypted wireless signal transmitted from the first device using the wireless receiver and/or processor.

101. The method of claim 100, further comprising acts of:

looking up a public key of the user with the second device; and

decrypting, with the second device, the authentication information with the public key of the user.

102. The method of claim 101, wherein the authentication information includes any of a name, an identification number, an e-mail address, and at least a portion of a picture of the user.

103. The method of claim 100, further comprising an act of periodically updating the public keys of the plurality of users with the second device.

104. The method of claim 63, wherein the second device includes a processor, and a memory configured to store picture data, and wherein the method further comprises acts of:

decrypting, with the wireless receiver and/or processor, an encrypted wireless signal transmitted from the first device, and

accessing, with the second device, the picture data based on the decrypted authentication information.

105. The method of claim 104, further comprising an act of viewing the picture information of the user with the second device.

106. The method of claim 104, further comprising an act of including a first portion of the picture information of the user in the encrypted wireless signal transmitted from the first device.

107. The method of claim 106, further comprising acts of:

IPR2025-01150
Apple EX1071 Page 1228

accessing a second portion of the picture information of the user with the second device; and

combining the first portion of the picture and the second portion of the picture with the second device.

108. The method of claim 63, wherein the second device includes a processor, and wherein the method includes acts of:

decrypting an encrypted wireless signal transmitted from the first device with the wireless receiver and/or processor;

encrypting the authentication information with a first private key of the user; and

including the encrypted authentication information in the encrypted wireless signal.

109. The method of claim 63, wherein the second device includes a processor, and wherein the method further comprises acts of:

decrypting an encrypted wireless signal transmitted from the first device with the wireless receiver and/or processor, and

requesting the encrypted wireless signal from the first device with the second device.

110. The method of claim 63, further comprising an act of transmitting a first wireless signal including first encrypted authentication information with the first device.

111. The method of claim 110, wherein the first device includes a first processor, a first biometric detector and a first memory, and wherein the method further comprises acts of:

comparing stored biometric data with detected biometric data of the user with the first processor;

enabling or disabling use of the first device based on a result of the act of comparing with the first processor;

IPR2025-01150
Apple EX1071 Page 1229

encrypting first authentication information with a first private key into first encrypted authentication information with the first processor;

detecting biometric data of the user with the first biometric detector; and

storing biometric data of the user, a private key of the user authorized to use the first device, and the first authentication information in the memory.

112. The method of claim 111, wherein the second device includes a second processor, a second biometric detector and a second memory, and wherein the method further comprises acts of:

detecting biometric data of a user of the second device with the second biometric detector,

storing, in the second memory, biometric data of the user of the second device and a plurality of public keys of a plurality of users associated with a plurality of devices configured to transmit authentication information to the second device.

113. The method of claim 112, wherein the biometric data is fingerprint data and each biometric detector is a fingerprint sensor.

114. The method of claim 112, further comprising an act of decrypting the encrypted first authentication information with the public key of the user.

115. The method of claim 111, wherein the first encrypted authentication information includes an encrypted DES key of the user.

116. The method of claim 115, wherein the first encrypted authentication information also includes a DES key encrypted portion of biometric data of the user.

117. The method of claim 116, wherein the portion of biometric data is a portion of a digital image of the user.

118. The method of claim 111, wherein the first encrypted authentication information comprises a digital signature of the user.

IPR2025-01150
Apple EX1071 Page 1230

119. The method of claim 111, wherein the first encrypted authentication information comprises a one-time random code of the user.

120. The method of claim 112, further comprising an act of including a portion of authentication data of a plurality of first users in the second memory.

121. The method of claim 120, wherein the biometric data of the plurality of first users comprises at least a portion of a digital image of the plurality of first users.

122. The method of claim 112, wherein the first device can be any of a handheld device, a cell phone, a PDA, a PC, a credit card sized device, an ID badge, a key FOB, a passport, and a wrist watch.

123. The method of claim 112, further comprising an act of including biometric information of a plurality of users in the database.

124. The method of claim 123, further comprising an act of including at least a portion of digital image data of the plurality of users in the biometric information of the plurality of users.

125. The system of claim 1, wherein the second device communicates an amount of purchase by a user of the first device with the secure system and receives any of an approval or denial for the purchase without the credit card number, a credit card number of a user and an approval or denial of the purchase, and an available balance of the user.

126. The system of claim 1, wherein the second device validates the information transmitted from the first device and transmits the validated information to the secure system, and wherein the secure system provides the additional information to enable or prevents the occurrence of the event based on the validated information as communicated by the second device.

IPR2025-01150
Apple EX1071 Page 1231

127. The system of claim 1, wherein the secure system validates the information transmitted from the second device and wherein the secure system provides the additional information to enable or prevents the occurrence of the event based on the validated information.

128. The system of claim 1, wherein the second device validates the information transmitted from the first device based on the validation information transmitted from the first device and the additional information provided by the secure system, and wherein the second device enables or prevents the occurrence of the event based on the validation information and the additional information.

129. The method of claim 63, further comprising acts of communicating with the second device an amount of purchase by a user of the first device to the secure system and receiving from the secure system any of an approval or denial for the purchase without the credit card number, a credit card number of a user and an approval or denial of the purchase, and an available balance of the user.

130. The method of claim 63, further comprising acts of validating with the second device the information transmitted from the first device and transmitting the validated information to the secure system, and receiving from the secure system the additional information to enable or prevent the occurrence of the event based on the validated information.

131. The method of claim 63, further comprising the act of validating with the secure system information transmitted from the second device and providing with the secure system the additional information to enable or prevents the occurrence of the event based on the validated information.

132. The method of claim 63, further comprising validating with the second device the information transmitted from the first device based on the validation information transmitted from the first device and the additional information provided by the secure

IPR2025-01150
Apple EX1071 Page 1232

system, and enabling or preventing with the second device the occurrence of the event based on the validation information and the additional information.

IPR2025-01150
Apple EX1071 Page 1233

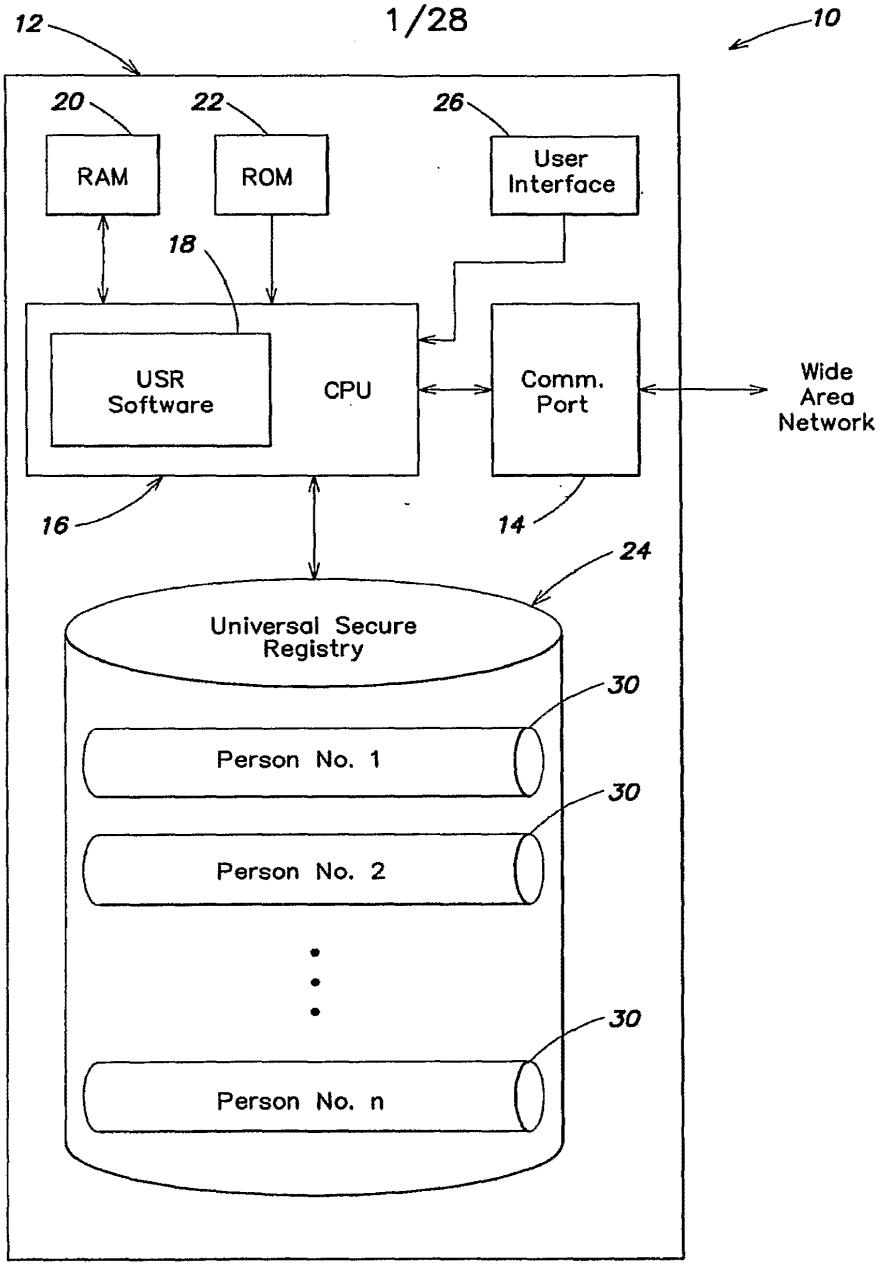


FIG. 1

IPR2025-01150
Apple EX1071 Page 1234

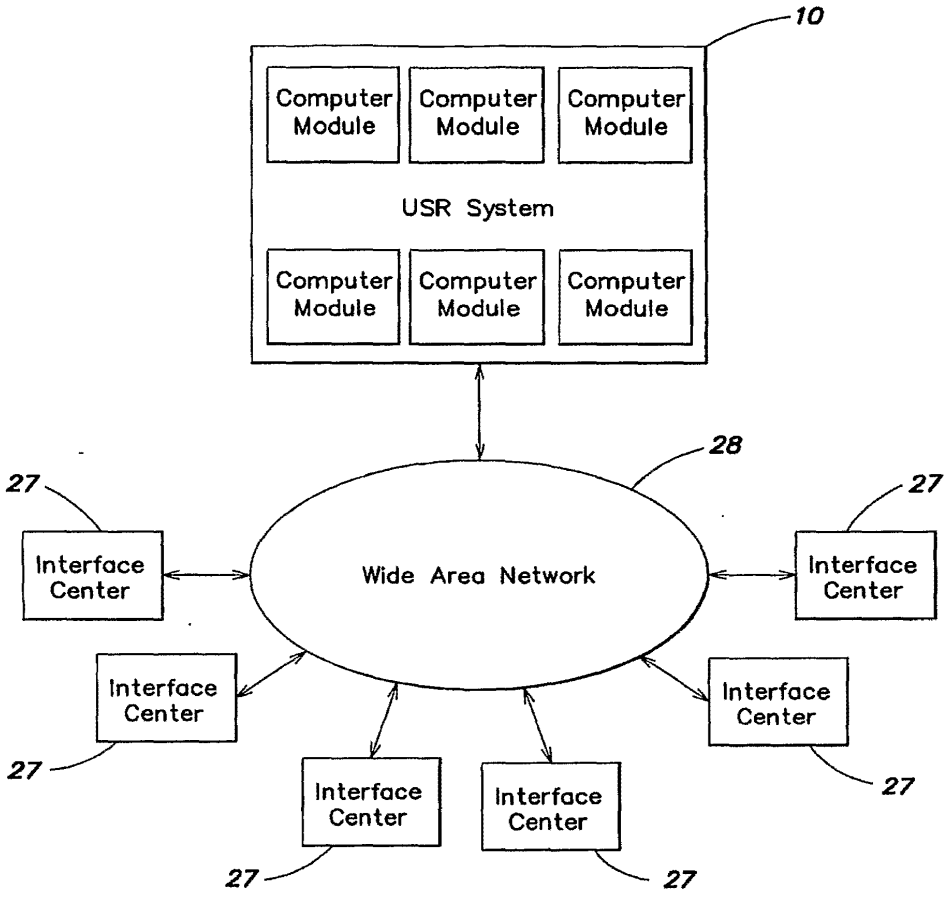


FIG. 2

IPR2025-01150
Apple EX1071 Page 1235

FIG. 3

SUBSTITUTE SHEET (RULE 26)

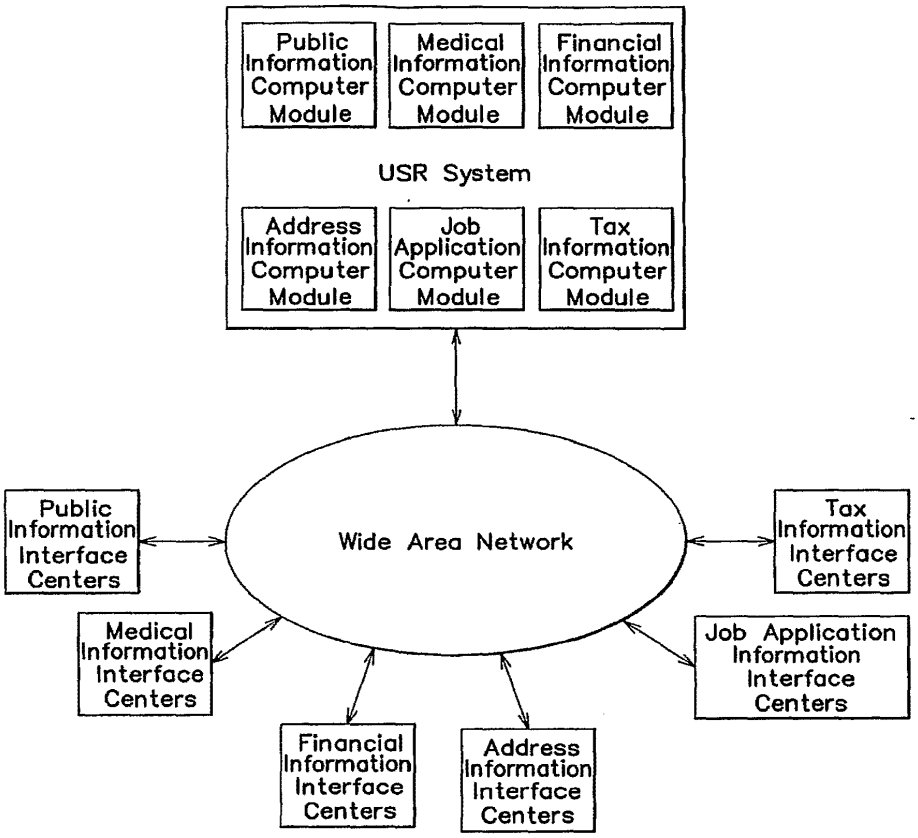


FIG. 4

IPR2025-01150
Apple EX1071 Page 1237

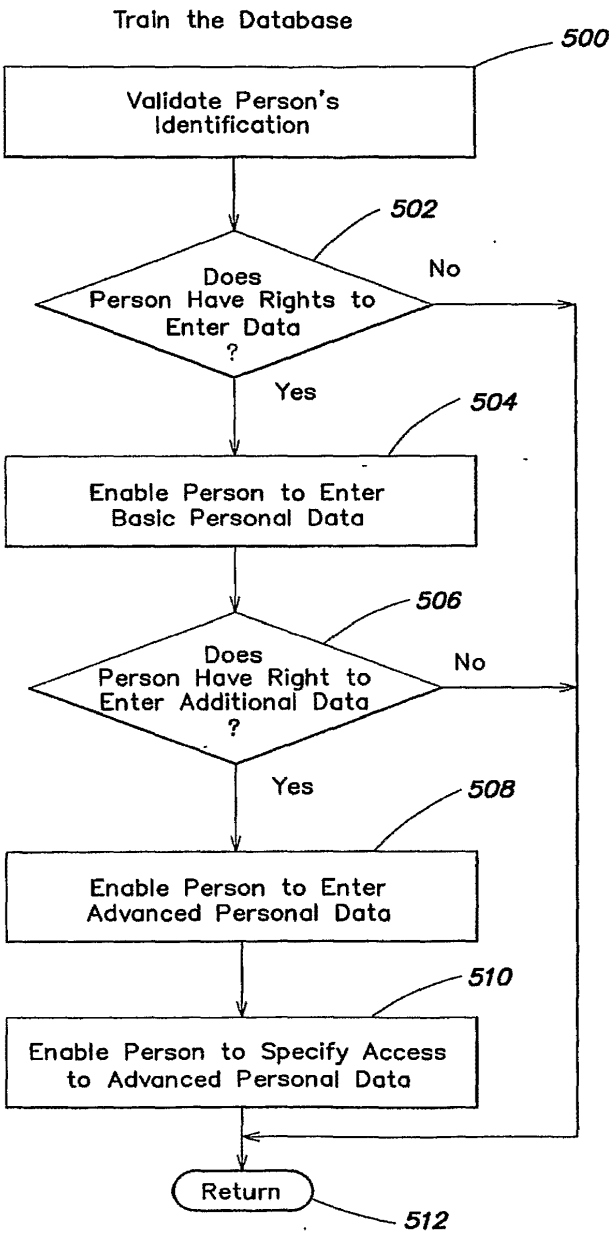


FIG. 5

IPR2025-01150
Apple EX1071 Page 1238

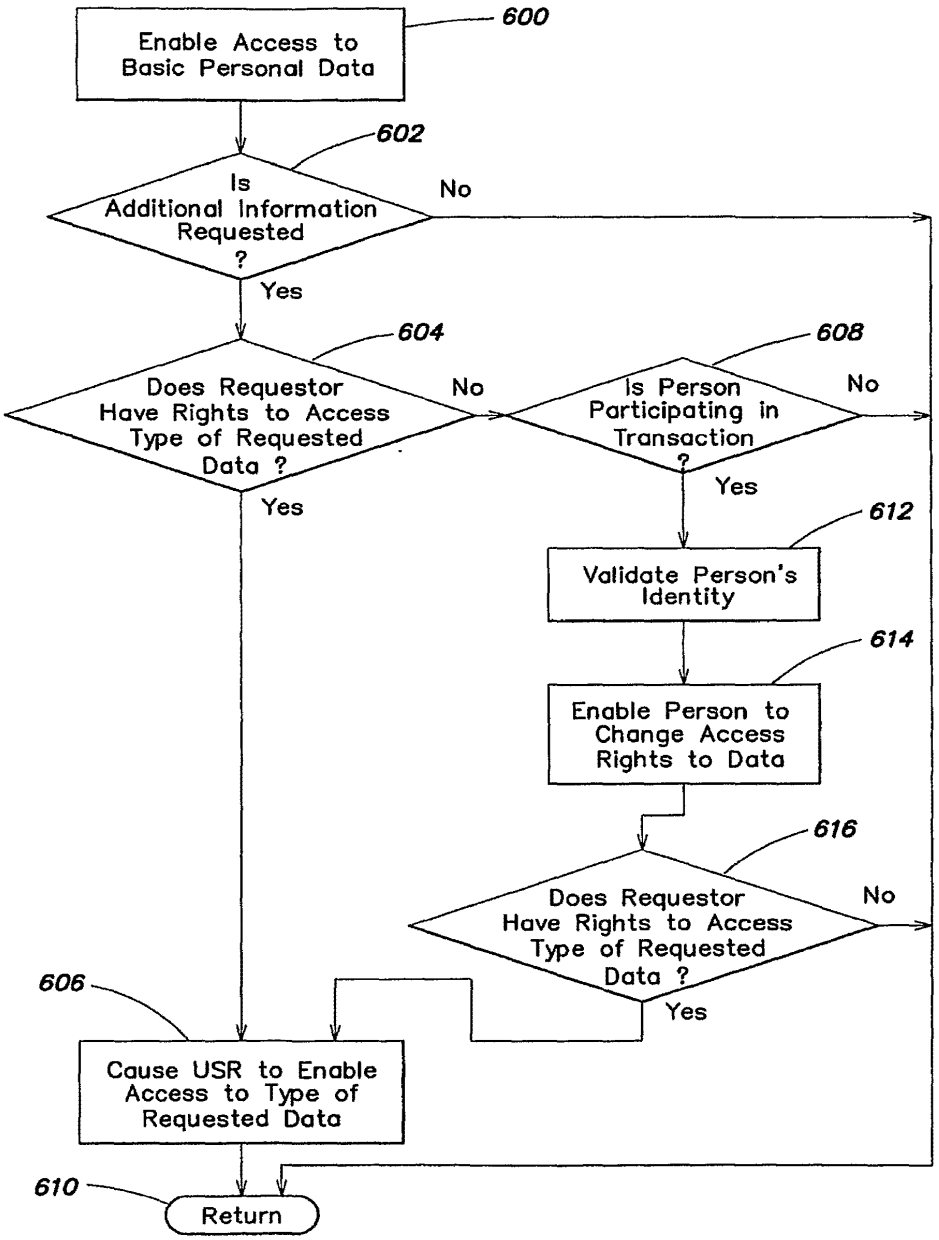


FIG. 6

IPR2025-01150
Apple EX1071 Page 1239

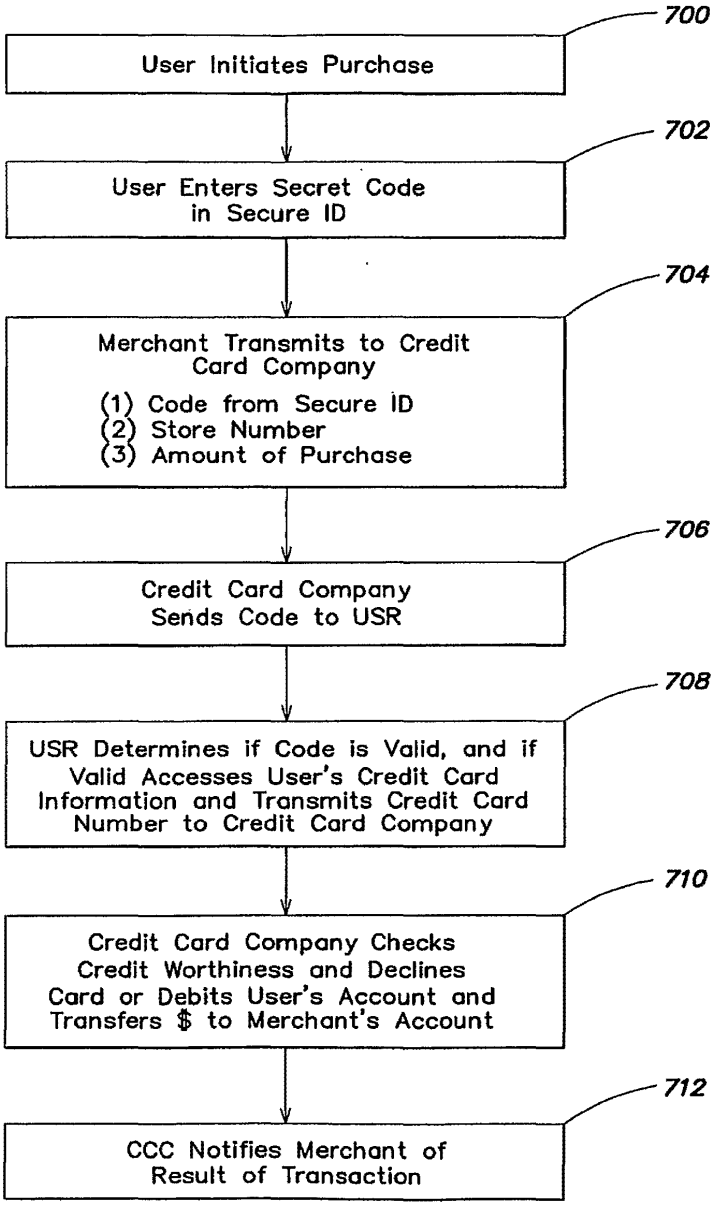


FIG. 7

IPR2025-01150
Apple EX1071 Page 1240

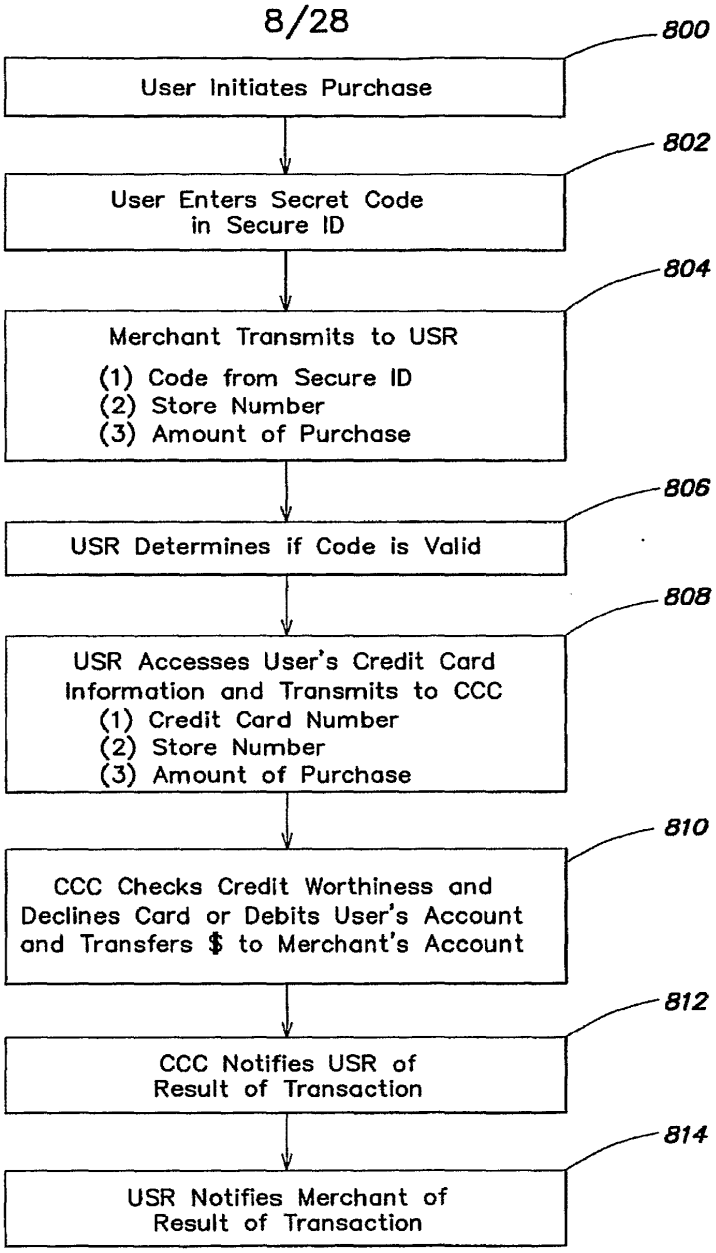


FIG. 8

IPR2025-01150
Apple EX1071 Page 1241

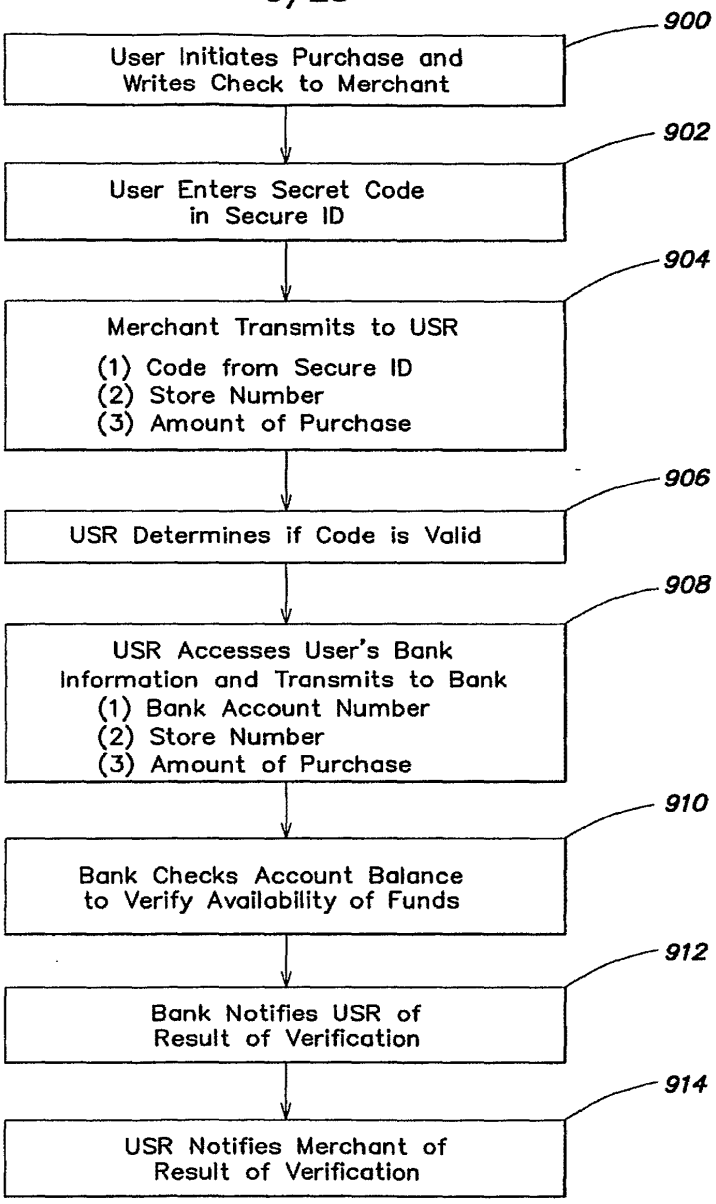


FIG. 9

IPR2025-01150
Apple EX1071 Page 1242

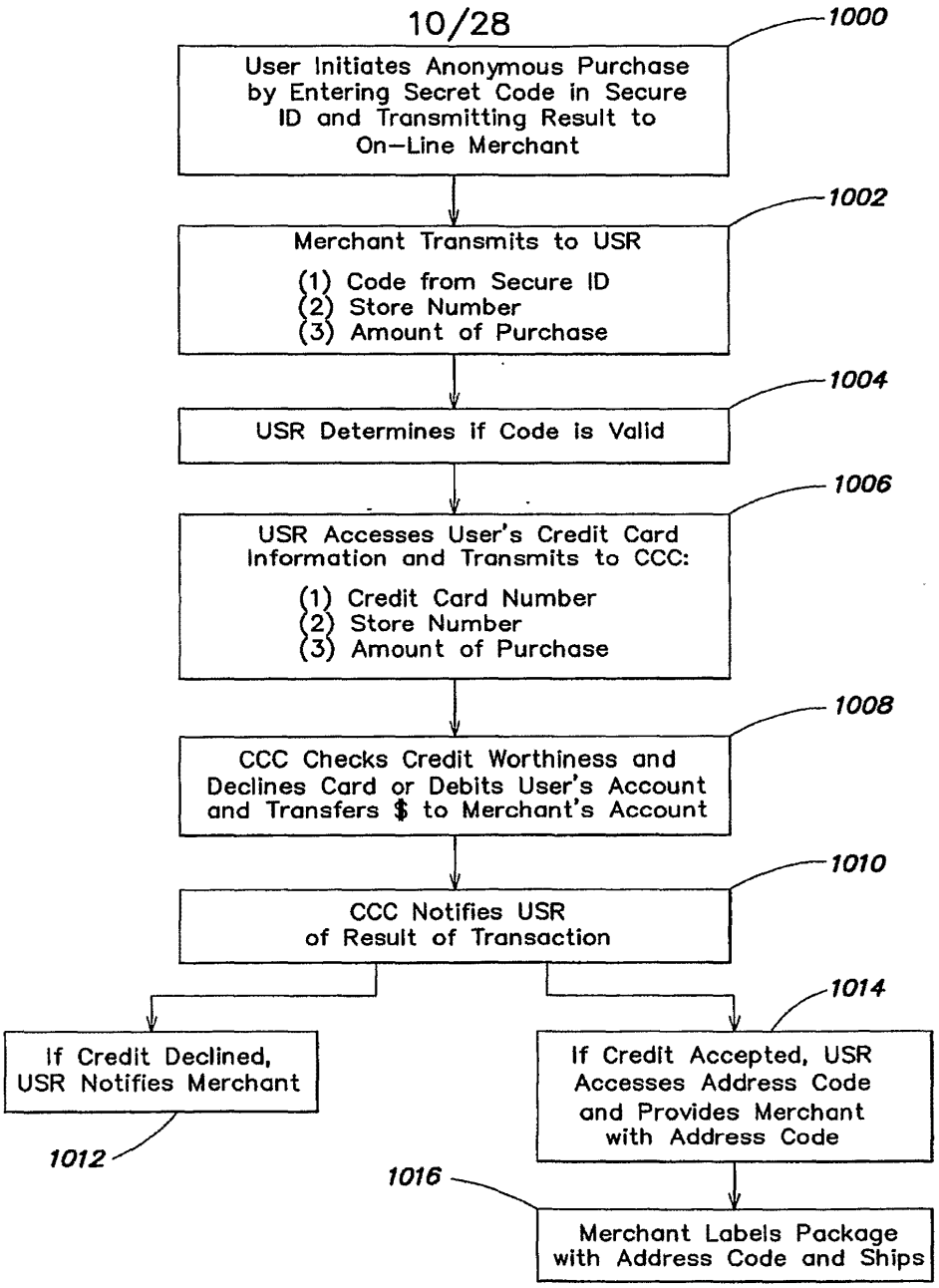


FIG. 10

IPR2025-01150
Apple EX1071 Page 1243

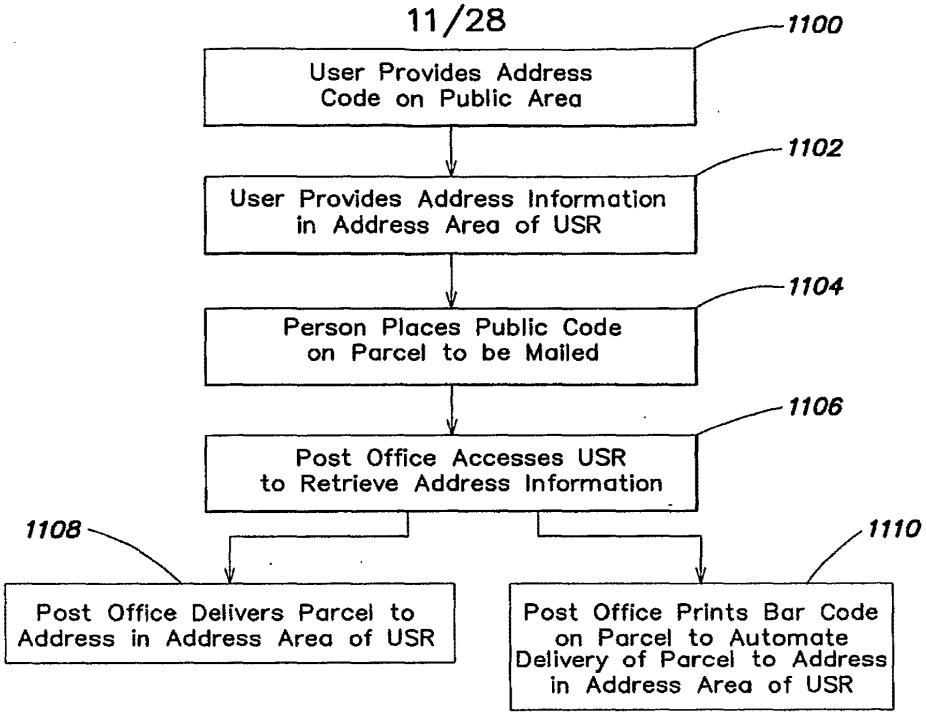


FIG. 11

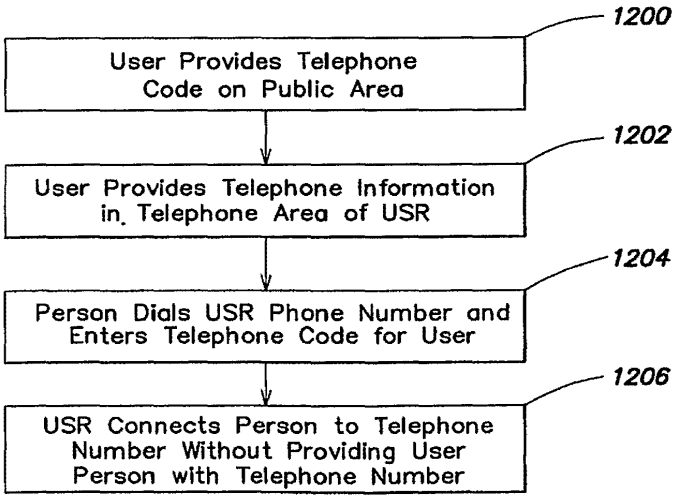


FIG. 12

IPR2025-01150
Apple EX1071 Page 1244

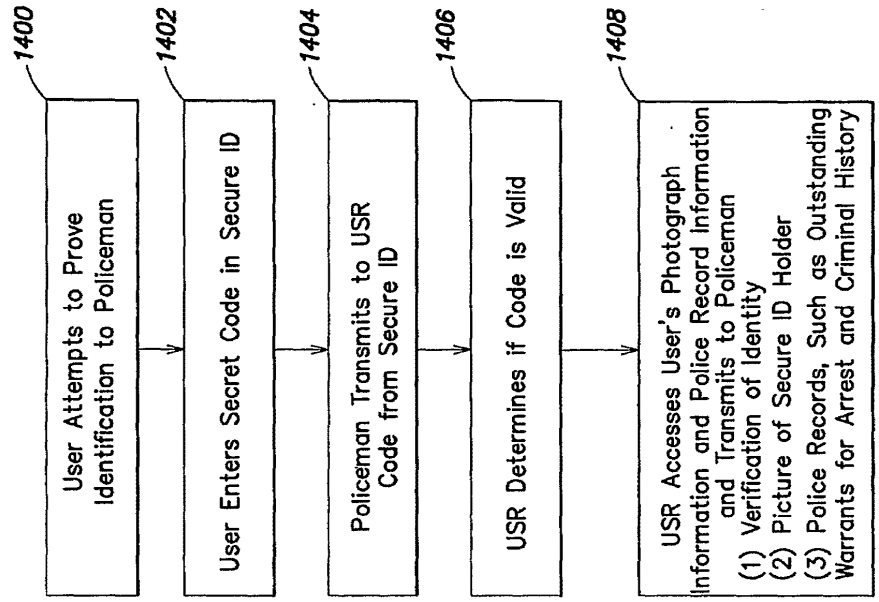


FIG. 14

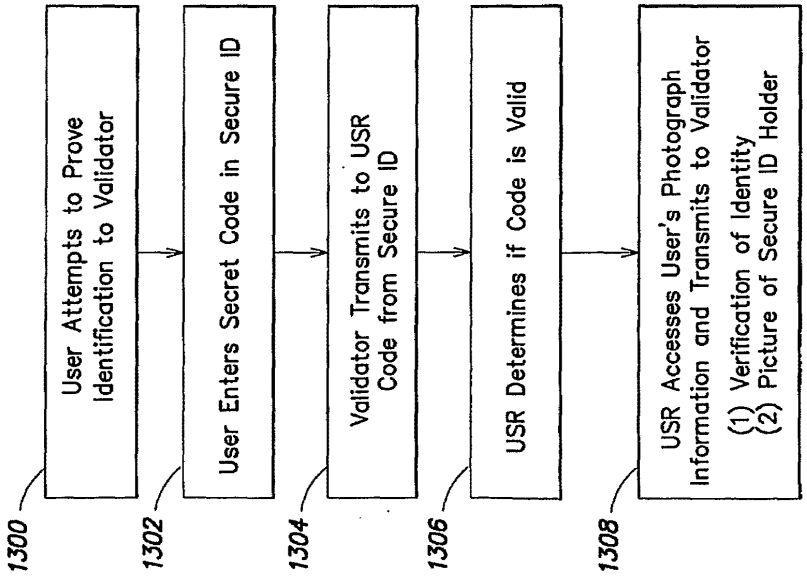


FIG. 13

IPR2025-01150
Apple EX1071 Page 1245

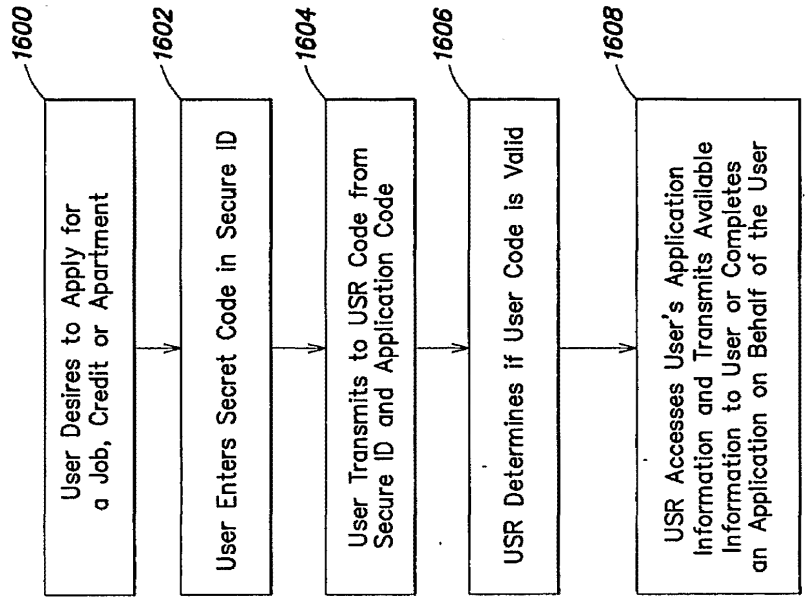


FIG. 16

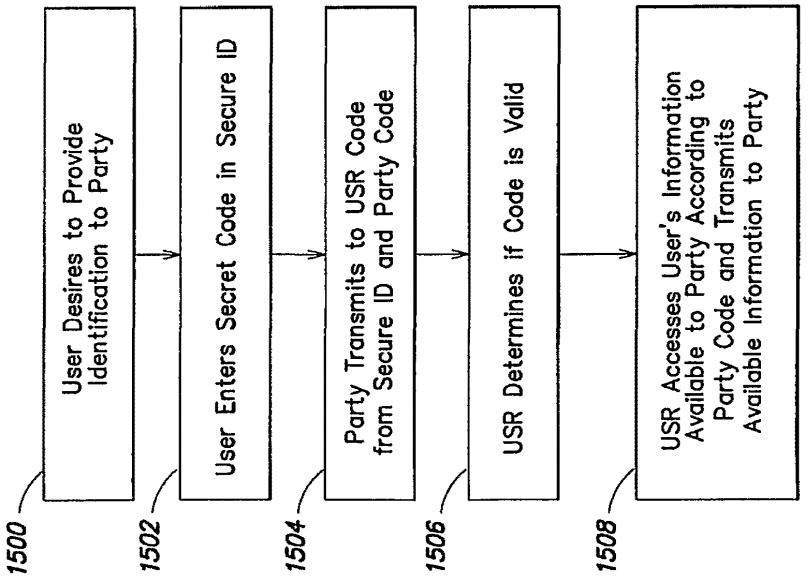


FIG. 15

IPR2025-01150
Apple EX1071 Page 1246

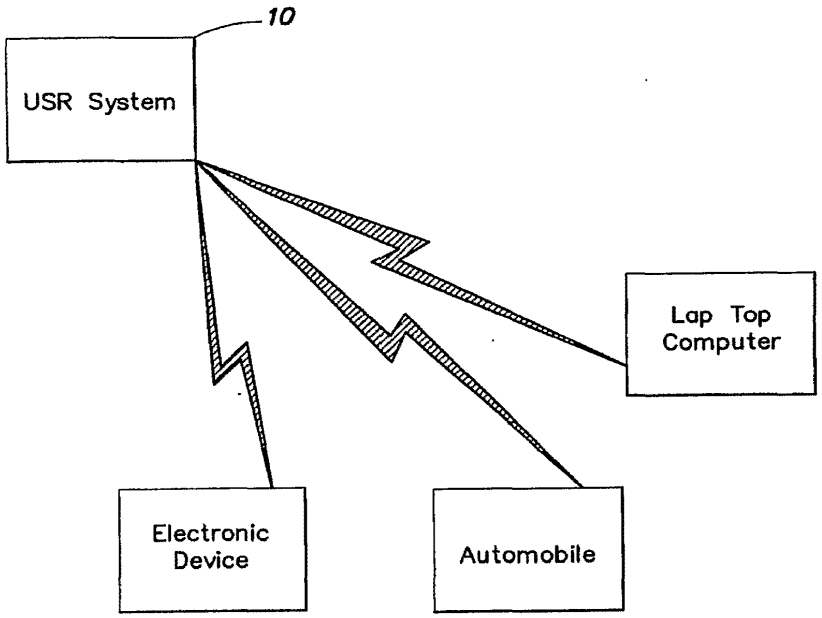


FIG. 17

IPR2025-01150
Apple EX1071 Page 1247

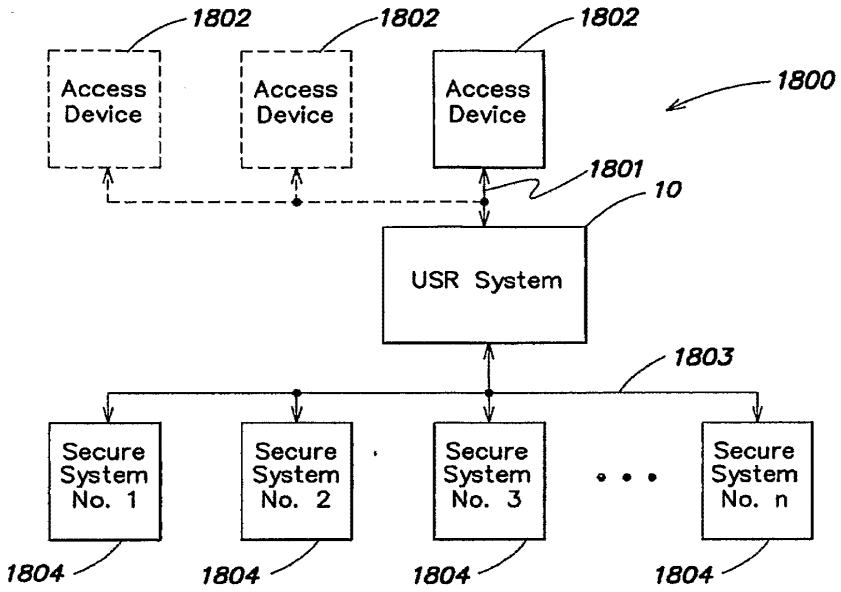


FIG. 18A

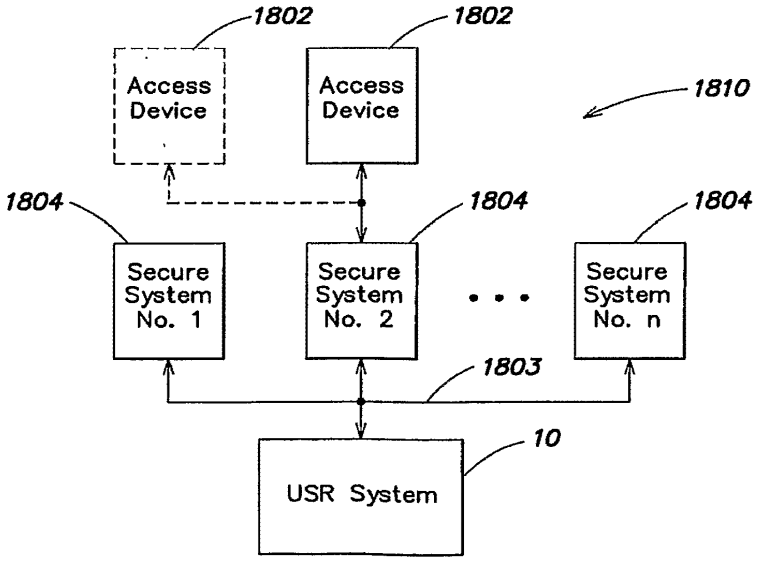


FIG. 18B

IPR2025-01150
Apple EX1071 Page 1248

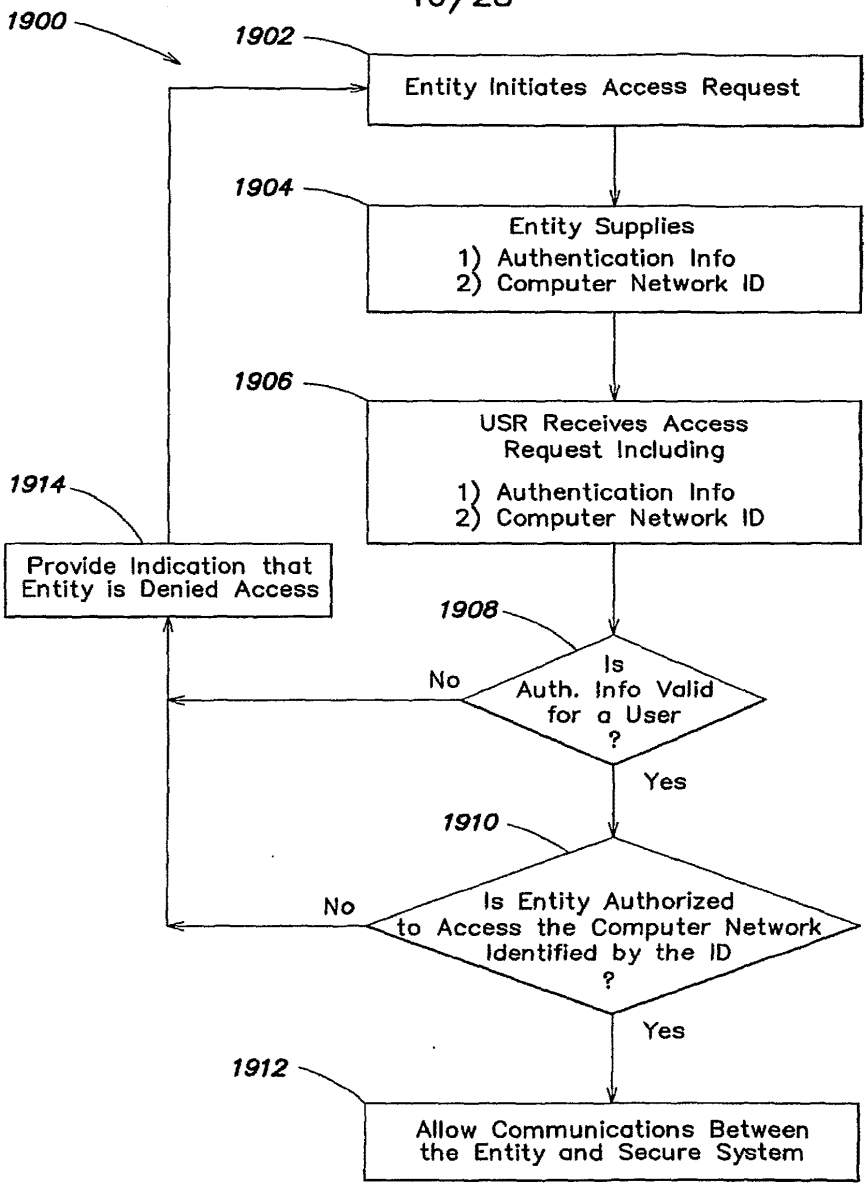


FIG. 19

IPR2025-01150
Apple EX1071 Page 1249

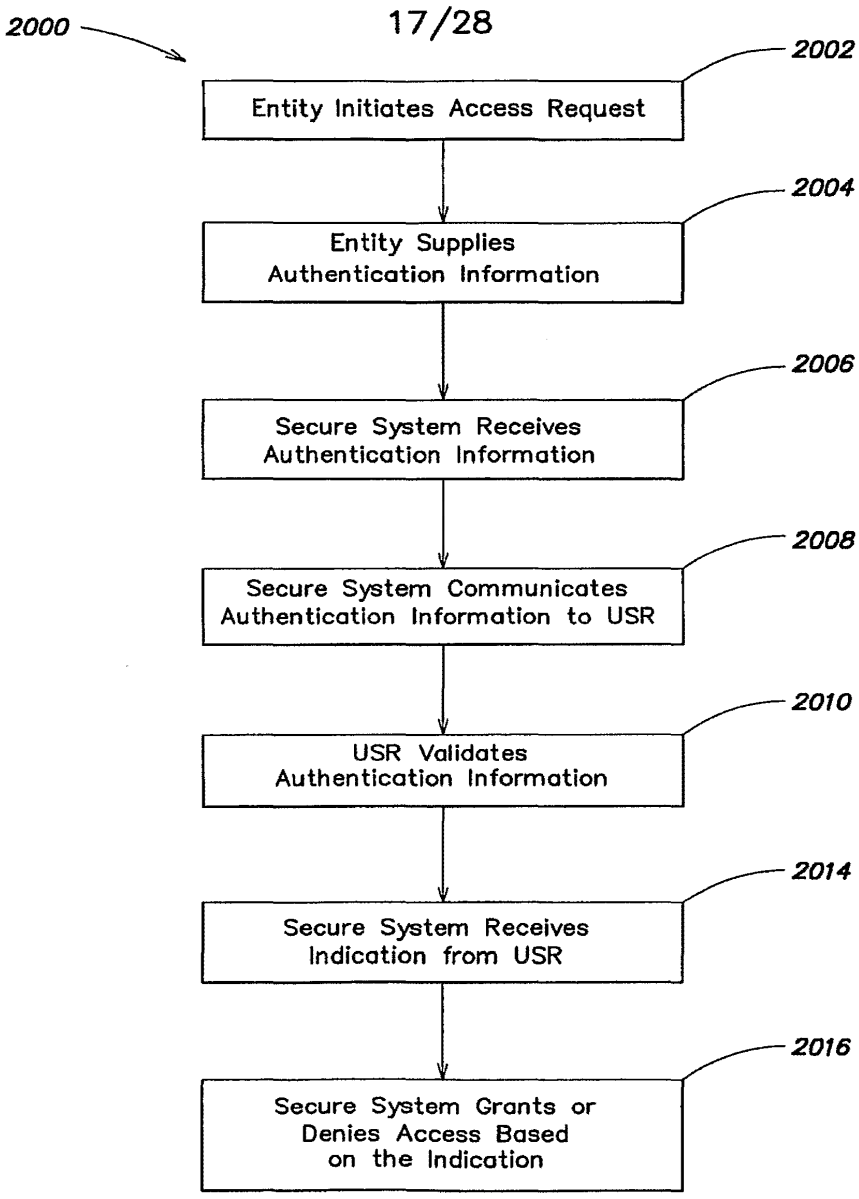


FIG. 20

IPR2025-01150
Apple EX1071 Page 1250

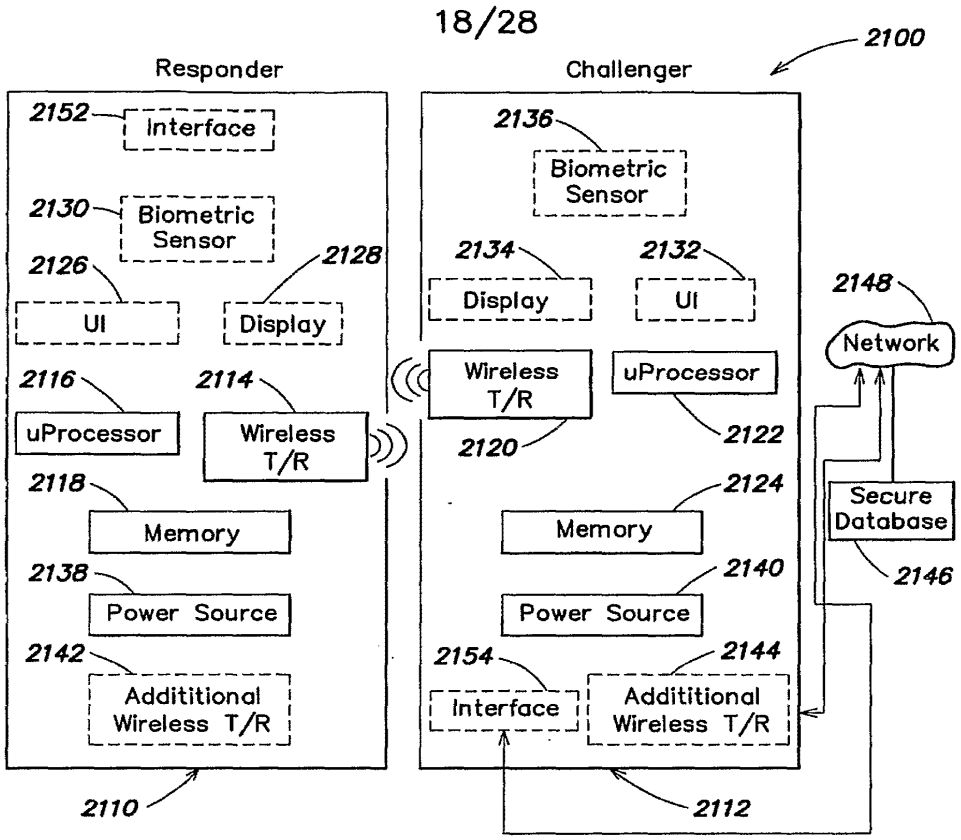


FIG. 21

IPR2025-01150
Apple EX1071 Page 1251

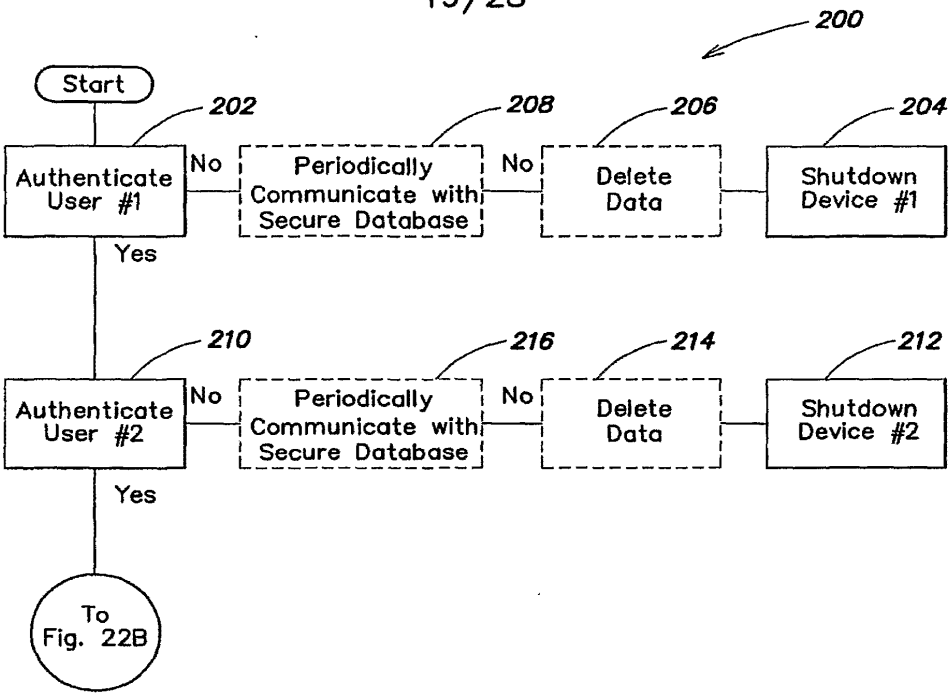


FIG. 22A

IPR2025-01150
Apple EX1071 Page 1252

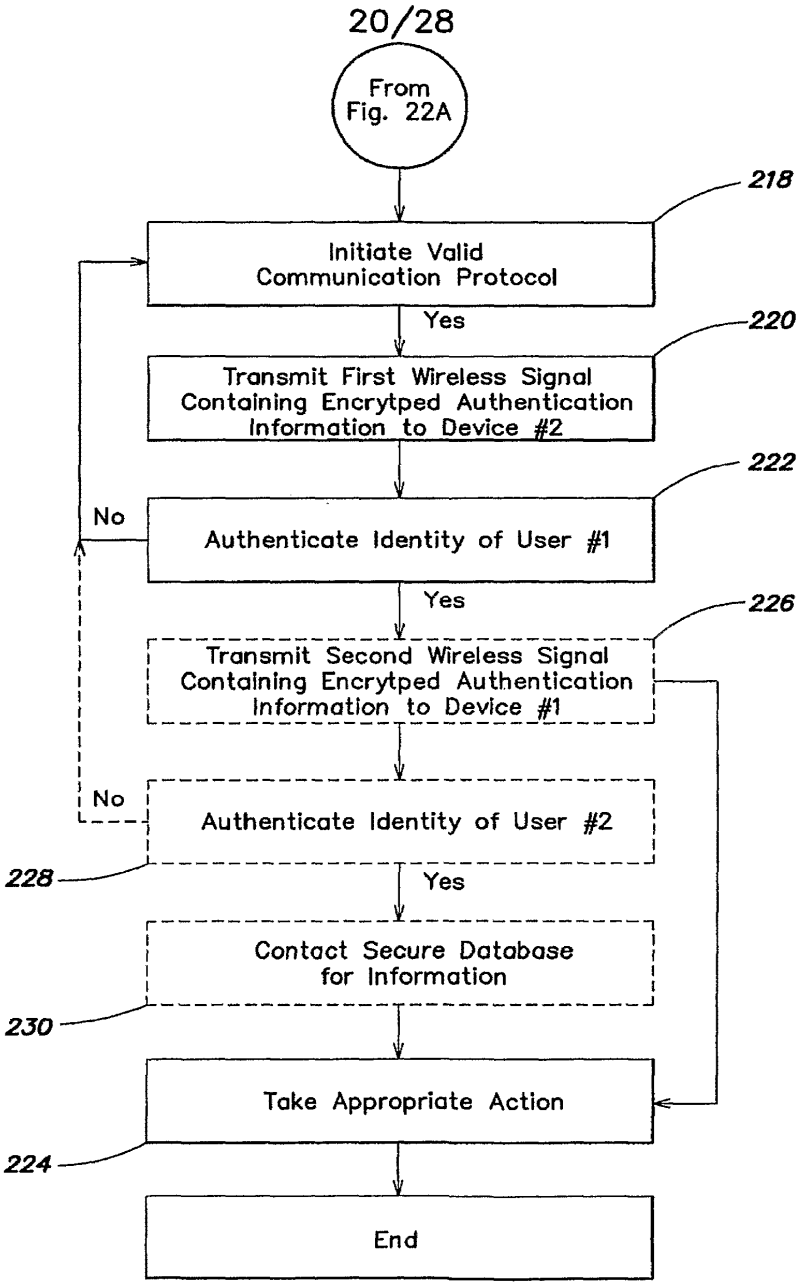


FIG. 22B

IPR2025-01150
Apple EX1071 Page 1253

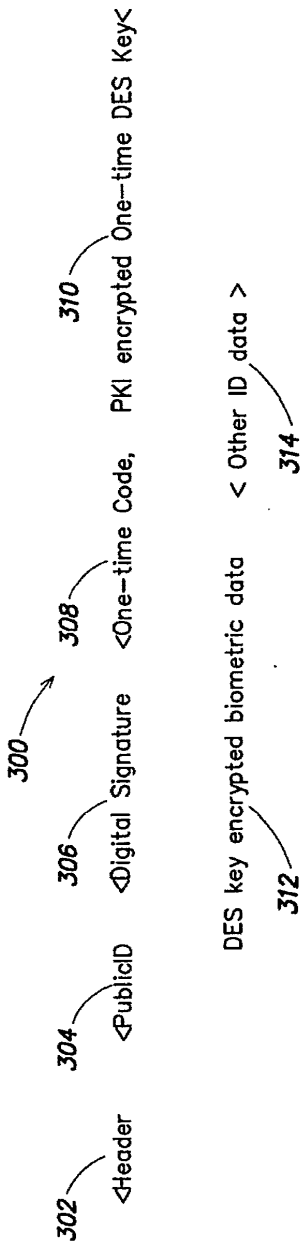


FIG. 23

IPR2025-01150
Apple EX1071 Page 1254

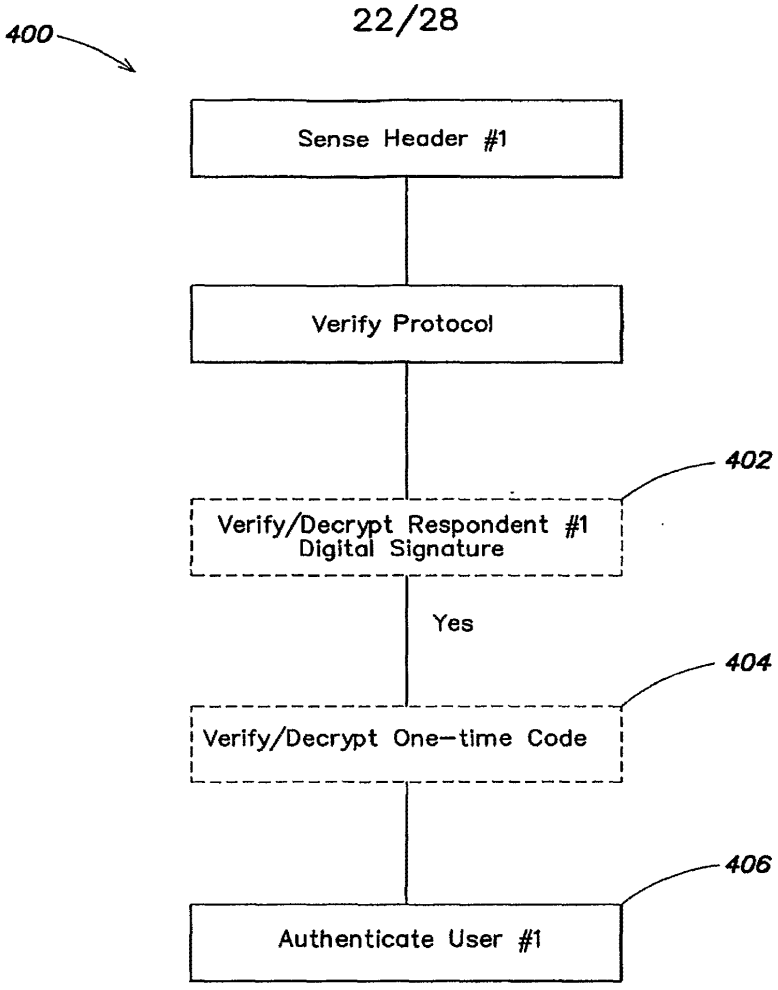


FIG. 24

IPR2025-01150
Apple EX1071 Page 1255

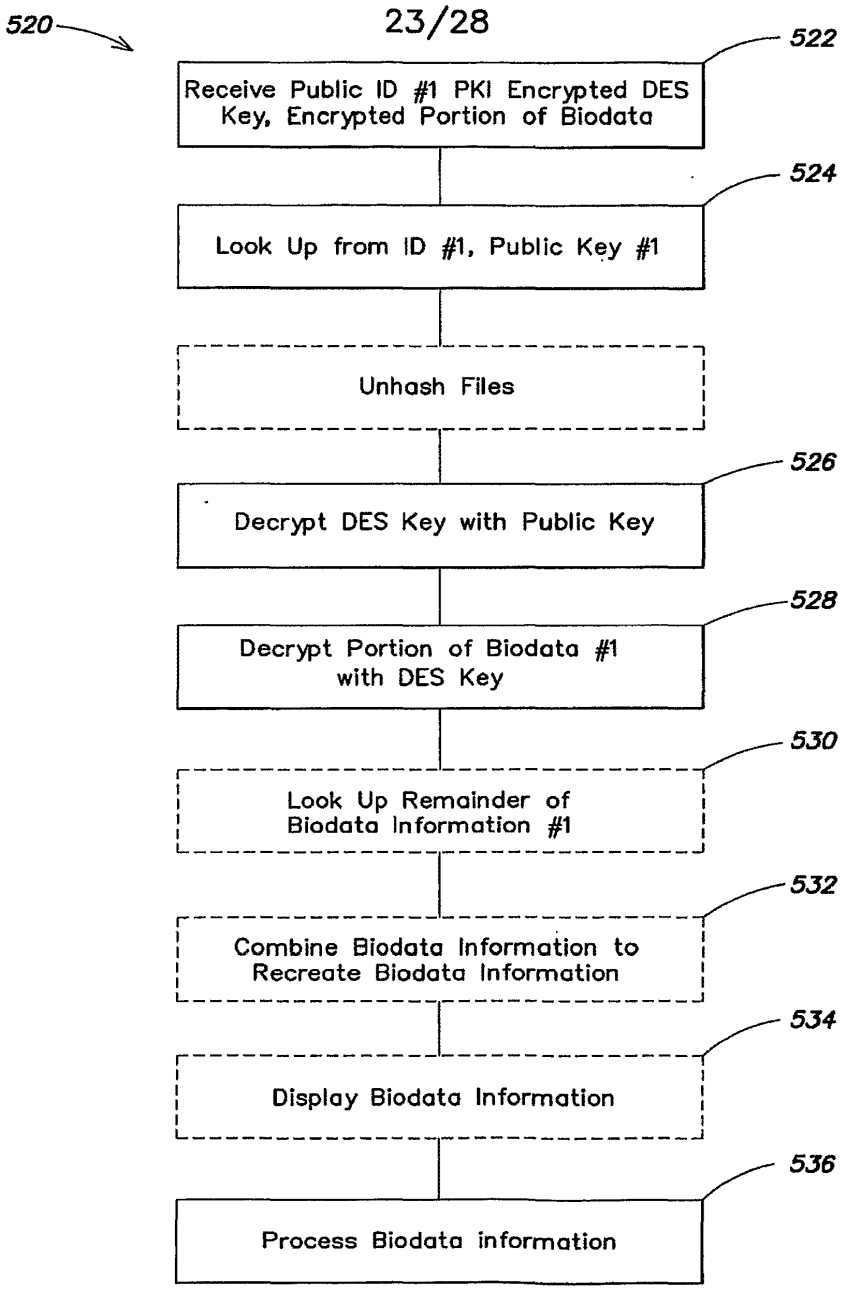


FIG. 25

IPR2025-01150
Apple EX1071 Page 1256

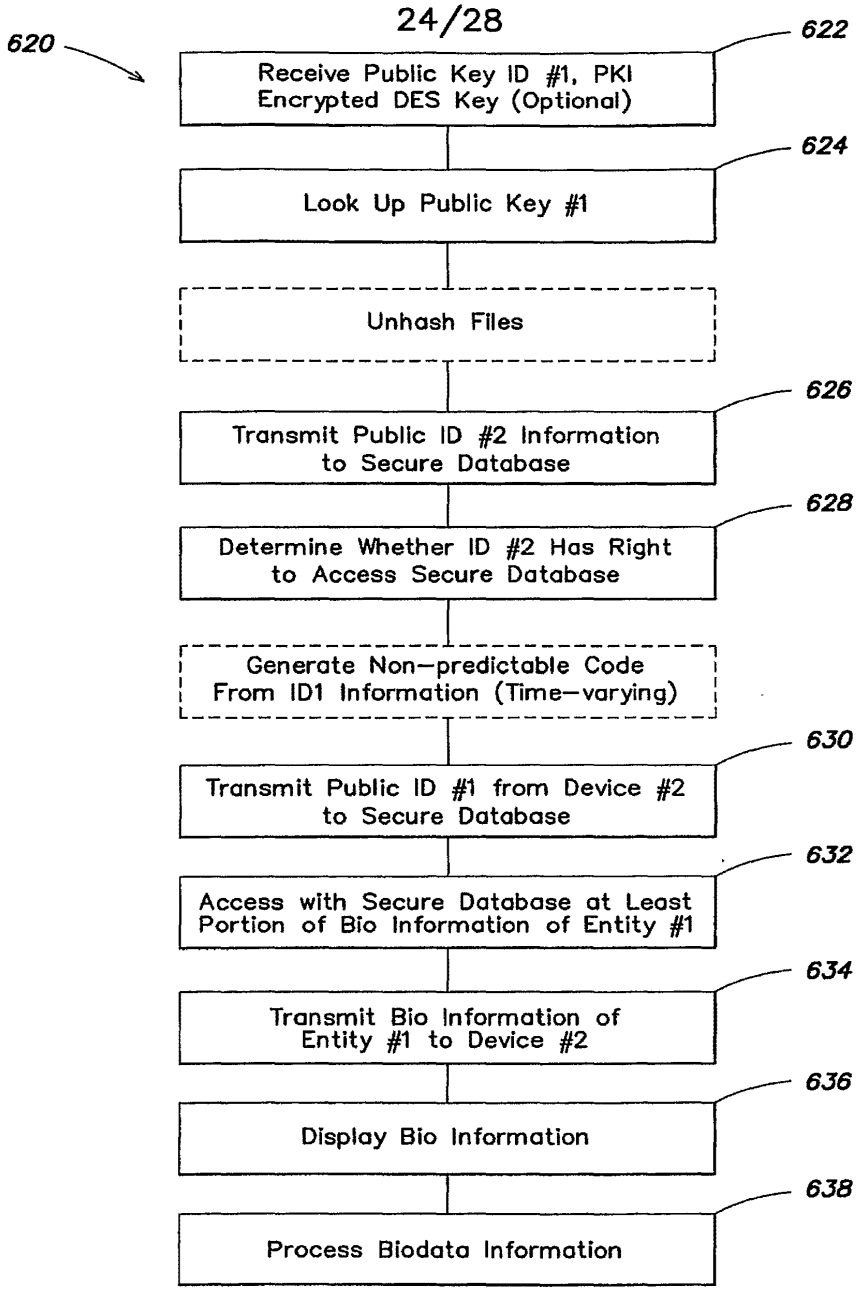


FIG. 26

IPR2025-01150
Apple EX1071 Page 1257

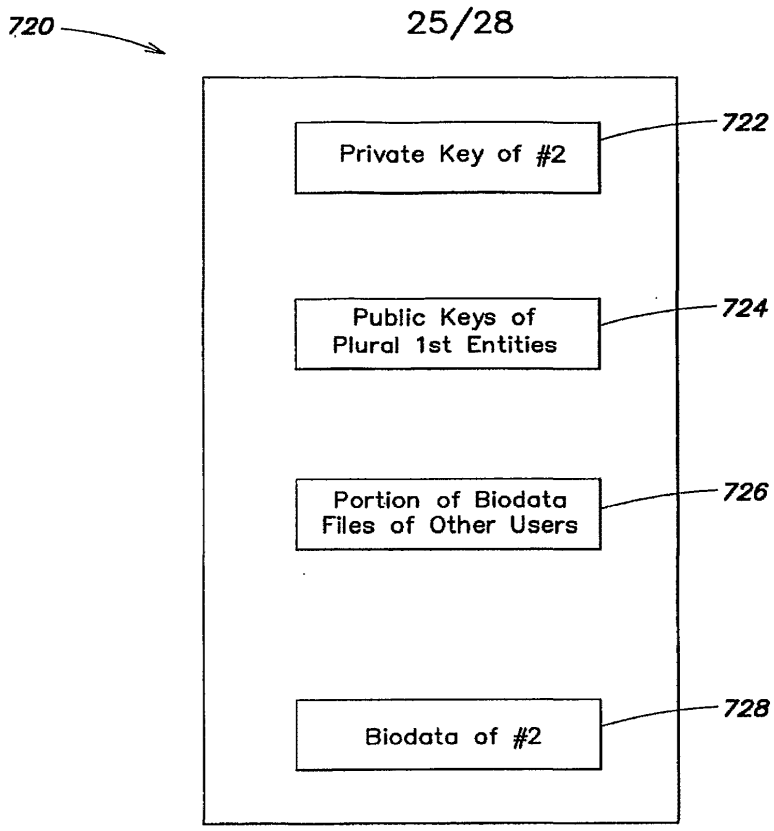


FIG. 27

IPR2025-01150
Apple EX1071 Page 1258

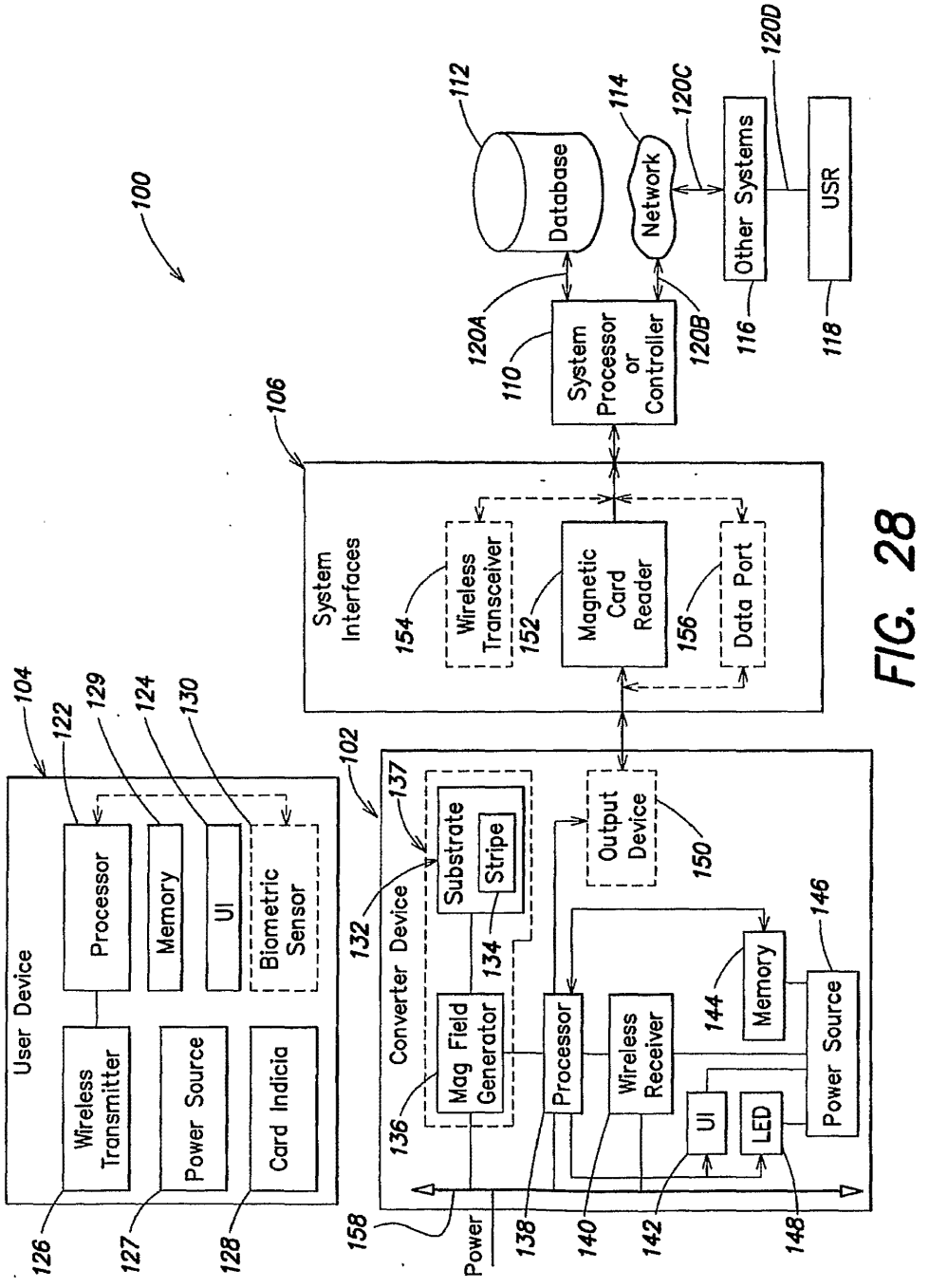


FIG. 28

IPR2025-01150
Apple EX1071 Page 1259

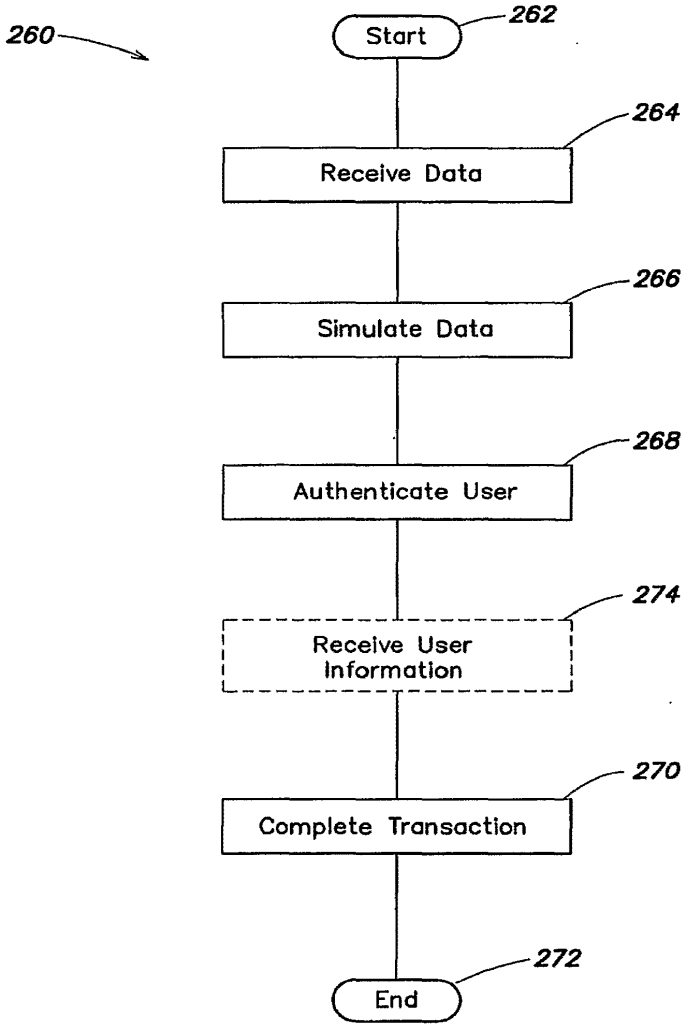


FIG. 29

IPR2025-01150
Apple EX1071 Page 1260

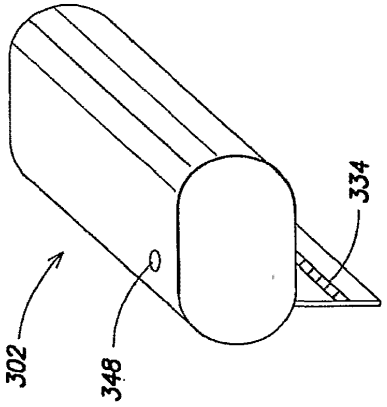


FIG. 30B

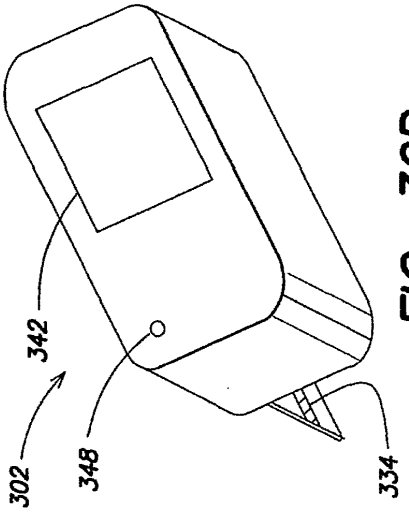


FIG. 30D

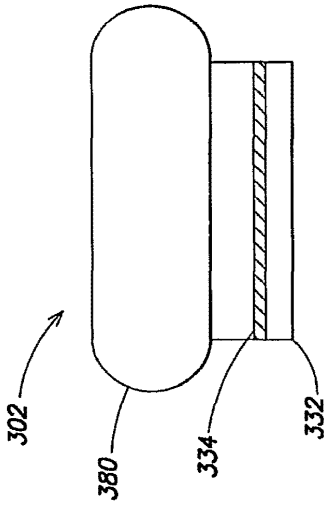


FIG. 30A

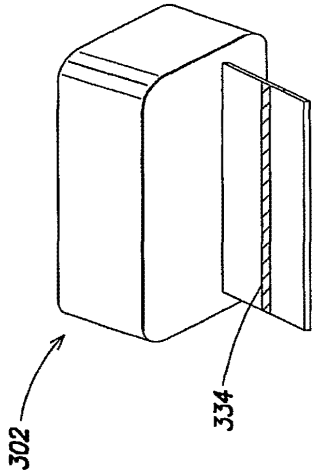


FIG. 30C

IPR2025-01150
Apple EX1071 Page 1261

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/004646

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 382 006 A (IBM [US]) 14 May 2003 (2003-05-14) figure 3 page 4, line 29 - line 34 page 17, line 10 - line 27 page 18, line 5 - line 24	1,63
Y		2-9,13, 20-22, 64-84
Y	US 2005/001711 A1 (DOUGHTY RALPH O [US] ET AL) 6 January 2005 (2005-01-06) paragraph [0012] paragraph [0061]	2-9,13, 20-22, 64-84

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 November 2007	27/11/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Chabot, Pedro

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2007/004646

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☒ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

1-9,13-14,20-22,63-84

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

IPR2025-01150
Apple EX1071 Page 1263

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1,63

   Giving authorization for an operation to a second device by a third device depending on information given by a first device.

   ---

2. claims: 2-9, 20-22, 13-14,64-84

   Emulating a credit card and providing the services associated to the credit card.

   ---

3. claims: 10-12, 38-41,46,47, 100-103, 108-109

   Secure communications between the first and the second devices using cryptography.

   ---

4. claims: 15-19, 24-32, 86-94

   Different methods of authenticating the user at a second the device, using user information sent from the first device.

   ---

5. claims: 33-37, 95-99

   Accessing user information from a data base by the secure system. The secure system access user authentication information and send it to the second device.

   ---

6. claims: 42-45, 48-62, 104-107, 110-124

   Authentication of a user at a first device, a second user at a second device, sending authentication information from the first device to the second to authenticate the first user at the second device. Permit two users to manipulate their respective devices and authenticate the one first user by the second via information sent from the first device to the second.

   ---

7. claims: 23,85 125, 129

   Send to credit card information for validation at a credit card service.

   ---

8. claims: 126-128, 130-132

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Information validation based on information sent from a first and third devices to a second device.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/004646

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2382006 A	14-05-2003	NONE	
US 2005001711 A1	06-01-2005	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
G06F 17/60, H04K 1/00, H04L 9/00

A1

(11) International Publication Number: **WO 00/62214**

(43) International Publication Date: 19 October 2000 (19.10.00)

(21) International Application Number: PCT/IL00/00211

(22) International Filing Date: 6 April 2000 (06.04.00)

(30) Priority Data:

129361	8 April 1999 (08.04.99)	IL
60/174,476	3 January 2000 (03.01.00)	US

(71) Applicant *(for all designated States except US)*: CLEARTOGO.COM [IL/IL]; Amnon Ve–Tamar Street 12, 46417 Herzliya (IL).

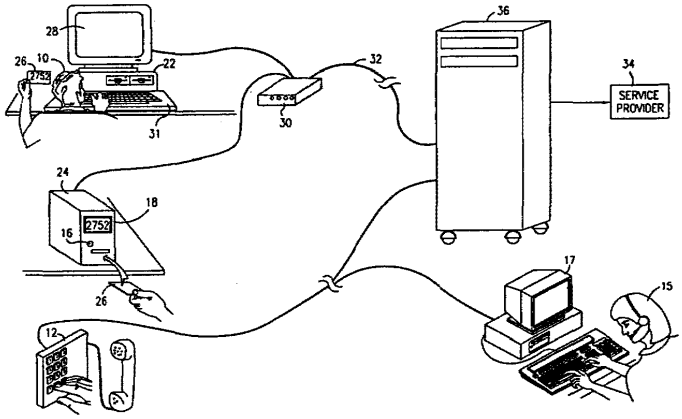
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SOLBERG, Yoram [IL/IL]; Amnon Ve–Tamar Street 12, 46417 Herzliya (IL). BERLIN, Arie [IL/IL]; Yoram Solberg, Amnon Ve–Tamar Street 12, 46417 Herzliya (IL).

(74) Agents: SANFORD T. COLB & CO. et al.; P.O. Box 2273, 76122 Rehovot (IL).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CREDIT CARD SECURITY TECHNIQUE



(57) Abstract

A technique for secure electronic commerce is disclosed wherein a transaction initiator (26) has a primary identifier and a list of secondary identifiers stored therein, each of which is valid for a single transaction. An identification center (36) receives the primary and secondary verification numbers and verifies that the primary number is valid and that the secondary number is appropriate for a current transaction using the primary number. The transaction initiator comprises an enhanced monetary card, such as a credit card or a stored value card, which includes an embedded processor, and which provides the secondary number for each transaction. The secondary numbers are stored in a lookup table, which is also available to the identification center. The values in the lookup table are indexed according to a transaction counter and are preferably communicated to the identification center without encryption or challenge. In some embodiments the transaction initiator comprises other types of hardware such as a personal computer in conjunction with secondary memory such as a CDr for storing secondary numbers and software.

IPR2025-01150
Apple EX1071 Page 1267

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Credit Card Security Technique

BACKGROUND OF THE INVENTION

1. Field of the Invention.

The present invention relates generally to the execution of remote transactions, and to the secure transmission of identification data over insecure channels. More particularly the invention relates to authentication in monetary transactions and electronic commerce, and in other fields such as cellular telecommunication, electronic document transmission, application service providers, and home banking transactions over public communication networks.

2. Description of the Related Art.

Commerce over open public networks, such as the Internet and telephone lines, especially cellular telephones, is rapidly increasing. Generally, it is desired to use public networks to pass a credit card number from a user who constitutes a first party of a transaction to a service provider who constitutes a second party of the transaction. However, unauthorized users may easily listen to data passed over the open network, and thus gain access to credit card numbers and use them for unauthorized transactions. Furthermore, regular telephone calls and transactions over point to point networks, such as specially established computer connections, are not immune from unauthorized use, especially due to the wide number of service providers who receive credit card numbers from users. It is also known that at the present time merchant credit card databases are notoriously insecure, and prone to hacking attacks.

A most serious problem is the possibility of hackers obtaining access to credit card numbers and personal information stored in merchant databases, and appropriating them for unauthorized transactions or illegal resale. Consequently, the consumer is reluctant to expose his credit number to the Internet. This problem is solved by the present invention, which provides the consumer with a degree of security heretofore unknown, yet preserves the convenience and advantages of electronic commerce. Various encryption methods have been proposed to overcome unauthorized determination and use of the credit card number. In such methods only the user (or a computer of the user) and the credit card provider have access to the rules of encryption and decryption. However, technologies to break encryption schemes are being developed as rapidly as the encryption schemes themselves.

Digital signature schemes are also well known in the art. In a conventional signature scheme, a user has a public code and a secret code. The user sends a digital "signature" which can be easily verified using only the public code, but may be generated efficiently only with knowledge of both the public and secret codes. However, such schemes have been successfully attacked by forgers, using methods such as an adaptively chosen plaintext attack which is described, for example, in U.S. Patent No. 5,016,274 to Micali *et al.*, which is incorporated herein by reference. U.S. Patent No. 5,016,274 suggests a more complex method, which can be performed partially off-line before the message is chosen. However, it is commonly believed that as computer hardware and software develops any code may be successfully attacked. Also, the coding and decoding require large computation resources

PCT publication WO96/34471, which is incorporated herein by reference, suggests using, for identification of credit card users, a unique calling party identification code which is passed from the telephone of a user to a network switch. Such a unique code, referred to as a calling party identifier number (CPIDN), limits the credit card user to performing transactions only from specific telephone numbers.

In U.S. Patent No. 5,991,412 to Wissenburgh *et al.*, a method is proposed for protecting transactions involving a smart card and a terminal, such as a cash register. Security is provided by having the terminal (e.g. a cash register) provide a random number to the smart card. The smart card then responds by generating a first authentication value, which could be an incrementing counter, and a first authentication code, which may be an encrypted form of the random number combined with the first authentication value, and also combined with the balance sought to be transferred. The terminal supplies a different random number for each subsequent transaction, and the smart card responds with a different authentication value. In a further step, a second authentication code is provided by the terminal to the smart card which is an encrypted version of the smart card's new balance and a second random number, again generated by the terminal.

U.S. Patent No. 5,559,887 to Davis *et al.* discloses a financial transaction system, adapted to smart cards, in which encrypted certification signals are employed to establish a secure session using any of a plurality of transaction devices, or transaction processors. Among the various devices or processors disclosed in the system are vending machines, collection devices, off-line terminals, and various processors used for internetwork financial settlements. En-

IPR2025-01150
Apple EX1071 Page 1270

cryption is accomplished using the conventional data encryption standard DES. The smart card, which is typically a stored value card (SVC), stores a unique card identification number, a transaction count, a derived password, and the identification number of the issuing entity or financial institution. Each smart card is provided with a unique set of keys derived from a master set maintained in a separate secure location. These keys are derived by an encryption technique from a set of master keys maintained by a card issuing entity.

Blind signatures are used in smart cards to form a monetary transaction system. Each blind signature represents a specified amount of money and may be used only once. A verification system may verify that a user is entitled to use a specific blind signature and that the blind signature was not used already. However, use of blind signatures is very limiting when it is desired to perform transactions which involve arbitrary sums, as is common with credit cards.

Similar verification systems are used in cellular and wireless phones to prevent unauthorized use of a phone line. For example, the Panasonic KX-TC256BX-W model wireless phone, selects a different one of 65,000 security codes each time the handset of the phone is placed on the base. In order to initiate a call, this code must be transferred from the handset to the base. However, in some cases the users of wireless phones do not place the handset on the base for a few days, providing sufficient time for an unauthorized user to determine the security code and use the phone line.

In cellular communications based on the GSM standard, in order to make a cellular call, a user must insert a dedicated "smart card" into the telephone handset. The card includes a private key number. When a call is initiated, a cellular switching center sends the handset an authentication message, indicating a proprietary algorithm which is used by a processor in the handset together with the private key to return an authentication response to the switching center. Only if the response is correct will the handset be allowed to initiate the call. This method is computationally intensive and is not suitable for all purposes.

SUMMARY OF THE INVENTION

It is an object of some aspects of the present invention to provide methods and apparatus for securely performing transactions over public networks.

It is another object of some aspects of the present invention to provide simple methods and apparatus for securely performing remote transactions which do not require complex coding or decoding.

It is another object of some aspects of the present invention to provide methods and apparatus for securely performing remote transactions which are immune to systematic access attacks.

It is another object of some aspects of the present invention to provide methods and apparatus for preventing unauthorized users from deriving identification information of a transaction and using the information to perform unauthorized transactions.

It is still another object of some aspects of the present invention to provide methods and apparatus for securely performing monetary and non-monetary transactions, in which an unauthorized person who derives identification information passed from a credit card to a verification station does not have sufficient information to perform unauthorized transactions.

In aspects of the present invention, a first party to a transaction uses a device, referred to herein as a transaction initiator, which is identified by a fixed primary identification number and a varying secondary identification number. An identification center (or centers) receives the primary and secondary verification numbers and verifies that the primary number is valid and that the secondary number is appropriate for a current transaction using the primary number. Optionally the secondary numbers can be stored on other devices such as a CD, or in software that may be loaded into a computer.

In some aspects of the present invention, the transaction initiator comprises a transaction card, such as a credit card or a stored value card, which includes an embedded processor which provides the secondary number for each transaction. The stored value card may use the secondary number in performing purchase transactions and/or to perform reloading transactions.

In other aspects of the present invention, the transaction initiator comprises a cellular or wireless phone, and the secondary number is provided separately for each phone call or number of phone calls. The identification center is accordingly within the base of the wireless phone or within a cellular switching center which provides services to the cellular phone.

In still other aspects of the present invention, the transaction initiator may be used to monitor access to sensitive information, such as, bank accounts, health information, etc.

Preferably, the secondary number is passed from the transaction initiator to the identification center over the telephone, either by dialing appropriate numbers or by voice, over the Internet or other computer connections, facsimile, or any other suitable communication mechanism. In some embodiments the secondary number is passed in an unencrypted format.

IPR2025-01150
Apple EX1071 Page 1272

In some aspects of the present invention, the secondary number is selected from a look up table (LUT) of values of the secondary number. Preferably, the LUT includes a series of random or pseudo-random numbers which do not allow determination of a next number in the series based on some or even all of the previous numbers in the series. Identical copies of the LUT are kept both in the transaction initiator and in the identification center.

Preferably, the secondary identification number is selected according to a rule based on external data known both to the transaction initiator and the identification center. The external data includes at least some information unrelated to the transaction. Preferably, the rule is entirely unrelated to the details of the transaction, such that the secondary number may be provided before the details of the transaction are known. Alternatively, the rule is partially based on external data related to the transaction, such as the date, time and/or sum of the transaction. In a preferred embodiment of the present invention, the rule is based on the number of transactions performed using the transaction initiator. Preferably, the secondary identification numbers are retrieved sequentially from the LUT.

In some aspects of the present invention, each of the secondary numbers in the LUT may be used only once. When all of the entries in the LUT are exhausted, the transaction initiator is replaced or is refilled with new secondary numbers. Preferably, a display on the transaction initiator notifies the user of the card when the number of secondary numbers remaining therein is below a predetermined value. Alternatively, when all of the entries in the LUT are exhausted, the secondary numbers in the LUT are reused using the same or a different access rule. The LUT in an authentication server may store some keys and algorithms from which a secondary number can be generated. This avoids the storage of actual secondary numbers which could be detected by an unauthorized person, and provides an additional line of defense against hacking of the authentication server.

In some aspects of the present invention, both the transaction initiator and the identification center keep track of an entrance key to the LUT. Each time a transaction is performed, the entrance keys are updated according to the rule. Alternatively or additionally, when the identification center is not connected on-line to the parties performing the transaction, the entrance key is updated by the transaction initiator only a few minutes after the transaction is performed in order to allow sufficient time for the identification center to receive notification of the transac-

tion. Preferably, transactions performed during these few minutes use the same secondary number. Alternatively, during these few minutes another transaction may not be initiated.

Alternatively or additionally, the secondary number is determined or changed according to a predetermined function without the use of a LUT. The predetermined function may comprise a pseudo-random function or any other function which does not allow easy determination of the next secondary number based on a series of previous secondary numbers. Additionally or alternatively, the function is partially dependent on details of the transaction, such as, the date and/or time of the transaction, and/or the monetary sum of the transaction.

An unauthorized user who intercepts the primary and secondary identification numbers cannot use the intercepted data to perform any transactions since the unauthorized user knows only one possible secondary identification number and furthermore does not know the rule which governs the changes of the secondary number.

In some aspects of the present invention, the LUT is implemented by a memory or logic chip, such as a programmable logic array (PLA), which cannot be read by an external reader. Thus, even one who holds the transaction initiator cannot make a copy of the LUT.

In some aspects of the present invention, the transaction initiator includes a display which presents the secondary number, and a switch or button for indicating the completion of a transaction. When a transaction is to be performed the holder of the initiator reads the secondary number from the display and passes it to the other party in the transaction or directly to the identification center. Thereafter, the user presses the button to receive a new secondary number. Alternatively, the user presses the button before the transaction is performed, and only then the secondary number is displayed. Further alternatively, a secret code is necessary to display the secondary number, so that the transaction initiator cannot be used even if an unauthorized user has possession of the transaction initiator.

In some aspects of the present invention, a monetary card-reader reads both the primary and secondary numbers and instructs the processor to change the secondary number once the number was read. Preferably, the card-reader is connected to the center to verify the primary and secondary numbers.

In some aspects of the present invention, the card-reader may be coupled to a personal computer in order that a user of the personal computer may easily perform transactions over the Internet. Alternatively or additionally, the monetary card includes a display window which

shows the secondary number. When a user desires to perform a transaction over the Internet and the identification number of his card is requested, the user types in the primary number of the card and the secondary number from the display window. If the transaction was successful, the user is instructed to notify the card to update the secondary number, for example, by pressing a button on the card. Alternatively or additionally, the user may be required to sign his signature or give his finger print in order to update the secondary number.

In some aspects of the present invention, each card may have three identification numbers: a card identification number which is generally imprinted on the card, a secret code which is known only to the user and prevents unauthorized use of the card in case it is lost, and the secondary number which changes with each transaction. It is noted that the term "identification number" is used herein in a general way to refer to any type of code.

It is noted that the present invention may be used together with other coding schemes which may be used to code the primary and/or secondary identification numbers.

In some aspects of the present invention, when the identification center encounters an attempt to perform a transaction with an incorrect secondary number, the use of the transaction initiator is suspended in order to prevent continuous attacks directed to determine the secondary number. Preferably, the secondary number on which a possible attack was performed may not be used to perform a transaction, and the next secondary number must be used. Preferably, when a suspended transaction initiator requests to perform a transaction, the identification center requests that it provide the correct secondary number to remove the suspension. Only then may a new transaction be performed using the next secondary number.

According to some aspects of the invention, a virtual credit card number is provided for a first credit card company, suitable for co-branding with a second credit card company. A fixed identifier, such as a specific prefix (4-5 digits) indicates that a credit card is associated with the first credit card company, while the rest of the identifier may contain identifying information and a current secondary number. In this case the virtual credit card is suitable for a one-time transaction.

In some aspects of the invention, credit card transactions can be conducted in a manner that protects merchant databases and consumers by omitting the storage of primary credit card numbers in the merchant databases, instead utilizing one-time secondary identification numbers.

IPR2025-01150
Apple EX1071 Page 1275

The invention provides a method of performing a remote transaction, which is performed by initiating a first communication link between a first party and a second party. The first party has a fixed primary identification. At the first party, a variable secondary identification is selected from a list carried by the first party, responsive to a predetermined rule. The secondary identification is transferred from the first party to the second party via the first communication link. A second communications link is established between the second party and an authentication center, the secondary identification is communicated from the second party to the authentication center via the second communications link. The authentication center is aware of the fixed primary identification of the first party. The method further includes verifying at the authentication center that the secondary identification is a permissible identification for performing the transaction, establishing a third communications link between the authentication center and a payment processing agent, and communicating the fixed primary identification from the authentication center to the payment processing agent via the third communications link.

According to another aspect of the invention the method further includes establishing a fourth communication link between the first party and the authentication center, and communicating the secondary identification from the first party to the authentication center via the fourth communication link.

According to yet another aspect of the invention the first party effects communication on the first communication link using a communication device that has memorized data and program instructions. The data and program instructions may be stored on a CD, or on software which has been transferred to the communication device.

Preferably confidential information is transferred from the first party to the authentication center prior to initiating a first communication link.

According to an aspect of the invention the authentication center associates the secondary identification with the confidential information of the first party, and transfers the confidential information and the fixed primary identification to the payment processing agent.

BRIEF DESCRIPTION OF THE DRAWING

For a better understanding of these and other objects of the present invention, reference is made to the detailed description of the invention, by way of example, which is to be read in conjunction with the following drawings, wherein:

IPR2025-01150
Apple EX1071 Page 1276

Fig. 1 is a schematic view of a system for performing monetary-card transactions, in accordance with a preferred embodiment of the present invention;

Fig. 2 is a schematic view of a monetary card, in accordance with a preferred embodiment of the present invention;

Fig. 3 is a schematic view of a LUT in the monetary card of Fig. 2 and in a compatible identification center, in accordance with another preferred embodiment of the present invention;

Fig. 4 is a flow chart illustrating the actions of an identification center in processing a transaction, in accordance with a preferred embodiment of the present invention;

Fig. 5 is a schematic illustration of a cellular communication system, in accordance with a preferred embodiment of the present invention;

Fig. 6 is a block diagram illustrating an arrangement of electronic commerce suitable for use with preferred embodiments of the invention;

Fig. 7 is a plan view of a transaction card in accordance with a preferred embodiment of the invention;

Fig. 8 is a diagram of a ROM which is a component of the transaction card shown in Fig. 7;

Fig. 9 is a perspective view of a transaction card in accordance with an alternate embodiment of the invention;

Fig. 10 is a block diagram of the electronic circuitry of the transaction card illustrated in Fig. 9;

Fig. 11 illustrates a check out form of a merchant site to be completed by a consumer;

Fig. 12 illustrates a merchant's version of a check-out form similar to the form shown in Fig. 11;

Fig. 13 illustrates information which is stored in a central authentication server in the arrangement of Fig. 6;

Fig. 14 illustrates an arrangement of electronic commerce in accordance with an alternate embodiment of the invention;

Fig. 15 is a block diagram of an arrangement of an authentication server in a system of electronic commerce in an alternate embodiment of the invention;

Fig. 16 illustrates an arrangement of electronic commerce in accordance with another alternate embodiment of the invention; and

Fig. 17 is a block diagram illustrating an arrangement of electronic commerce in accordance with another alternate embodiment of the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following description, numerous specific details are set forth in order to provide a through understanding of the present invention. It will be apparent however, to one skilled in the art that the present invention may be practiced without these specific details. In other instances well known circuits, control logic, and the details of computer program instructions for conventional algorithms and processes have not been shown in detail in order not to unnecessarily obscure the present invention.

Fig. 1 is a schematic view of a system for performing remote monetary-card transactions, in accordance with a preferred embodiment of the present invention. A user 10 performs a remote transaction with a service provider 34 using details of a transaction card 26. Card 26 preferably comprises either a credit card or a stored value card, and is also referred to in the context of the present patent application and in the claims as a type of "transaction initiator." Some of the details of card 26 vary for each remote transaction, as described hereinbelow. An identification center 36 receives the details of card 26 and verifies that the card is valid and that the details are compatible with the current transaction. Identification center 36 receives the details of card 26 either directly from user 10 as described hereinbelow, or from service provider 34, which in turn receives the details from user 10. If the details of card 26 allow performance of the transaction, identification center 36 notifies service provider 34, and the transaction is carried out. Preferably, identification center 36 also notifies user 10 of the successful completion of the transaction, whereupon the user updates the details of card 26 as described hereinbelow.

Preferably, user 10 relays the details of card 26 via a telephone 12, either by reading the details to an operator 15 or by inputting the details directly to service provider 34 or identification center 36, using the telephone keypad, for example, as is known in the art. Alternatively or additionally, user 10 may send the details to operator 15 using e-mail, fax, etc. The details of card 26 can optionally be automatically transmitted via an e-wallet platform, in which case the consumer does not have to type in the details.

Alternatively or additionally, the details of card 26 are read by a card reader 24, which passes the details, preferably via a modem 30 and a communication line 32, to server 36. Preferably, reader 24 includes a display 18 which shows the details of card 26, and a button 16

which is actuated by user 10 to update the details of card 26 when and as required. Preferably, reader 24 operates with any compatible card 26. Alternatively, each card 26 operates only with specific readers 24, so that an unauthorized user who finds card 26 cannot perform remote transactions using the card without having the proper reader 24.

In some aspects of the present invention, reader 24 updates the details of card 26 automatically upon acknowledgment of the transaction by identification center 36, before card 26 is ejected from the reader. Alternatively, the details are updated when a transaction is initiated or when a significant number of steps of the transaction have been performed, without acknowledgment from identification center 36. Preferably, reader 24 comprises an additional button (not shown) which may be used to cancel an update which was performed erroneously.

Further alternatively or additionally, user 10 establishes a computer connection with service provider 34, using a computer 22. The computer connection is established either through a direct computer link or through a public network such as the Internet. When user 10 desires to perform a monetary transaction, computer 22 prompts the user (for example, by displaying an appropriate message on a display 28) to enter the details of card 26. Preferably, the details are entered through a keyboard 31. Alternatively or additionally, reader 24 may be coupled to computer 22 so that the details are automatically passed to computer 22. Thereafter computer 22 passes the details of card 26 to identification center 36 via modem 30

An individual who eavesdrops on the traffic on link 32 cannot determine sufficient information to perform remote transactions using card 26, because the details of the card change between transactions. Preferably, by the time the eavesdropper determines the current details passed on link 32, a transaction has been completed, and an additional transaction cannot be performed using these details.

Fig. 2 is a schematic view of card 26, in accordance with a preferred embodiment of the present invention. Card 26 has a primary identification number which identifies the card. Preferably, the primary number appears in an embossment 66 on card 26, as is known in the art. Preferably, card 26 includes an embedded memory 52 which stores a look-up table (LUT) of secondary identification numbers. Card 26 preferably also includes an embedded processor 50, which generates and/or updates a key for access to the LUT. Preferably, processor 50 comprises a simple counter, and the key is an indexing integer number whose maximum value is of the size of the LUT.

Alternatively or additionally, the key is chosen according to a more complex rule, for example one which is partially dependent on the time, date and or sum of the transaction. It is noted however, that the rule is at least partially dependent on external data not related to the details of the specific transaction. Further alternatively or additionally, processor 50 calculates the secondary number directly without access to a LUT. In such a case, processor 50 generates and applies a pseudo-random number, so that it is substantially impossible to determine the next secondary number based on a short sequence of secondary numbers. Preferably, memory 52 comprises or is coupled to a programmable logic array (PLA) which cannot be read by an external device. Other memory devices may also be used, including memories internal to processor 50.

Card 26 preferably comprises a display 54, such as an LED or LCD display, which shows the secondary number. Preferably, card 26 comprises an additional display 56, which shows the index of the secondary number in the LUT. Card 26 preferably further comprises a button 58 which is actuated by user 10 to change the secondary number. Alternatively, card 26 comprises a privileged input device which may only be actuated by a user who knows a proper code. For example, card 26 may comprise a signature receiving pad, and the card provides a new secondary number only if the signature resembles the signature of the true owner of the card. Thus, even if an unauthorized person has access to card 26, the person cannot use the card more than once without properly signing the signature of the card's owner.

In a preferred embodiment of the present invention, card 26 comprises an additional button 59 which undoes the operation of button 58 in case it was erroneously pressed. Alternatively or additionally, card 26 comprises a keypad (not shown) for entering data and commands to the card.

In a preferred embodiment of the present invention, processor 50 includes an internal clock, which keeps track of the current date and/or time.

Fig. 3 is a schematic illustration of a LUT 70 in memory 52 and a compatible LUT 72 in identification center 36, in accordance with a preferred embodiment of the present invention. LUT 70 comprises a plurality of entries of secondary numbers, in a predetermined order, such that there is substantially no correlation between the entries in the LUT. Specifically, the secondary numbers are preferably chosen randomly so that from the knowledge of a sequence of a few secondary numbers, it is not possible to deduce the next secondary number. Preferably,

LUT 70 comprises a large number of entries, for example between 1,000 and 10,000 entries, although the LUT may comprise substantially any number of entries. Preferably, each entry to LUT 70 is used for only a single transaction. Alternatively, once all the entries of the LUT are used, the entries of the LUT are reused.

LUT 72 in identification center 36 is an identical copy of LUT 70 in memory 52. For each card 26, identification center 36 comprises, in addition to LUT 72, an index 74 to the current entry in the LUT, and a status variable 76. Index 74 points to the same entry as is pointed to by processor 50, and is updated in the same manner and preferably at the same time as the index in processor 50. Status variable 76 states whether card 26 is ready for use or is suspended due to a possible unauthorized use, as described hereinbelow.

Fig. 4 is a flow chart illustrating the actions of identification center 36 in processing a transaction, in accordance with a preferred embodiment of the present invention. When a user of card 26 desires to perform a remote transaction, identification center 36 receives the primary number of card 26. Identification center 36 checks that the primary number is of a valid card, and preferably also checks for a password, if a password is associated with card 26. Thereafter, identification center 36 checks whether card 26 was suspended due to a possible attempt to illegally use the card. If the card is not suspended, index 74 (having a value N) is updated according to a rule known both to center 36 and processor 50. In a preferred embodiment of the present invention, the rule is a simple incrementation. Thereafter, user 10 is requested to enter the secondary number having index N in LUT 70. Alternatively, user 10 is requested to enter the current secondary number without stating the current index. Preferably, user 10 keeps track of the current index by pressing button 58 each time a transaction is successfully concluded, as described hereinbelow.

If the secondary number is correct, approval of the transaction is passed to service provider 34. Preferably, user 10 is prompted to press button 58 so as to update the index to LUT 70 of card 26. However, if the secondary number from user 10 is incorrect, the card is preferably set to a suspended status, as indicated by status variable 76. Thus, it is not possible to determine the secondary number by continually guessing. The user is preferably immediately allowed to attempt to get card 26 out of the suspended status by entering the requested secondary number. Alternatively, the user must re-enter the primary identification and password in order to attempt to get card 26 out of the suspended status. If the secondary number is correct, status

variable 76 is set to ready, index 74 is incremented, and user 10 is preferably prompted to press button 58 so as to update the index to LUT 70. In order to perform the transaction, user 10 is requested to enter the next secondary number. Thus, an unauthorized user who succeeds in determining a secondary number in a systematic attempt to get card 26 out of its suspended status, still cannot perform a transaction without guessing the succeeding secondary number in a single try. On the other hand, if the card was suspended due to a mistake, all that is needed in order to cancel the suspension and perform a transaction is to enter two numbers.

Preferably, user 10 is instructed to press button 58 upon conclusion of the transaction. Alternatively, user 10 presses button 58 immediately before performing a transaction.

Alternatively or additionally, each time a transaction is performed, identification center 36 sends card 26 a key to be used in the next transaction of the card to point to a selected value in LUT 70. It is noted that an unauthorized listener cannot use the key without knowing the contents of the LUT. Further alternatively or additionally, center 36 may send to processor 50 a function or set of commands to be performed in providing the secondary number for the next transaction.

Alternatively or additionally, each time a transaction is performed, identification center 36 sends user 10 a random index for which the user must return the corresponding secondary number. In such a case, card 26 preferably comprises a suitable number pad or another user interface for entering the received index. Alternatively or additionally, reader 24 (Fig. 1) comprises a keyboard (not shown) for entering the received index. Thus, card 26 remains relatively simple while allowing relatively large amounts of data to be entered to the card.

Optionally, transactions involving small purchases made in person, which are generally performed by physically passing card 26 through a reader, as is known in the art, do not require use of the secondary number. Alternatively, the secondary number is automatically updated by a reader used in such a transaction.

Fig. 5 is a schematic illustration of a cellular phone 90, in accordance with a preferred embodiment of the present invention. Phone 90 comprises a memory chip 92 which stores a LUT of secondary identification numbers. When a call is initiated from phone 90, identification information is passed from the phone to a base station 94. The identification information includes a secondary number which changes for each call. Thus, an unauthorized user who determines the identification information of phone 90 by eavesdropping on the call between the phone and sta-

IPR2025-01150
Apple EX1071 Page 1282

tion 94 cannot use the information to perform calls. Preferably, base station 94 passes the identification information to an identification center 96 which has an identical copy of the LUT in memory 92, in a manner similar to that described above regarding card 26. Preferably, the process of checking whether the secondary number is correct is performed automatically, without need of any human intervention.

It is noted that although the term secondary number is used to refer to the secondary identification of card 26, any type of identification may be used including letters, symbols, voltage levels, tones, etc.

Application to Electronic Commerce

The invention disclosed herein solves two major problems of electronic commerce ("e-commerce") transactions as well as in offline ones: (a) extensive fraud, causing consumer hesitance in using credit cards, and (b) non-secure merchant credit card databases. The basis for this technology is a specific transaction personal identification number (STP), a code which can be used for one transaction only and then becomes meaningless and cannot be used for future transactions. STPs are generated and ordered randomly and uniquely, or are created using an STP generation algorithm and thus STPs applying to subsequent transactions cannot be determined by detecting a currently transmitted STP, even after decryption. The STP generation algorithm can be dependent on several parameters such as time, personal details, transaction information or personal password. At the time that the STPs are created they are mirrored in a database file which exists in the authentication server.

According to some aspects, the technology of the invention provides consumers with several different options to receive STPs which can be entered at an e-commerce site instead of a credit card number. The user of the device has an optional personal password that makes it impossible for a thief or otherwise unauthorized person to use the device without knowledge of this personal password. A consumer in e-commerce can further prevent unauthorized use by configuring the device, or his account such that only transactions utilizing STPs can be made at e-commerce sites. The stored STPs can also function in e-commerce that is conducted via cellular telephone.

Elements of the system which are disclosed hereinbelow are the consumer's STP device, optional software on the e-commerce site, which can be integrated into the merchant's shopping engine, payment server or a third party e-commerce payment gateway, and the authentication

server, which can be central or distributed. It is further contemplated that the STP device may be provided with loadable software for initial programming and updating.

Fig. 6 illustrates an arrangement for the execution of e-commerce suitable for use with the invention. According to this embodiment the consumer transmits an STP to the merchant. The merchant relays the STP to a secure identification center, which in turn converts the STP to the actual credit card number. The actual credit card number is transmitted by the secure identification center to the next processing entities in the payment chain as disclosed hereinbelow.

An STP device 100 communicates with a merchant e-commerce site 102 over a communications network 104, which is typically the Internet. The merchant e-commerce site 102 is in communication with an authentication server 106 over a network 108, which could also be the Internet, or a private network. The authentication server 106 authenticates the STP device 100 seeking to execute a transaction. Following authentication, the authentication server 106, which is aware of the actual credit card number of the consumer, submits information to a payment processing facility 110, which may be a backend server integral to the merchant e-commerce site 102, or an independent facility such as a third party payment gateway. The payment processing facility 110 communicates via a secure channel 112 with an appropriate credit card transaction processor 114. Thus the merchant stores only the STP in his database, but not the actual credit card number of the consumer. The information retained by the merchant is meaningless to a person wishing to perform future unauthorized transactions. This is an important advantage of the present invention. To the inventors' knowledge, All other existing methods known to the inventors, including smartcards, encryption techniques, and digital signatures, do not prevent the merchant from receiving and storing the consumer's credit card number in his database. The STP device 100 in accordance with one preferred embodiment of the invention is now disclosed in further detail with reference to Fig. 7, wherein the consumer's STP device 116 is a modified transaction card, such as a credit card, which has a screen 118, and a keypad comprising one or more buttons 120 which are used to advance an STP once it has been used, and for other functions. The STP device 100 can also be a cellular phone; personal digital assistant ("PDA"); pager; compact disk; diskette; hard disk (installed via the Internet or via a physical medium); a plurality of conventional credit cards; a sheet of paper with a list of STPs; or any other device which can create, store and or process STPs. If a credit card-like device is used then one or more of the following enhancements may be added in order to conveniently transfer the STP

and other encoded information: a magnetic strip, reader interface, calculator, photosensor, key-pad, microphone, speaker, radiofrequency or infrared interface, and image sensor. As shown schematically in Fig. 8, the STP device 116 holds any number of randomly generated STPs which are either embedded on a read-only memory ("ROM") or erasable programmable read-only memory ("EPROM") chip 122 in the device or created on the fly. Once the number of STPs runs low the device will alert the consumer so that he can simply call the issuing company and receive a new STP device. The STP device 116 may also be constructed as a reusable card which can be recharged with new STPs once they run out, using a reader, the Internet, special software, or other techniques as are known to the art. Once consumers receive their STPs they can add information about other credit cards they may want to use to the information stored in the STP device 116, as well as change the password that they have been given. It should be noted that since the STPs are prestored, no computational resources or time need be dedicated to their generation during execution of the transaction.

In some aspects of the invention the STP is constructed so that part of the number can be constant, signifying personal details about the card holder, such as issuing bank, country, etc., while the rest of the number changes for each transaction. The STP can also be produced through a mathematical integration of these details with the STP. The card also has a serial number 124, which is used only when the consumer deals directly with the company for customer service and reloading of the STP device 116.

Another embodiment of the STP device 116 (Fig. 6)is disclosed with reference to Fig. 9, in which the STP device 116 is realized as an enhanced transaction card 126. The transaction card 126 is provided with a display 128, which is preferably a liquid crystal type, and most preferably has graphic capabilities. In some versions the display 128 could be limited to a 7 segment type for reasons of economy, but it provides at least a single line of 16 characters. A printed coil, magnetic emulator 130, emulates a sequence of magnetic indications that occur when the transaction card 126 is swept through a credit card reader (not shown). It is intended that the user place the transaction card 126 into a card reader, rather than sweeping it, during which period the magnetic emulator 130 will operate to identify the transaction card 126 to the card reader. The magnetic emulator 130 is important mainly when conducting off-line transactions.

The transaction card 126 has lockout capability, which will protect the user against losing the card. In order to activate the card the user will have to enter his code.

The transaction card 126 has a keypad comprising five top pushbuttons 132, which allow the user to create a 5-digit personal code. The card locks itself permanently after three trials. The probability of an unauthorized user breaking this personal code in three attempts is negligible.

A standard smart card interface 134 is provided. The user is thereby afforded the ability to use and program the transaction card 126 as a smart card. The transaction card 126 is able to interface directly with a computer for verification and other purposes, using an infrared receiver 136 and an infrared transmitter 138. It is possible to incorporate other communications features, for example ultrasonic communication or radiofrequency communication using protocols such as HomeRF™ or Bluetooth™.In operation the user places the transaction card 126 in front of a suitably programmed computer, and the transaction will be verified automatically.

The processor 140 of the transaction card 126 is disclosed in further detail with reference to Fig. 10. A single ASIC 142 generally controls the transaction card 126, handles the I/O, and controls the power supply. A battery 144 provides power, and is preferably a poly-lithium flat battery, zinc oxide button battery or a light-powered battery. The battery 144 should provide power for at least 3 years and should allow the transaction card 126 to exceed 5000 operations. Provision is made for self-deactivation of the transaction card 126 after 15 seconds of powered operation.

The memory, preferably a 64 kb PROM 146, is capable of storing up to 10,000 STP numbers, each containing 16 characters (6 bits each). A controller 148 and an ancillary display controller 150 are provided for controlling the display 152, the PROM 146, and a RAM 154, which is used for various computational functions. The controller 148 controls the magnetic strip emulator 156 and the IR interface 158. Programming of the transaction card 126 is accomplished through a standard smart card interface 160. The interaction of the STP device 116 with software on the e-commerce site in accordance with some preferred embodiments of the invention is now disclosed with reference to Figs. 6, 11 and 12.

The consumer fills in the standard check-out form 162 of the merchant e-commerce site 102, and selects a payment method. The consumer is then directed to the appropriate page. The consumer manually fills in the STP number shown on the screen 118 of the STP device 116 (Fig. 7) on the line 164 instead of entering the credit card number. This entry could also be accomplished automatically or via a reader. Additional information which might be entered on

lines 166, 168, and 170, if relevant, are a personal password, the type of credit card being used, and its expiry. Appropriate software to process the consumer's order is integrated into the merchant's shopping engine, payment server or a third party e-commerce payment. Such software is known to the art, and is not further described herein, as it is outside the scope of the invention. An electronic "shopping cart" is filled by iteration of a portion of the check-out form 162 for different products. The product in some cases necessitates minimal changes to the electronic shopping cart, such as adding the card to the credit card list, which can be accomplished through an applications program interface ("API") available to conventional major shopping cart engines and internally developed ones. As shown in Fig. 12, the form 172 can be configured so that it is completely transparent to the merchant. The merchant's transaction directing software is integrated into a payment processing facility 110. This software may direct the transaction to the appropriate payment processing site or server according to the conditions specified by the STP device 100. The STPs can be entered through an e-wallet platform, or can be entered into a special coding area (not shown) within the check-out form 162.

The authentication server 106 stores data on all the STPs that have been issued to consumers, together with the comparable existing credit card numbers or bank account numbers and the consumer's personal details, as shown in Fig. 13. The data that the consumer has entered into the shopping cart is transferred through the payment processing facility 110 to the authentication server 106, together with the merchant identification, and the transaction amount. The authentication server 106 validates that the STP has not been used before, and crosschecks it against at least some of the consumer's name, address, and password. If valid, the transaction is authorized and directed to an appropriate transaction processor 114 which processes it in the same manner as a conventional credit card transaction. The merchant e-commerce site 102 may have commercial relationships with any number of transaction processors 114. The charge is then transferred from the authentication server 106 over the secure channel 112, which is typically a secure leased line, to the designated transaction processor 114, which authorizes the purchase through the card issuing bank specified by the consumer. An authorization number is returned to the merchant e-commerce site 102 via the authentication server 106, and the transaction is approved. The authentication server 106 can optionally send an email to a consumer address 119 via the Internet immediately following every transaction that occurs with an STP under his name with full transaction details. The actual transaction can be carried out using a per-

IPR2025-01150
Apple EX1071 Page 1287

sonal computer or a telephone circuit such as a cellular phone. In this way the consumer can track the purchases and verify that all are legitimate. Alternatively, the consecutive STP or the STP counter number is sent to the consumer in a transaction authorization notice. This is used as a verification signal to the consumer that the STP has indeed reached the authentication server 106.

According to preferred embodiments of the invention, the authentication server can be implemented in either a central or distributed configuration. With the central configuration, which was explained above with reference to Fig. 6, there is a single location for the authentication server 106, which can be realized at one of several dispositions: between the STP device 100 and the merchant e-commerce site 102; between the merchant e-commerce site 102 and the transaction processor 114; between the transaction processor 114 and an issuing bank (not shown); or between an issuing bank and a the server of a credit card company (not shown).

In accordance with an alternate embodiment of the invention, in a distributed configuration, illustrated schematically in Fig. 14, there are a plurality of authentication servers 176, located at a transaction processor 178, at an issuing bank 180, an Internet portal 182, an Internet e-commerce site 184, or at a credit card company 186.

In another alternate embodiment of the invention, which is disclosed with reference to Fig. 15, the authentication server can be realized as a central database server 188 which synchronizes information with a plurality of distributed database servers 190. The distributed database servers 190 are only allowed to hold the next available STP.

The authentication server has several fraud protection mechanisms such as fraud protection algorithms, address verification system ("AVS") checks, illegal user detection, hacking interference and blocks on random number tests, in which users are only allowed to try to enter an STP a small number of times, after which the transaction will be blocked.

In yet another alternate embodiment of the invention, the STP device 100 (Fig. 6) may be realized as a wireless communication device, as shown in Fig. 16. This is similar to the previous embodiments, except now an authentication server 192 accesses the consumer's wireless device 194, preferably over a wireless channel 196. The authentication server 192 includes an STP generator 198, which produces a randomly generated STP which then is displayed on the screen of the wireless device 194. The consumer then enters this STP into the electronic shopping cart in the same manner as disclosed with respect to the previous embodiment. The STP is then

passed back to the authentication server 192, which verifies the data. The authentication server can be either centrally located or distributed. The transaction continues as explained with respect to the previous embodiment. The wireless device 194 communicates information such as the PIN, password and STP to a wireless internet provider 200 over a wireless channel 202, and receives back a transaction acknowledgement on the same wireless channel 202 or another wireless channel 204. It is still possible for the wireless device 194 to communicate directly with a merchant e-commerce site 206 over a conventional telephone line 208. At the conclusion of the transaction the authentication server 192 may communicate a transaction acknowledgment to the wireless device 194 over the wireless channel 196.

In an alternate embodiment of the invention, the consumer dials in to the authentication server through the wireless device 194 and receives an STP, which is displayed on the screen.

In still another alternative embodiment of the invention, the STPs are pre-stored on a ROM or EPROM chip of the wireless device 194. This embodiment has the advantage of increased reliability, as the transmission of the STP on the wireless channel 196 is eliminated.

Referring now to Fig. 17, an alternate embodiment of the invention is now disclosed which is suitable for use by an association of organizations which participate in e-commerce. A consumer 210 is a client of a an e-commerce service provider 212, which is a collaborator in a credit card organization. The consumer 210 has been issued appropriate credentials 214 by the e-commerce service provider 212, which allow the use of its facilities for conducting e-commerce transactions. The credentials 214 preferably include an STP device as disclosed in the previous embodiments. The e-commerce service provider 212 can be a credit card company, or an organization which facilitates e-commerce by providing secure electronic facilities for authentication for the benefit of the transaction participants, and for the transmission of other transaction-related information as will be disclosed in further detail hereinbelow. The consumer 210 is provided with an electronic communications device 216, such as a personal computer, for interfacing with they e-commerce service provider 212 and other participants in the transaction. The communications device 216 may communicate over the public telephone network, a wireless channel, or an Internet. The Internet communication may occur via the World-Wide-Web. Software in the communications device 216 can be periodically updated by downloading from the computing facilities of the e-commerce service provider 212.

IPR2025-01150
Apple EX1071 Page 1289

When the consumer 210 accesses the Internet, using the communications device 216, he is connected immediately to a specialized authentication server 218 which checks from time to time to determine whether the connection has been terminated or is still active. When the consumer 210 desires to make a transaction he completes a check-out form 162 (Fig. 11) and submits it to a merchant web server 222. The transaction information is routed via a payment application server 224, and a gateway processing server 226, ultimately reaching a card issuing bank 228, which is a co-participant in the association. The bank 228 recognizes the relationship between the consumer 210 and the e-commerce service provider 212. The bank 228 then communicates with the authentication server 218 via the gateway processing server 226.

Upon receiving the communication from the bank 228 the authentication server 218 presents the consumer 210 with a pop-up window on the display (not shown) of the communications device 216, and requests the consumer's STP. The consumer 210 inputs the STP, which is returned to the authentication server 218 and authenticated as disclosed above. The result of the authentication is returned to the bank 228 via the gateway processing server 226, and if successful, the transaction process continues in the manner disclosed with respect to the previous embodiments.

In yet another alternate embodiment of the invention, even greater efficiency can be achieved. This is similar to the previous embodiment, except now the consumer 210 includes his STP in the check-out form 162 (Fig. 11) which is submitted to the merchant web server 222, and concurrently to the authentication server 218. Now, when the bank 228 communicates with the authentication server 218, the response is immediate because the authentication server 218 has been expecting a communication in respect of the particular STP. Communication between the consumer 210 and the authentication server 218 can be direct, or via a trusted third party, and by any communications technique, as described above. It may be encrypted or unencrypted. The technology is also applicable to offline shopping methods such as point-of-sale ("POS") shopping or card-not-present methods, such as telephone or mail transactions. This can be accomplished in several ways, for example using a magnetic strip on the card and card reader for telephone transmission. New STPs are loaded into the magnetic strip and from there they are transferred under a conventional offline transaction process into an authentication server. The STPs can be installed in a multi-application smart card or into a stand-alone credit card. The technology can also be used for non-monetary transactions such as building security, medical

file transmission, and fields such as cellular telecommunication, electronic document transmission, application service providers, and home banking transactions over public communication networks.

While this invention has been explained with reference to the structure disclosed herein, it is not confined to the details set forth and this application is intended to cover any modifications and changes as may come within the scope of the following claims:

IPR2025-01150
Apple EX1071 Page 1291

Claims

1. A method for verifying by an identification center permissibility of a remote transaction, comprising:

selecting a variable secondary identification from a list carried by a remote party, said party being remote from said identification center, responsive to a predetermined rule;

transferring said secondary identification together with a primary identification of a transaction initiator to said identification center; wherein said secondary identification is transferred to said identification center in an unencrypted format; and

verifying at said identification center that said secondary identification is a permissible identification for performing said transaction.

2. The method according to claim 1, wherein selecting said secondary identification comprises selecting said secondary identification from a look up table.

3. The method according to claim 1, wherein selecting said secondary identification comprises determining a key to said look up table.

4. The method according to claim 3, wherein determining said key comprises incrementing an index of said key.

5. The method according to claim 3, wherein determining said key comprises receiving said key from said identification center together with acknowledgment of a previous transaction.

6. The method according to claim 1, wherein determining said secondary identification comprises changing said secondary identification responsive to performing a previous transaction.

7. The method according to claim 6, wherein changing said secondary identification comprises changing said secondary identification upon reception of confirmation of said previous transaction from said identification center.

8. The method according to claim 1, wherein said list in said remote party is carried in a memory of a transaction card; and

wherein determining said secondary identification comprises changing said secondary identification responsive to a command of a user of said card.

9. The method according to claim 8, wherein communication between said transaction card and said identification center is effected via a wireless channel.

10. The method according to claim 8, wherein changing said secondary identification responsive to said command comprises changing said secondary identification responsive to an action which uniquely identifies an owner of said card.

11. The method according to claim 1 wherein determining said secondary identification comprises determining said secondary identification responsive to one or more details of said transaction.

12. The method according to claim 1, wherein determining said secondary identification comprises determining said secondary identification irrespective of any details of said transaction.

13. The method according to claim 12, wherein determining said secondary identification comprises determining said secondary identification substantially immediately after a previous transaction.

14. The method according to claim 1, wherein verifying that said secondary identification is a permissible identification for performing said transaction comprises verifying that said secondary identification has not been used before with said primary identification.

15. The method according to claim 1, wherein said secondary identification may be used more than once with said primary identification provided said secondary identification fulfills said predetermined rule.

16. A method for verifying by an identification center permissibility of a remote transaction, comprising:

causing a remote party to initiate a communication link with an identification center, wherein said remote party is remote from said identification center;

at said remote party, selecting a variable secondary identification from a list carried by said remote party, responsive to a predetermined rule;

transferring said secondary identification together with a constant primary identification of a transaction initiator to said identification center; and

verifying at said identification center that said secondary identification is a permissible identification for performing said transaction.

17. The method according to claim 16, wherein said secondary identification is transferred to said identification center in an unencrypted format.

18. The method according to claim 16, wherein selecting said secondary identification comprises selecting said secondary identification from a look up table.

19. The method according to claim 16, wherein selecting said secondary identification comprises determining a key to said look up table.

20. The method according to claim 19, wherein determining said key comprises incrementing an index of said key.

21. The method according to claim 19, wherein determining said key comprises receiving said key from said identification center together with acknowledgment of a previous transaction.

22. The method according to claim 16, wherein determining said secondary identification comprises changing said secondary identification responsive to performing a previous transaction.

23. The method according to claim 16, wherein said list in said remote party is carried in a memory of a transaction card; and

wherein determining said secondary identification comprises changing said secondary identification responsive to a command of a user of said card.

24. The method according to claim 23, wherein communication between said transaction card and said identification center is effected via a wireless channel.

25. The method according to claim 23, wherein changing said secondary identification responsive to said command comprises changing said secondary identification responsive to an action which uniquely identifies an owner of said card.

26. The method according to claim 16 wherein determining said secondary identification comprises determining said secondary identification responsive to one or more details of said transaction.

27. The method according to claim 16, wherein determining said secondary identification comprises determining said secondary identification irrespective of any details of said transaction.

28. The method according to claim 27, wherein determining said secondary identification comprises determining said secondary identification substantially immediately after a previous transaction.

29. The method according to claim 16, wherein verifying that said secondary identification is a permissible identification for performing said transaction comprises verifying that said secondary identification has not been used before with said primary identification.

30. The method according to claim 16, wherein said secondary identification may be used more than once with said primary identification provided said secondary identification fulfills said predetermined rule.

31. A method for verifying by an identification center permissibility of a remote transaction, comprising:

selecting a variable identification from a list carried by a remote party, said remote party being remote from said identification center, responsive to a predetermined rule;

transferring said variable identification to said identification center; wherein said variable identification is transferred to said identification center in an unencrypted format; and

verifying at said identification center that said variable identification is a permissible identification for performing said transaction.

32. The method according to claim 31 wherein selecting said variable identification comprises selecting said variable identification from a look up table.

33. The method according to claim 31, wherein selecting said variable identification comprises determining a key to said look up table.

34. The method according to claim 31, wherein determining said key comprises incrementing an index of said key.

35. The method according to claim 31, wherein determining said key comprises receiving said key from said identification center together with acknowledgment of a previous transaction.

36. The method according to claim 31, wherein selecting said variable identification comprises changing said variable identification responsive to performing a previous transaction.

37. The method according to claim 36, wherein changing said variable identification comprises changing said variable identification upon reception of confirmation of said previous transaction from said identification center.

38. The method according to claim 31, wherein said list in said remote party is carried in a memory of a transaction card; and

wherein selecting said variable identification comprises changing said variable identification responsive to a command of a user of said card.

39. The method according to claim 38, wherein communication between said transaction card and said identification center is effected via a wireless channel.

40. The method according to claim 38, wherein changing said variable identification responsive to said command comprises changing said identification responsive to an action which uniquely identifies an owner of said card.

41. The method according to claim 31, wherein selecting said variable identification comprises selecting said variable identification responsive to one or more details of said transaction.

42. The method according to claim 31, wherein selecting said identification comprises selecting said identification irrespective of any details of said transaction.

43. The method according to claim 42, wherein selecting said identification comprises selecting said identification substantially immediately after a previous transaction.

44. The method according to claim 31, wherein verifying that said variable identification is a permissible identification for performing said transaction comprises verifying that said variable identification has not been used before.

45. The method according to claim 31, wherein said variable identification may be used more than once provided said variable identification fulfills said predetermined rule.

46. A transaction card for performing transactions with a verifying center, comprising:

a primary memory which stores a primary permanent identification; and

an embedded unit having a secondary memory disposed in said transaction card which provides according to a predetermined rule a secondary varying identification which is at least partially based on information non-related to any details of said transaction;

wherein said secondary varying identification is selected from a plurality of memorized identifiers in said secondary memory.

47. The transaction card according to claim 46, wherein said embedded unit comprises a processor which determines an index to said memorized identifiers.

48. The transaction card according to claim 47, wherein said processor comprises a counter of completed transactions, and a value of said index to said memorized identifiers is responsive to a value of said counter.

49. The transaction card according to claim 46, further comprising:

a display screen for displaying a currently selected secondary identification; and

a keypad for data entry by a user; and

a communications interface.

50. A method of performing a remote transaction, comprising the steps of:

initiating a first communication link between a first party and a second party, said first party having a fixed primary identification;

at said first party, selecting a variable secondary identification from a list carried by said first party, responsive to a predetermined rule;

transferring said secondary identification from said first party to said second party via said first communication link;

establishing a second communications link between said second party and an authentication center, and communicating said secondary identification from said second party to said authentication center via said second communications link, wherein said authentication center is aware of said fixed primary identification of said first party;

verifying at said authentication center that said secondary identification is a permissible identification for performing said transaction;

establishing a third communications link between said authentication center and a payment processing agent; and

communicating said fixed primary identification from said authentication center to said payment processing agent via said third communications link.

51. The method according to claim 50, wherein said secondary identification is transferred to said authentication center in an unencrypted format.

52. The method according to claim 50, wherein selecting said secondary identification comprises determining a key to a look up table.

53. The method according to claim 52, wherein determining said key comprises incrementing an index of said key.

54. The method according to claim 50, wherein selecting said secondary identification comprises changing said secondary identification responsive to a previous transaction.

55. The method according to claim 50,wherein selecting said secondary identification comprises selecting said secondary identification responsive to a detail of said transaction.

56. The method according to claim 50, wherein determining said secondary identification comprises determining said secondary identification irrespective of any details of said transaction.

57. The method according to claim 50, wherein verifying that said secondary identification is said permissible identification for performing said transaction comprises verifying that said secondary identification has not been used before with said primary identification.

58. The method according to claim 50, further comprising the steps of:

establishing a fourth communication link between said first party and said authentication center; and

communicating said secondary identification from said first party to said authentication center via said fourth communication link.

59. The method according to claim 50, wherein said first party effects communication on said first communication link using a communication device having memorized data and program instructions.

60. The method according to claim 59, wherein said communication device comprises a CD.

61. The method according to claim 59, further comprising the steps of:

storing a plurality of identification data as software on a media;

transferring said software to said communication device; and

selecting a datum from said identification data for use as said secondary identification.

62. The method according to claim 60, further comprising the step of transferring confidential information from said first party to said authentication center prior to initiating a first communication link.

63. The method according to claim 62, further comprising the step of

at said authentication center associating said secondary identification with said confidential information of said first party; and

transferring said confidential information with said fixed primary identification to said payment processing agent.

FIG. 1

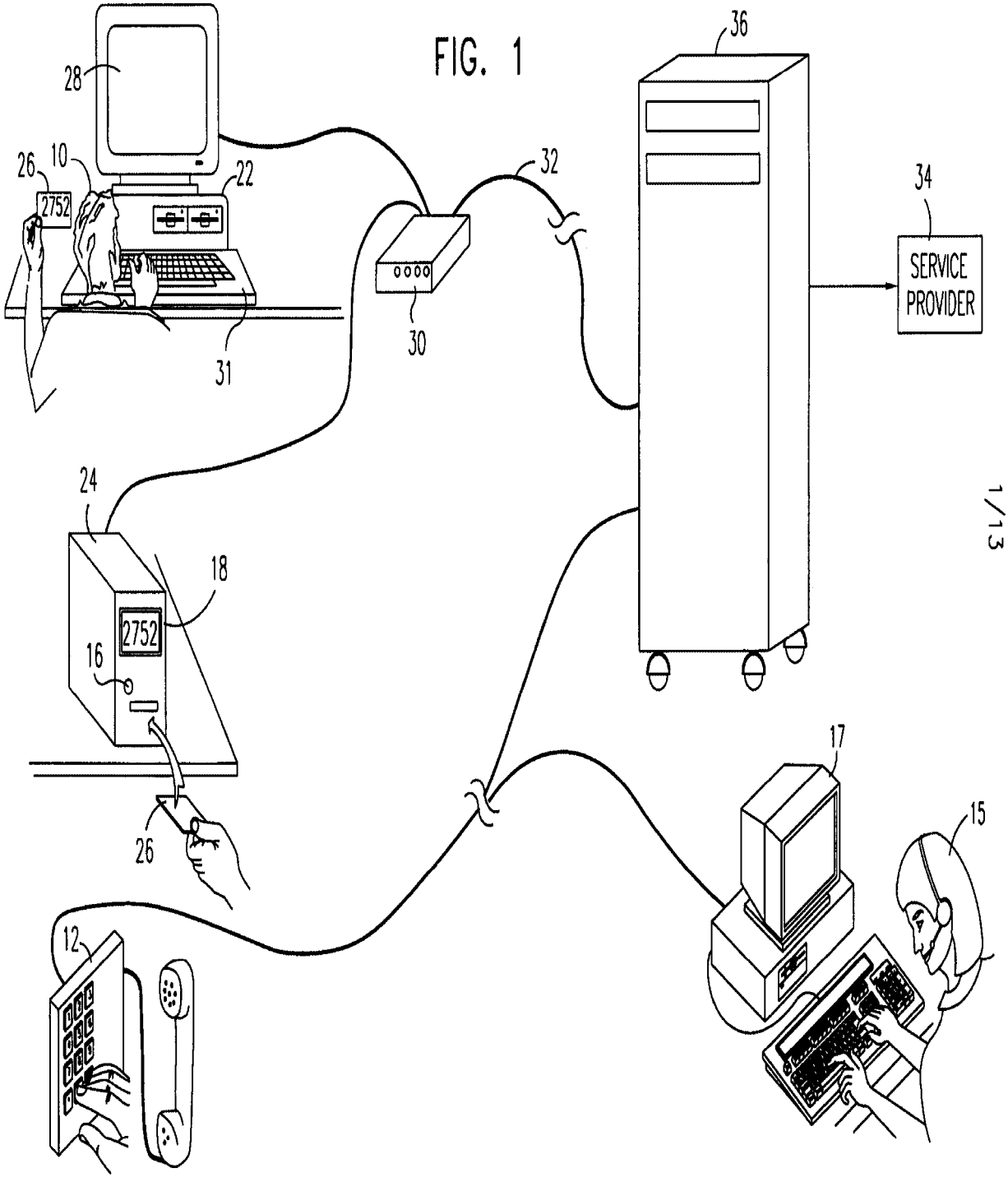

28
10
26
2752
22
31
32
30
36
34
SERVICE PROVIDER
24
18
2752
16
26
17
15
12

FIG. 2

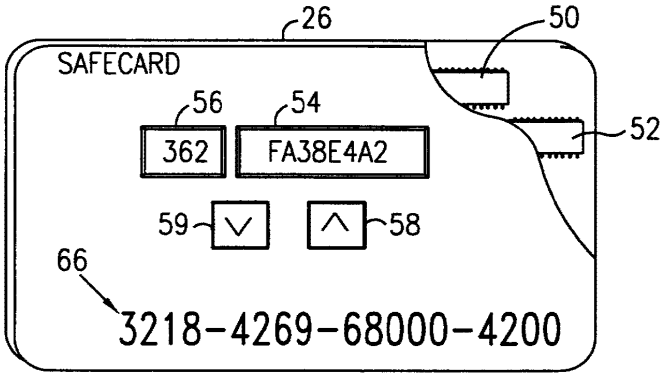

26
50
SAFECARD
56
54
362
FA38E4A2
52
59
58
66
3218-4269-68000-4200

FIG. 3

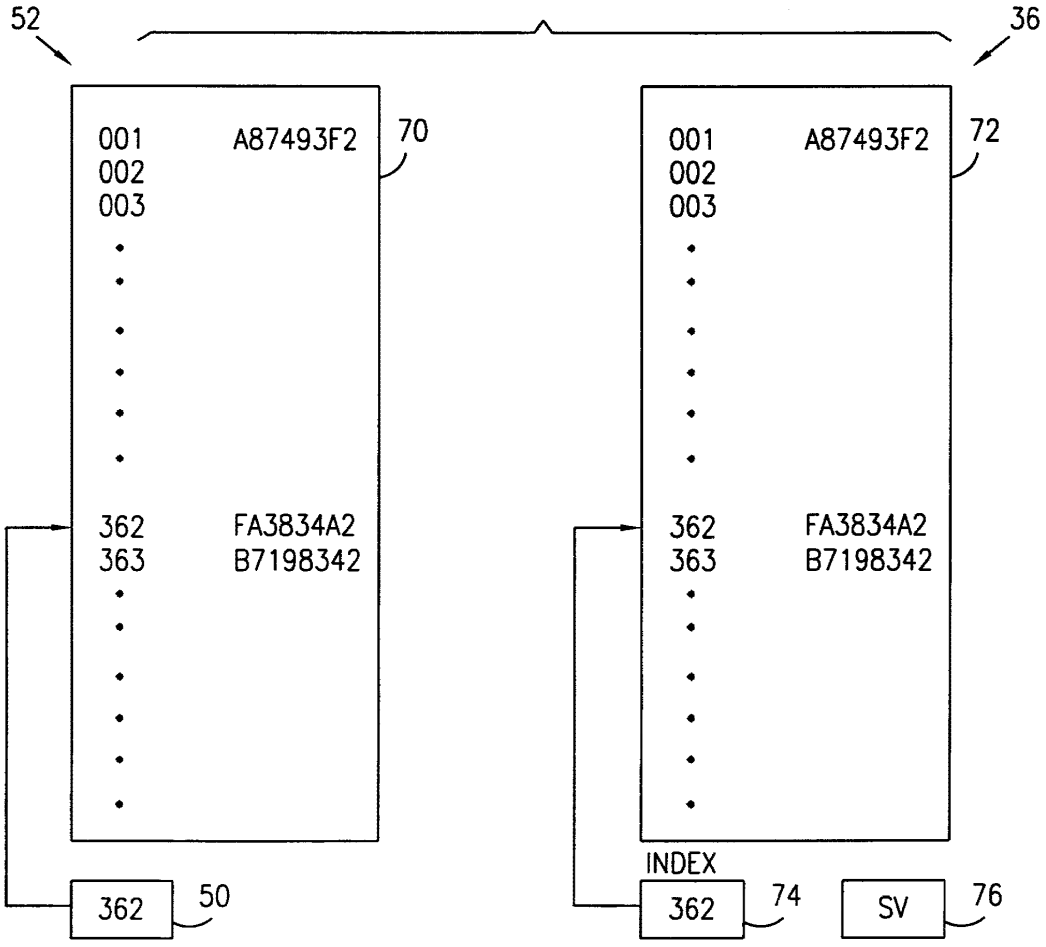

52
36
001 A87493F2
002
003
70
362 FA3834A2
363 B7198342
362
50
001 A87493F2
002
003
72
362 FA3834A2
363 B7198342
INDEX
362
74
SV
76

FIG. 4

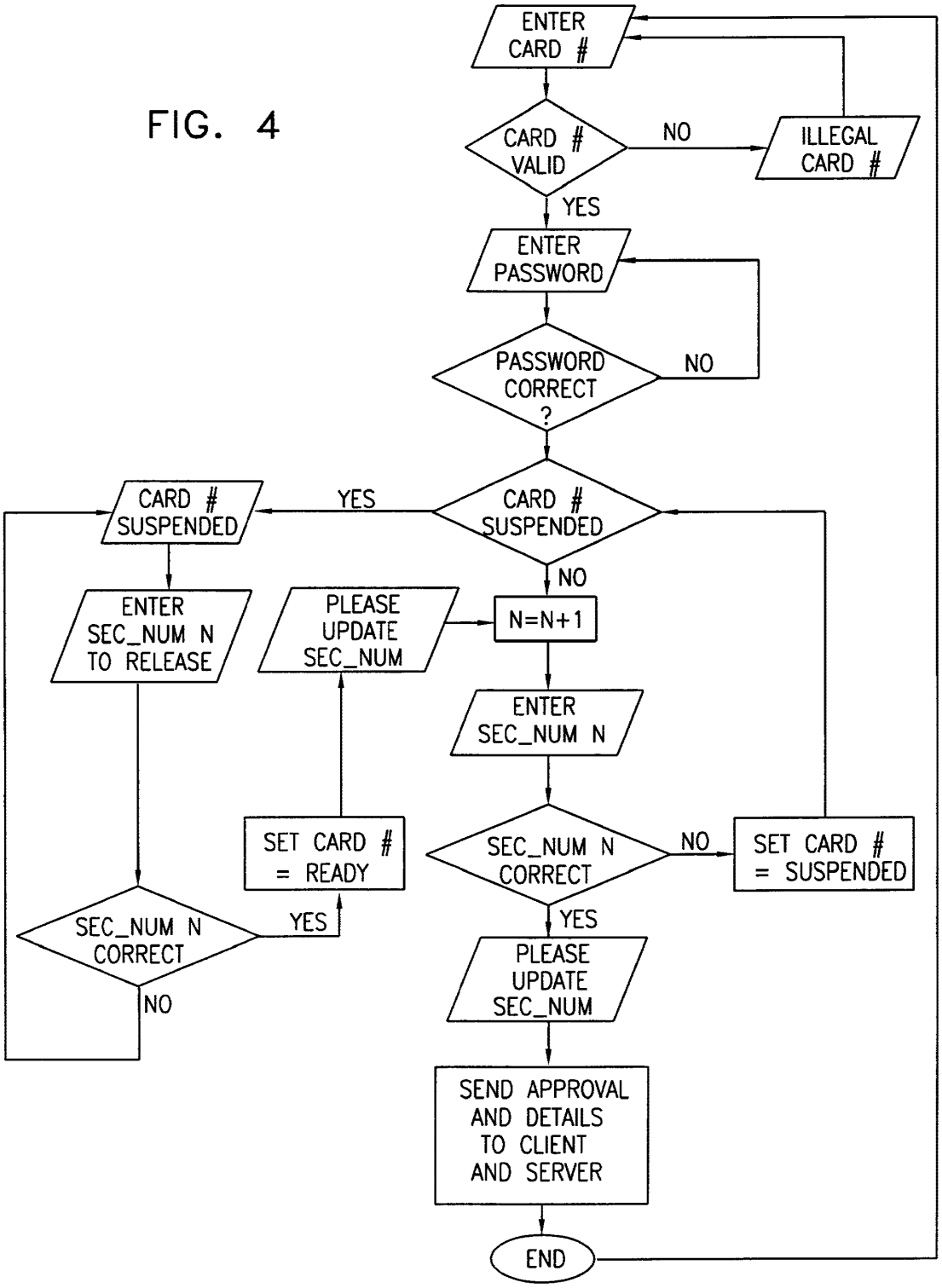

ENTER CARD #
CARD # VALID
NO
ILLEGAL CARD #
YES
ENTER PASSWORD
PASSWORD CORRECT ?
NO
CARD # SUSPENDED
YES
CARD # SUSPENDED
NO
ENTER SEC_NUM N TO RELEASE
PLEASE UPDATE SEC_NUM
N=N+1
ENTER SEC_NUM N
SET CARD # = READY
SEC_NUM N CORRECT
NO
SET CARD # = SUSPENDED
SEC_NUM N CORRECT
YES
NO
YES
PLEASE UPDATE SEC_NUM
SEND APPROVAL AND DETAILS TO CLIENT AND SERVER
END

FIG. 5

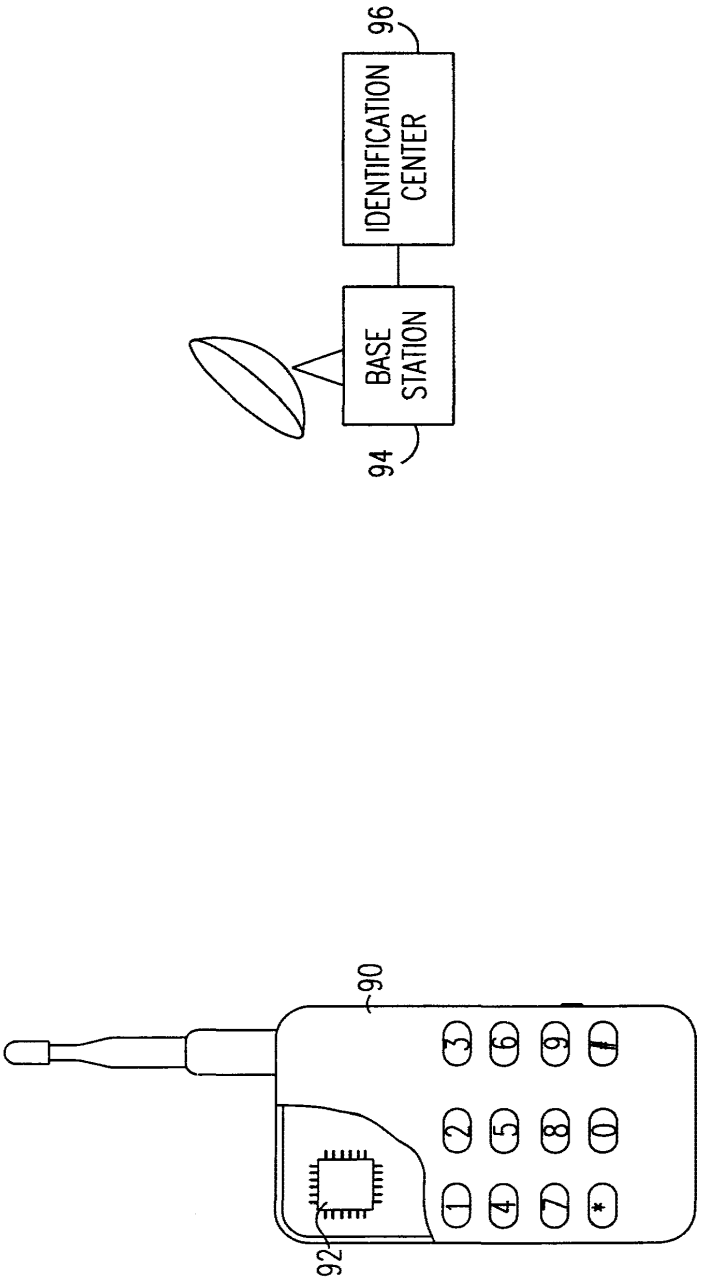


FIG. 6

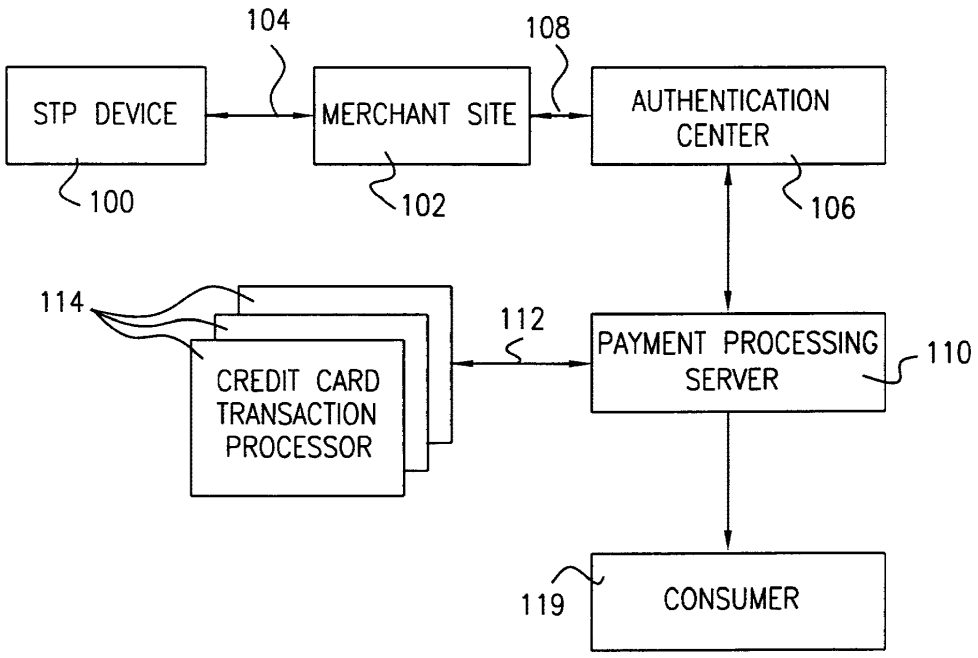

104
108
STP DEVICE
MERCHANT SITE
AUTHENTICATION CENTER
100
102
106
114
112
PAYMENT PROCESSING SERVER
110
CREDIT CARD TRANSACTION PROCESSOR
119
CONSUMER

FIG. 7

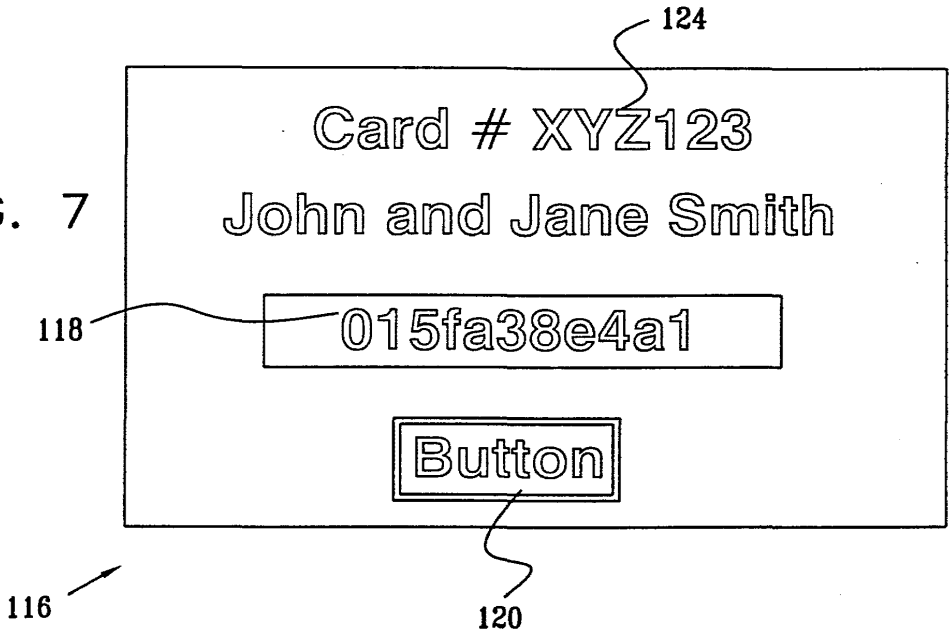


FIG. 8

ROM	001 rt237yu5 ... 015 fa38e4a1 016 xy568AD9 017 k6a7FI8

FIG. 9

129
132
A715H2, AP2206
APPARATUS
John and Jane Smith
138
136
130
134

FIG. 10

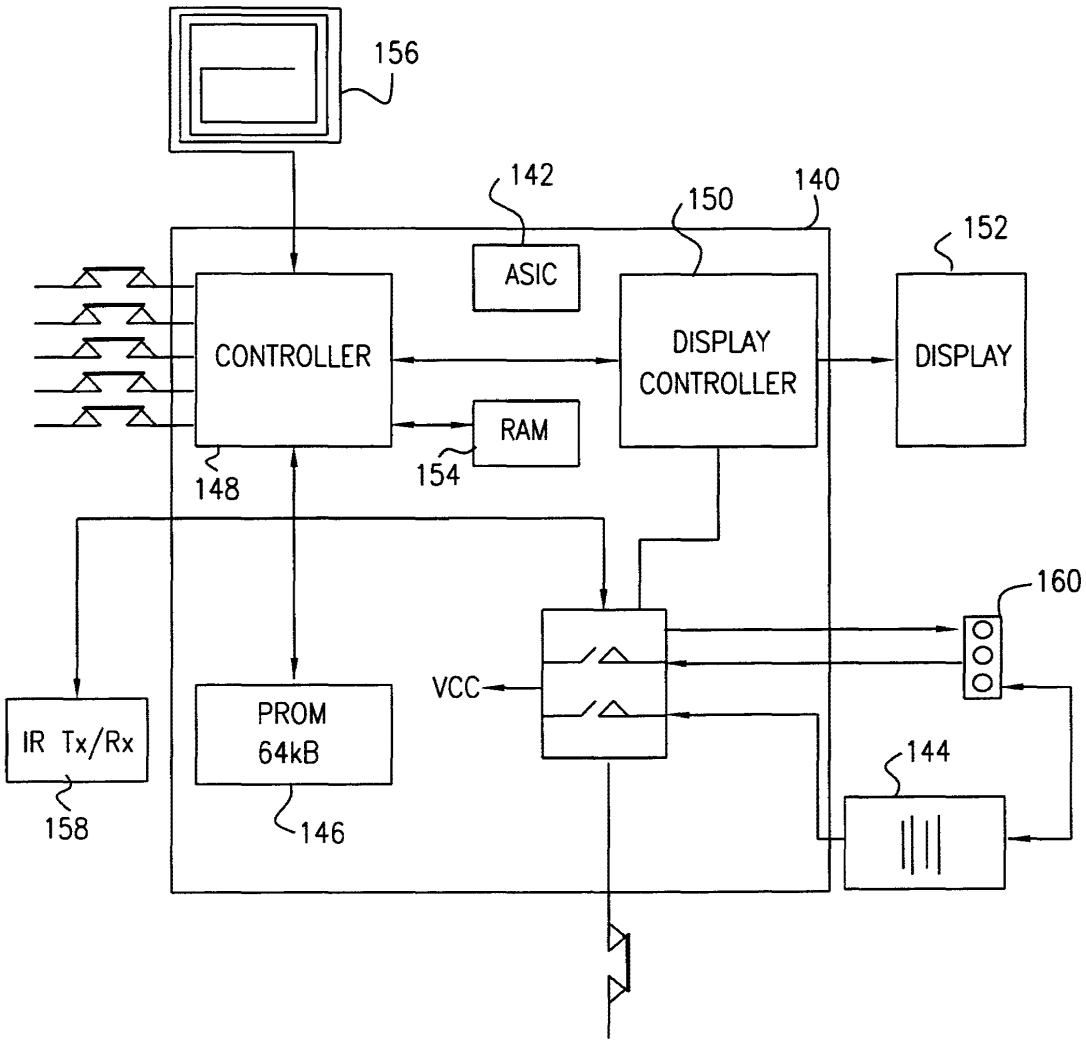

156
142
150
140
152
ASIC
CONTROLLER
DISPLAY CONTROLLER
DISPLAY
RAM
154
148
160
VCC
IR Tx/Rx
158
PROM 64kB
146
144

FIG. 11

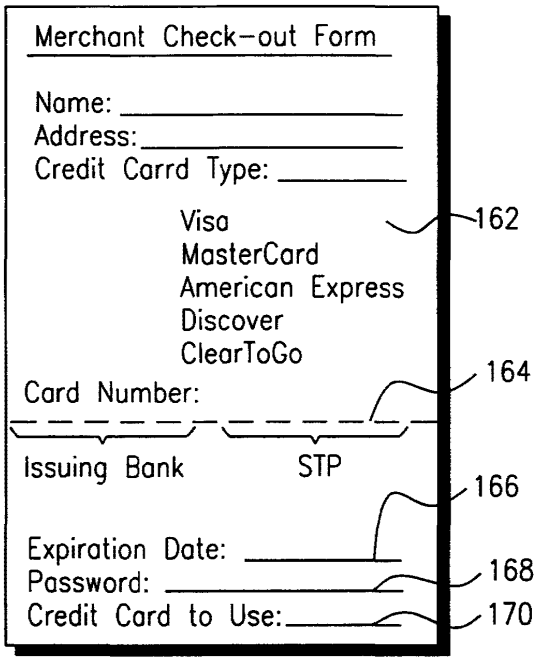


FIG. 12

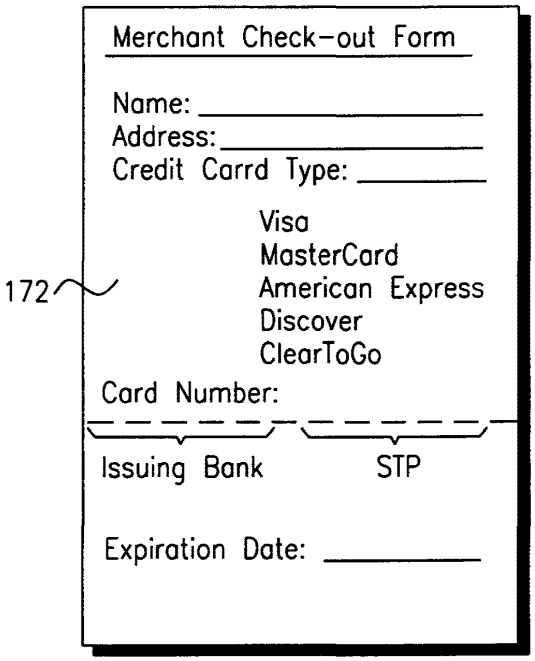


FIG. 13

Information stored in the Central Authentication Server			
Card # XYZ123, John and Jane Smith, Address, password: A2F8			
STPs:	001..... .... 015fa38e4a1 016.....	Credit Cards:	Visa# MasterCard # AmEx # Discover # ....

FIG. 14

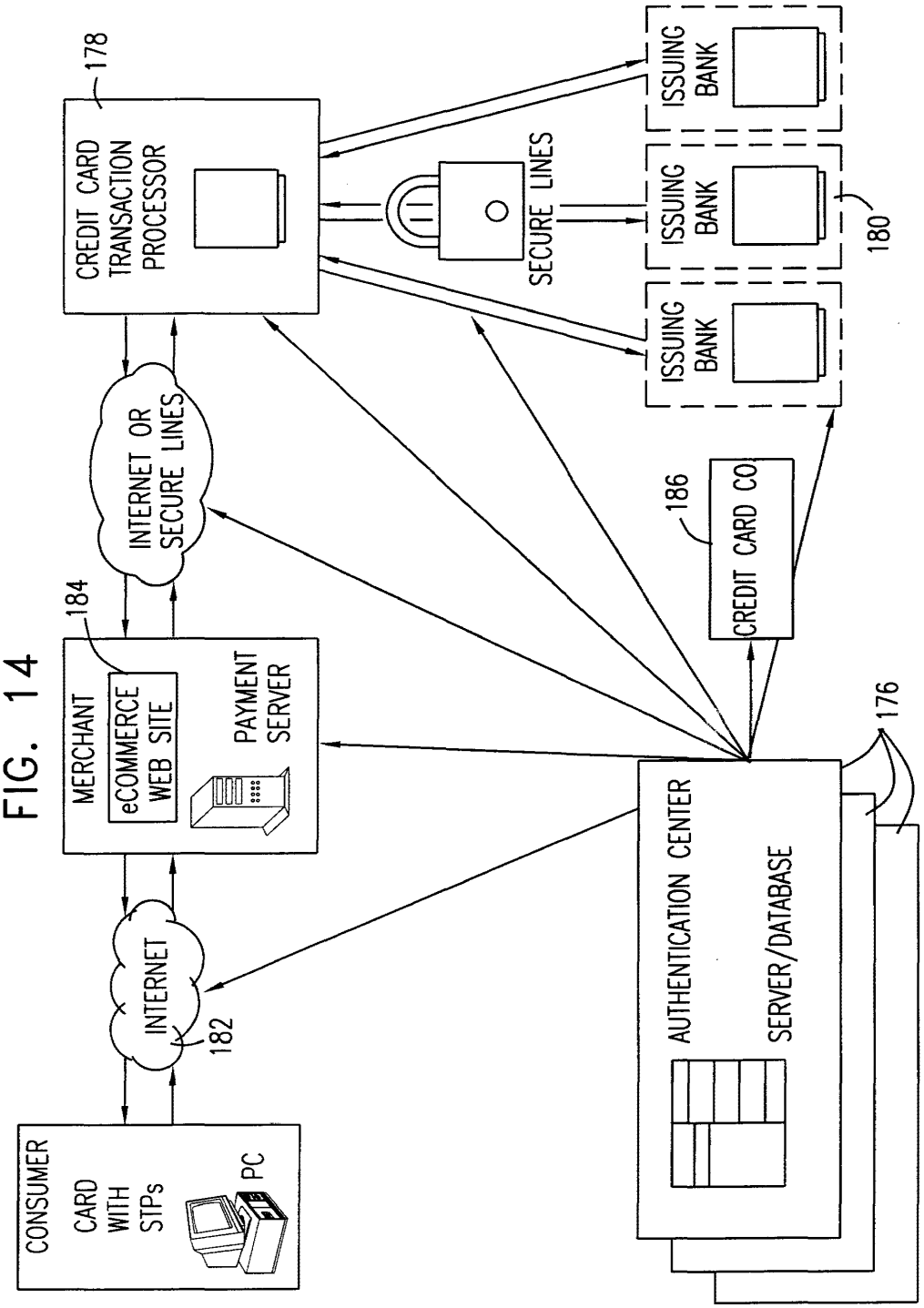

178
CREDIT CARD TRANSACTION PROCESSOR
SECURE LINES
ISSUING BANK
ISSUING BANK
ISSUING BANK
180
INTERNET OR SECURE LINES
186
CREDIT CARD CO
184
MERCHANT
eCOMMERCE WEB SITE
PAYMENT SERVER
176
AUTHENTICATION CENTER
SERVER/DATABASE
INTERNET
182
CONSUMER
CARD WITH STPs
PC

FIG. 15

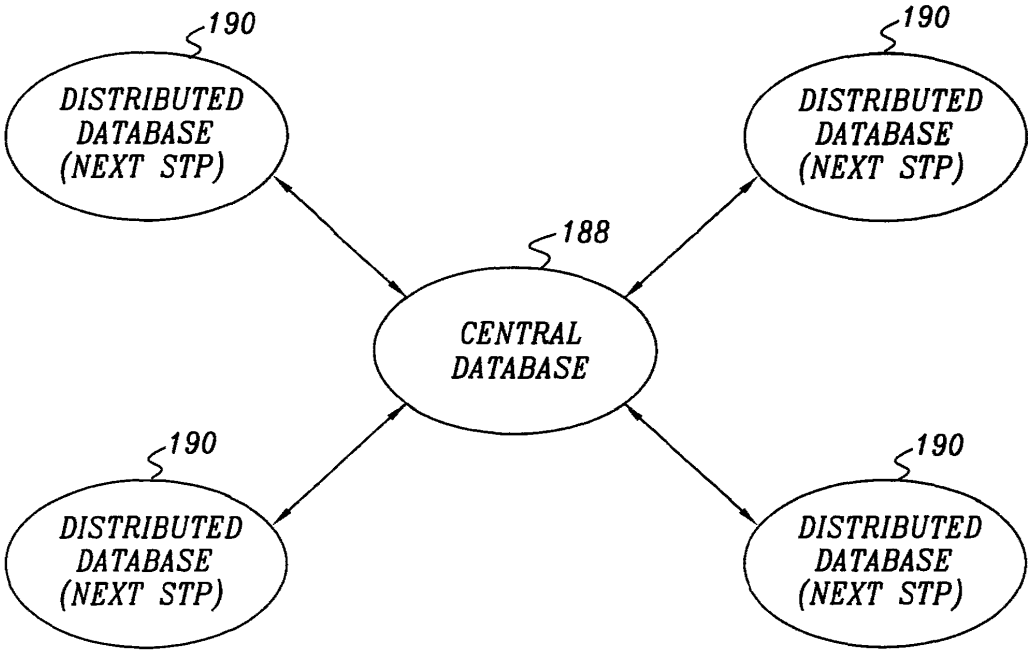

190
DISTRIBUTED DATABASE (NEXT STP)
190
DISTRIBUTED DATABASE (NEXT STP)
188
CENTRAL DATABASE
190
DISTRIBUTED DATABASE (NEXT STP)
190
DISTRIBUTED DATABASE (NEXT STP)

FIG. 16

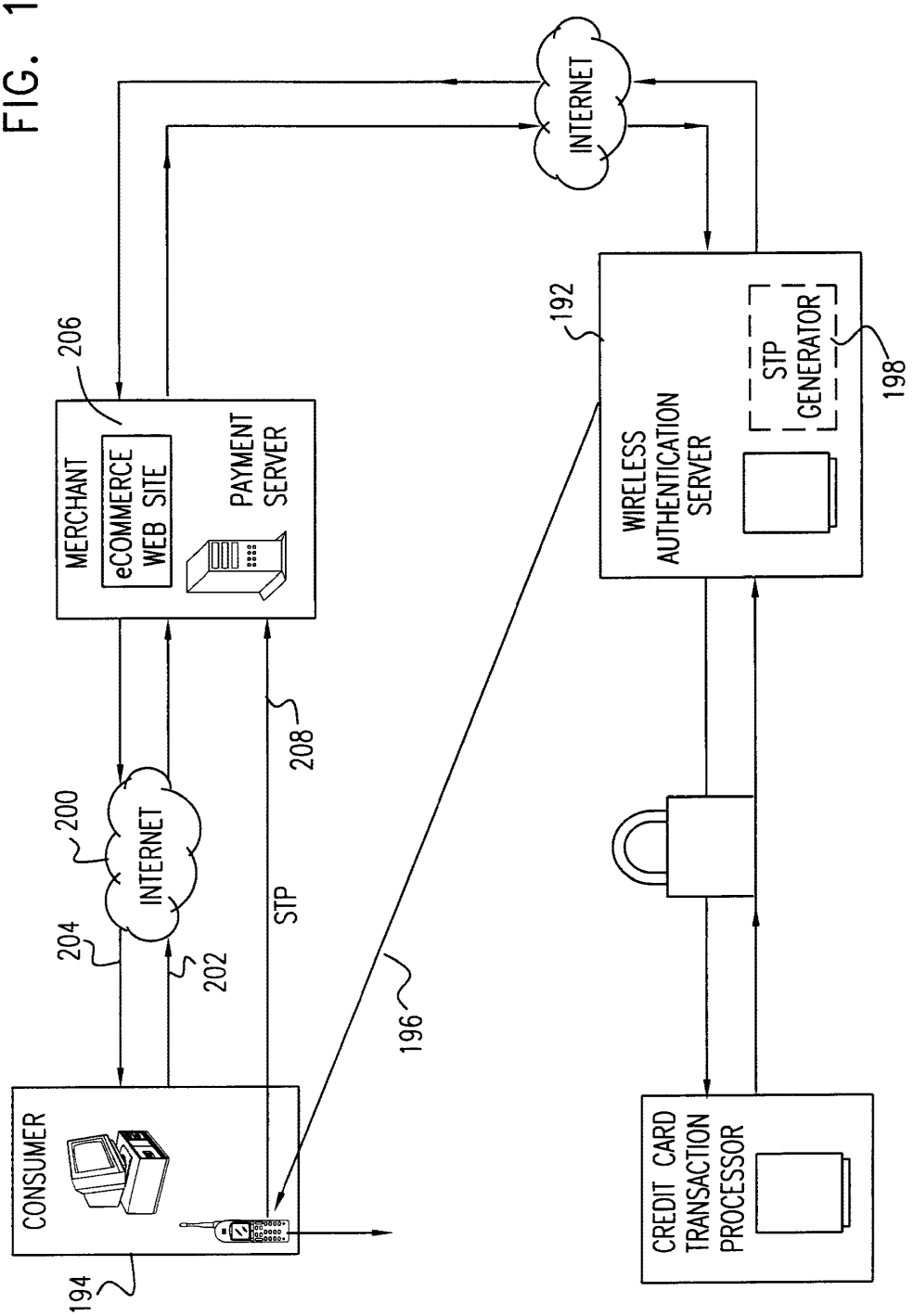
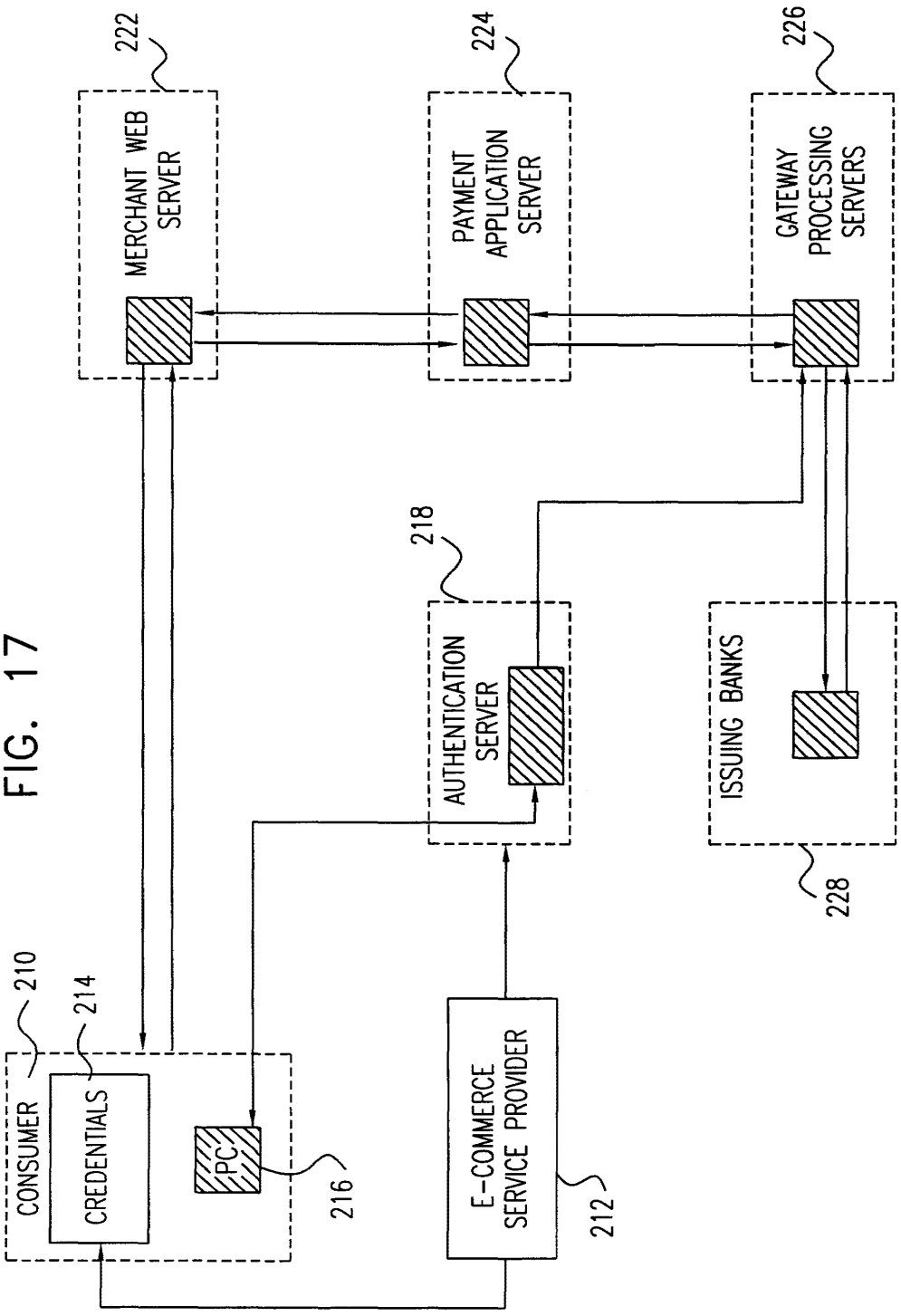

INTERNET
206
MERCHANT
eCOMMERCE WEB SITE
PAYMENT SERVER
192
WIRELESS AUTHENTICATION SERVER
STP GENERATOR
198
208
200
INTERNET
204
202
STP
196
CONSUMER
194
CREDIT CARD TRANSACTION PROCESSOR

FIG. 17


222
MERCHANT WEB SERVER
224
PAYMENT APPLICATION SERVER
226
GATEWAY PROCESSING SERVERS
218
AUTHENTICATION SERVER
ISSUING BANKS
228
210
CONSUMER
214
CREDENTIALS
PC
216
E-COMMERCE SERVICE PROVIDER
212

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL00/00211

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :GO6F 17/60; H06K 1/00; H04L 9/00
US CL :705/67

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/67

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,502,765 A (ISHIGURO et al.) 26 March 1996, Abstract; col. 2, lines 24-67; col. 3 lines 1-17; col. 5, lines 65-67; col. 6, lines 1-67; col. 7, lines 1-28; col. 8, lines 8-48; col. 10, lines 7-48; col. 11, lines 3-39; col. 12, lines 21-32; col. 14, lines 26-44; col. 16, lines 11-57	1-63
Y	US 5,717,756 A (COLEMAN) 10 February 1998, Abstract; col. 3, lines 31-63; col. 4, lines 47-55; col. 7, lines 46-67; col. 8, lines 1-60; col. 9, lines 24-44; col. 10, lines 48-67; col. 11, lines 1-67; col. 12, lines 1-6; fig. 3A [100, 202, 206, 208, 210, 212, 213, 214, 218]	1-63

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 16 JUNE 2000	Date of mailing of the international search report 20 SEP 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer ALLEN MACDONALD Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)★

IPR2025-01150
Apple EX1071 Page 1314

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL00/00211

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,721,781 A (DEO et al.) 24 February 1998, Abstract; fig. 1 [2b, 3, 4]; fig. 4A [2,4]; fig. 7 [4, 5, 6]; fig. 9 [2b, 4, 6]	1-63
A	US 5,396,558 A (ISHIGURO et al.) 07 March 1995, Abstract	1-63
A	US 5,436,970 A (RAY et al.) 25 July 1995, Abstract	1-63
A	US 5,526,428 A (ARNOLD) 11 June 1996, Abstract.	1-63
A	US 5,581,615 A (STERN) 03 December 1996, Abstract.	1-63
A	US 5,887,065 A (AUDEBERT) 23 March 1999, Abstract.	1-63
A,P	US 5,999,624 A (HOPKINS) 07 December 1999, Abstract.	1-63
A,P	US 6,005,939 A (FORTENBERRY et al.) 21 December 1999, Abstract.	1-63

IPR2025-01150
Apple EX1071 Page 1315

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL00/00211

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

DIALOG, STN
SEARCH TERMS: remote transaction, network, link, code, credit/purchase/debit/smart card, encrypt$4, identif$7, stor$4, database, table, list, verif$7

Form PCT/ISA/210 (extra sheet) (July 1998)★

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Susan Pandy, "Securing Payments: Payments Tokenization in Primetime," Federal Reserve Bank of Boston Payments Symposium, January 20, 2016, pp. 1-20.	
	2	"SUMMARY OF ANS X9.119-Part 2 USE OF TOKENS TO PROTECT SENSITIVE CARD DATA," September 2017, pp.1-2.	
	3	Marianne Crowe et al., "Is Payment Tokenization Ready for Primetime?," June 11, 2015, pp. 1-51.	
	4	Terence Spies et al., "ANSI X9.119 Part 2: Using Tokenization Methods," 2013, pp. 1-20.	
	5	ASSORA et al., "A web transaction security scheme based on disposable credit card numbers," Int. J. Electronic Security and Digital Forensics, 2007, Vol. 1, No. 2, Inderscience Enterprises Ltd., pp. 146-155.	
	6	BOYD, "A pragmatic approach to temporary payment cards numbers," Int. J. Electronic Security and Digital Forensics, 2009, Vol. 2, No. 3, pp. 253-268.	
	7	BUCCAFURRI et al., "Implementing disposable credit card numbers by mobile phones," Electronic Commerce Research, Feb. 23, 2011, Vol. 11, Springer Publishing, pp. 271-296.	
	8	JAVANI et al., "A new credit card payment system based on 3D-Secure using one-time-use transaction numbers," Information Assurance and Security Letters, 2010, Vol. 1, Dynamic Publishers, Inc., USA, pp. 060-065.	
	9	KILLORAN et al., "A New Secure Wireless Financial Transaction Architecture," EUROCON 2005, November 22-24, 2005, IEEE, pp. 1060-1063.	
	10	LI et al., "A security-enhanced one-time payment scheme for credit card," Mar. 28-29, 2004, IEEE, pp. 1-11.	
	11	MJØLSNES et al., "On-Line E-Wallet System with Decentralized Credential Keepers," Mobile Networks and Applications, 2003, Vol. 8, Kluwer Academic Publishers, The Netherlands, pp. 87–99.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	NARAYANASWAMI et al., "What Would You Do with a Hundred MIPS on Your Wrist?," RC 22057 (98634) January 22, 2001, IBM Research, pp. 1-10.	
	13	QASIM et al., "Interactive Shopping with Mobile Wallet," World Congress on Sustainable Technologies, 2012, IEEE, pp. 32-36.	
	14	HONIG, "A Week with Google Wallet," Endgadget, September 19, 2011, pp. 1-49.	
	15	KADAMBI et al.,"Near-Field Communication-Based Secure Mobile Payment Service," ICEC'09, August 12–15, 2009, pp. 1-11.	
	16	"A closer look at Google Pay and tokenization," Rambus Press, February 23, 2016, pp. 1-2.	
	17	GHAG et al., "A Comprehensive Study of Google Wallet as an NFC Application," International Journal of Computer Applications, November 2012, Vol. 58, No.16, pp. 37-42.	
	18	"Add any credit or debit card," Google Wallet Help (archive.org), 2012, page 1.	
	19	"Add any credit or signature debit card," Wallet Help, Google Wallet, September 20, 2012, page 1.	
	20	"Allynis Mobile NFC," Gemalto, September 2007, pp. 1-4.	
	21	"Allynis TSM for Transport," Gemalto, October 2009, pp. 1-2.	
	22	ADAMS, "Amex Plays a Major Role in Revamped Isis Mobile Wallet," Payments Source, November 15, 2013, Vol. 1, No. 1, SourceMedia LLC d/b/a Arizent, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	PEREZ, "Android Pay, Google's Apple Pay Rival, Arrives Today," DigitalOcean, September 10, 2015, pp. 1-8.	
	24	HEISLER, "Apple Pay: An in-depth look at what's behind the secure payment system," Engadget, October 2, 2014, pp. 1-7.	
	25	FEHR, "Apple Pay: How different is it from other Pay solutions, what role does tokenisation play, and to what degree can Card not Present payment benefit from Apple Pay in future," Technical Report RHUL–ISG–2018–3, April 3, 2018, Egham, Surrey, UK, pp. 1-79.	
	26	"ATMIA publishes contactless ATM best practices," ATM Marketplace, September 27, 2012, pp. 1-2.	
	27	POPPER, "Banks Did It Apple's Way in Payments by Mobile," New York Times, September 11, 2014, pp. 1-2.	
	28	"Bell ID Simplifies EMV Smart Card and NFC Application Management with Versatile New Platform," eBanking & Payment News, May 5, 2011, page 1.	
	29	"BofA pursuing contactless ATM patent," Mobilepaymentstoday.com News, September 20, 2012, Newstex LLC, pp. 1-2.	
	30	"Chip Advisory #20, Visa Recommended Practices for EMV Chip Implementation in the U.S," July 11, 2012, pp. 1-10.	
	31	"Commbank, Mastercard and Samsung collaborate to launch NFC payment service," MarketLine NewsWire (Formerly Datamonitor), December 13, 2013, pp. 1-2.	
	32	"Contactless Payment: Secure Enough?," Card Technology, September 1, 2005, SourceMedia, Inc., Section: SPECIAL ISSUE: CONTACTLESS TECHNOLOGY, Vol. 10, No. 8, page 36.	
	33	"Eligible Devices," Google Wallet Help (archive.org), November 18, 2012, page 1.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	MOTT, "EMV and Mobile Payments, Questions abound, answers divide," Payments Summit Workshop, February 4, 2013, pp. 1-22.
	35	"EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management Version 4.1," May 2004, pp. 1-187.
	36	"EMV Integrated Circuit Card Specifications for Payment Systems. Book 2, Security and Key Management, Version 4.3," November 2011, pp. 1-174.
	37	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.3," November 2011, pp. 1-230.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IPR2025-01150
Apple EX1071 Page 1323

UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 01:27:56 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424604	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 51

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_1.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
BOYD.pdf	16	Non Patent Literature	1484 KB
BUCCAFURRI.pdf	26	Non Patent Literature	18760 KB
Card_Technology.pdf	2	Non Patent Literature	1400 KB
Chip_Advisory.pdf	10	Non Patent Literature	4354 KB
Commbank.pdf	2	Non Patent Literature	915 KB

ADAMS.pdf	2	Non Patent Literature	1268 KB
Allynis.pdf	4	Non Patent Literature	2218 KB
Allynis_TSM.pdf	2	Non Patent Literature	1429 KB
ASSORA.pdf	10	Non Patent Literature	525 KB
ATMIA.pdf	2	Non Patent Literature	829 KB
Bell.pdf	1	Non Patent Literature	50 KB
BofA.pdf	2	Non Patent Literature	972 KB
EMV_Version4_1_5_of_5.pdf	35	Non Patent Literature	21890 KB
EMV_Version4_3_1_of_6.pdf	44	Non Patent Literature	18367 KB
EMV_Version4_3_2_of_6.pdf	22	Non Patent Literature	10609 KB
Eligible_Devices.pdf	1	Non Patent Literature	359 KB
EMV_Version4_1_1_of_5.pdf	38	Non Patent Literature	16276 KB
EMV_Version4_1_2_of_5.pdf	38	Non Patent Literature	20147 KB
EMV_Version4_1_3_of_5.pdf	38	Non Patent Literature	20660 KB
EMV_Version4_1_4_of_5.pdf	38	Non Patent Literature	21751 KB
EMV_Version4_3_Book_3_2_of_4.pdf	58	Non Patent Literature	17652 KB
EMV_Version4_3_Book_3_3_of_4.pdf	58	Non Patent Literature	19875 KB
EMV_Version4_3_Book_3_4_of_4.pdf	56	Non Patent Literature	17117 KB

EMV_Version4_3_3_of_6.pdf	22	Non Patent Literature	14463 KB
EMV_Version4_3_4_of_6.pdf	22	Non Patent Literature	12252 KB
EMV_Version4_3_5_of_6.pdf	22	Non Patent Literature	12697 KB
EMV_Version4_3_6_of_6.pdf	42	Non Patent Literature	22311 KB
EMV_Version4_3_Book_3_1_of_4.pdf	58	Non Patent Literature	14723 KB
MJØLSNES.pdf	13	Non Patent Literature	1222 KB
MOTT.pdf	22	Non Patent Literature	12395 KB
NARAYANASWAMI.pdf	10	Non Patent Literature	2820 KB
PEREZ.pdf	8	Non Patent Literature	3975 KB
FEHR_1_of_2.pdf	40	Non Patent Literature	16209 KB
FEHR_2_of_2.pdf	39	Non Patent Literature	12433 KB
GHAG.pdf	6	Non Patent Literature	1711 KB
Google_Wallet.pdf	1	Non Patent Literature	595 KB
HEISLER.pdf	7	Non Patent Literature	4135 KB
HONIG.pdf	49	Non Patent Literature	6061 KB
JAVANI.pdf	6	Non Patent Literature	4074 KB
KADAMBI.pdf	11	Non Patent Literature	6408 KB
KILLORAN.pdf	4	Non Patent Literature	3277 KB
LI.pdf	11	Non Patent Literature	2268 KB

Summary_of_X9_119_Part2.pdf	2	Non Patent Literature	79 KB
tokenization_prime_time.pdf	51	Non Patent Literature	930 KB
Wallet_Help.pdf	1	Non Patent Literature	588 KB
X9_Tokenization_Webinar.pdf	20	Non Patent Literature	572 KB
POPPER.pdf	2	Non Patent Literature	992 KB
QASIM.pdf	5	Non Patent Literature	2677 KB
Rambus_Press.pdf	2	Non Patent Literature	994 KB
Securing_Payments_Payments_Tokenization_in_Primetime_Susan_Pandy.pdf	20	Non Patent Literature	1814 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_1.pdf	4F0C61245B9B943C8CDD1980604C62915688BD2FB91ED153113BB7F505135EE0E56F14A31D9412F4C8E6A7FB5F0611AEB88CB24D3652D38E0338895D9253C4F4
BOYD.pdf	D39B5EA68D301627A34756AD9BD1B06CA843EED22AB642B4A876FB74C8AB1DEC0F5AE064DE5007D5DAEC8E15F8B120FA8419966594726C29DD2741D4A08B84A7
BUCCAFURRI.pdf	0A03D387FF0B573B3D44288C20DA995EA07BBB7131D4966B500AE4E9936C64E407DCE7B3D23A7179B9206733F06FF9524E9712AD50CE3D1B91F1AC9870CE2AA4
Card_Technology.pdf	0809D4A22C921A988D89D6F68E953187CCF21D33A66525F04C26A70249ECA367A7C5931BDD42838D1F6D842A4033F05BFD

	BC3F5A0250F2E0D99E4CCAEB277E50
Chip_Advisory.pdf	3BF42C638C86E4CCE628BAE2FEB50602C48DDB1A618BDE703DC8AA70C22FF865661653281160FC4A31EA6F335BF789B897473CD2017CF095ED8FDB11117499BF
Commbank.pdf	3F783425E0CD95911F262080166 4B942C6052C062D6BBB0A7D166DD2BEA9B0909ACADA35C1E4F6427EEBA1B11C1A987D3C06E5407AC2339F5656D210AA8DE8A5
ADAMS.pdf	5538A8606D81EDB46E767776C89CBC10DBE56E87CE7D75DBCA999C1E6B0C145FBF2497EC3CF335E8B558F3BD00F9A9B004038120791D8D10F3C6EED942CED267
Allynis.pdf	AE1ED03818B28EFA0A821437DFB702B2F12B64199C77B38993CFCC0E24812B6D8D73D57D72085004133C2D27B4B303F09097F666A043E93743532AF53FFB8589
Allynis_TSM.pdf	B59AE47468827AF15EA3731015D7531260D0614D26D57E5E2FD965DCAD55541EE8B1126BF5D50BD6467B5EF8D79A9D7A937121155068BB19D0CC665034BE897D
ASSORA.pdf	72152DD9C6DA5F3F4B76822DC8EAA9E9EEAF01D772804D70796B7A58EA7619D48E9103E844F97839729D3B2785B3E61E0106CAA97D4E32AEA14639AEF5780D8C
ATMIA.pdf	0211530F0CB6627EE4E37AE62337AC066512E89EF5B4ECE51627B15ADCA344A6B92C2D1578095A5CBA79B3986E3DDCD49FC7955A75437465B8DE32517DC6FDCF
Bell.pdf	8064F8F28BF156C8D715B4E3DD393729D85784F6826A8EC6A93BEF703B8275D6F92F259B048FB26BC2A4FC46ED9F3D52C32BCB6068ADB5F7315F5A08BA610ED2
BofA.pdf	B9C51D87CBD3E127E48A4FC323A5C9A4F879C8829F33908A47F584F3F722F35C4C5BC77994C3838382FC2F59C938CD35579B740E8E5986CBC26A31C13EA68335
EMV_Version4_1_5_of_5.pdf	09E8648272DD8B8A94C796DB06AB8A089115D2C23723F66468923A63872D3BF86953A6BEB638D487AC9D6295D2513B469C7

	D845452DDD783BB4DDC0A7ED73B7A
EMV_Version4_3_1_of_6.pdf	6A683BE6E45691E5B837EEC4F73905520507606ACA25EE9871EA1BB6A7F3A3E38CCA80B795821BD1106D35C761259B02099F3AFEF6D15211F86EFEF896CDEFE5
EMV_Version4_3_2_of_6.pdf	6AFB6443D402596DB9B44C3420A4E016E52B510D9B4447859712CF58A231D11AE27A0432B0A8118E2C163C55DBC4C3D97FB6615542E972A3F532FE37BF0D3C3A
Eligible_Devices.pdf	E7485117B1C2B03C3E57978C24C80F344996A0BF6557E4F3E90F451A3C500BFC4BFE9CA24FA7752FF1B0E9F0250E9C30564140A1AF528334590AB968FED09A03
EMV_Version4_1_1_of_5.pdf	C881DF5451E974C752DA52A2E2A562AB265F57EBAE2774E9E53E331226548481C121353F6139084E7919DDCF580273AC0187351A32511E68D9A1EBD240BFDB87
EMV_Version4_1_2_of_5.pdf	8DBABA99D5CD6B530FDFDCF28D2317C470922190A30F560E03FB89A8342B16D587AB65D0FD63354872D176E5095531EFE144E00779A6FE26B62C19EFB699C731
EMV_Version4_1_3_of_5.pdf	91E406A620A19206E31ACAC834F41A166493704F2D57E20CC50D535C8C4C40EBEBB3D94097A92C35CF6EA82A099FAFC491D329C676BC6F77E0ECF8A32434E936
EMV_Version4_1_4_of_5.pdf	95675B681FDF86E36D4A8B0344D06DAF1E0F2C5D3937C02520F842A987462F85EE8C5B31F299EFDF5DD7431C745535605633C3E8C756EA1FB14A8DA22175A2F8
EMV_Version4_3_Book_3_2_of_4.pdf	BB2AD512AEDF46C95CFA42BE7C6277998D6184EF60B52539CD4E5EDE27E506D90FC11BB3A2CE12291E04E208B3DEF94B078F3A357A3C5DD7ED96AB765576D512
EMV_Version4_3_Book_3_3_of_4.pdf	BAEA77F15EB89EF675EBF883C1F5F32AF04A38EE434A47301928684B540883BFEB6240205DD7B31DCC25D35B4AC6448D479A32D69D120026DC4364E11E90734F
EMV_Version4_3_Book_3_4_of_4.pdf	877FF29B90A238E12574539C7D37CDFE609378ADEEA723394B7DEB6010C5101B7484D0BFD2AA59F29C88753D20E91BB4BF

	DEF8EE81F26673F046C013CFCE1DA9
EMV_Version4_3_3_of_6.pdf	DD5243F6F4744D9BF7E4150AF33414BC0A1F63296836B91141 7F792DB28AC797ED52EEA5258B861462FCB1B63E1DC193E8F 7EB9328B91A4D79773FAF762FB7B5
EMV_Version4_3_4_of_6.pdf	A0CBF5DE048BB65A28342200AA90D2DB67518FB008402A154 9FE93C35D25646C3EA8893A36EBA38637123047B15F01ADE0 F40C9F6CACEC52F6D8365B96E1AF5A
EMV_Version4_3_5_of_6.pdf	EFDDAF48C250F6B032202793A25FDCCA391B321E4DAFF8D0 C4996D16C4224F3C80C3F5B7D6E06DE65F26040D8D0F9DC97 A21180AFA4F3F7A3806E1F8EA2C25D0
EMV_Version4_3_6_of_6.pdf	CCB68CAA90AB233F7A81EB8F0FADE2E709869436A22CEB6A 193D5EF1B88FB0BA25925173DF9C63741D99525CB8C895E50 1944A012E4A57891934C4ED15938229
EMV_Version4_3_Book_3_1_of _4.pdf	6930BDEDACE65535E0B1CE174B42C865A1A3C89352C0C9AB 7F76AFBC4E156DFFBDBFE45F4012A00BF2CB17EC782ECB8A 0FF9EC4169CB4432769374BF89F91488
MJØLSNES.pdf	09D5809D62DD012C6ADEE666A17D3182F18B22AF9B8DDFB7 F7398D10FB60242B48F30404B8F6B0DE4D33990511D03F310C 0547287EC3FCE7A7EFCE19769D5AE0
MOTT.pdf	F5787F4B247AE378139D1974886D273B671EFCA194DC5FF1E D6B1042123433DA4645B7FEC6D27414D143831D29ABCC930F 9006D5FE9C30577465965562E9D566
NARAYANASWAMI.pdf	1F01E07A4118809664E0D9CC83FC20A6B960A9AFF640C1752F 7F5CD80BF49CF293A8B00AC0140898CE6CAAB2FF8CA551AF 0DADA899EFB9B74F6368245E993795
PEREZ.pdf	338F26C8F06091EA9D3BBC34096CF77DF4E11F23D432D66CB 5775D98DE781A68804BA5E436D31C561B8B643B1171C22B4D 0C93FC5F1E5B3DA12DA5B535C922FC
FEHR_1_of_2.pdf	85FFB2B011773749EDC984747130C968BDA51C0260966D1FE0 44F389270F548C01A44ECCC5BAFC2FEE2DE83A022EFBF057

	B7F2EDA4D651C8DAB11F066B049B5A
FEHR_2_of_2.pdf	7900EC82C6BE4655B37103766DE66F86E5F6E5C12D3BFD8C05BE0547E53E684DE6D10C38D4362E0C399194C2BE5CD3CB148F05ABE3653DA24D73E5014BEC0DBB
GHAG.pdf	954672BA13D15FA8ABC894A85FA1FDAA59C8D856E871460C1C5B95DB127B63B415127F3F04315362904D3C35C02CCF82696EC8A7C706337175A277A404356253
Google_Wallet.pdf	8DE6568D7B8A287E65F9A5F38DAFE05157D68838BECF7D5C9A39077B87AA9C2603AFFBB7D5D8089105BE7C8E50A44CB11ABF434A46703A917F25857DB21F9336
HEISLER.pdf	0E16D814795430518BA5A076A2E7E9B9BD3FE9634A06F6244938DE72238F52193449D709F2AB1038F861D111C47136E1EB04707564ED39AF1BA37EB4A8E34E7C
HONIG.pdf	A2884CD2EC73B871CA75F215B7BCBAA9499D4BC858336EAE80AD7D60DB03890910554D16C790E802FEBF3B7CFD4329056557D99134401E90100FBF42214068E8
JAVANI.pdf	C1C1C6016E392BE5703EE23C81F44301C270112C39F70E46BF154EC418C795EB1D58752408E78114556D07AB4F625631BB93AD09897016178230 2BE80FF9E7FC
KADAMBI.pdf	55DDD4E83880ADE76EAC158D99CFF5CBA4F5F19788B43599DD9F25CCCAEFB4A47D3EE87763CF0DE37BBE0D29A60E14AF6EE32AB836EB0793194BC576334A21E9
KILLORAN.pdf	31D22C0393C99C2464F7E79D35CD518E2D8BE96574C00C6E052BAA2FE4658D25DE3E026CF660C67217EDAA58C43431136600996FAA4D959D210B95488FEBA2B3
LI.pdf	A5D9430B1149889FAE605EE6A9BCF8F3ACA84E058B1ECE680EF9F5BB967BB48862D1C09ADC185AFCA1442C77FA356C82B37FC19D6ECAB8027A5ECC285E0646C8
Summary_of_X9_119_Part2.pdf	869F6F2AFA594E838EF6B0589B11819DE452077F807B36F28C5C961E0CD26E9ACD6B6603C18F908D5194429A78A419349889

	ED7018FD23D8B59D629A223C34BA
tokenization_prime_time.pdf	B8AE3162E55ED2C8A346634174D192DF3C5CD0D92CA3C6A FE7D55A6214EA2C66EC8137D326C3AB62BD50B10D0B918EE B2423781024213532A1BB6C33B8FACCC
Wallet_Help.pdf	093CF9F287C81267050436 8F67CCAEE14CCA994045365B2812 6FD67E0852A79FC2B32E4C24D202DEA6E271A07A5ED194BD 7ABE31317FC62F107F13373A0E60BA
X9_Tokenization_Webinar.pdf	0AF132928B9667E9A7A146D1990C6E6C3A1A7D667A170C3D6 036A151B1244C339D26937084A01AAA44A1876E5A08DB9BAF4 6B6FF1F70CD8883DAD2DEE005B8B3
POPPER.pdf	14723D8F1788F840B6227D379A0D6D637AF2BEFC5B0456B12 D6215F3753F9226E3C13654E41514804952720 5B68F19D410E7 566A8542FEC22F09FFB4B0E6C7BE
QASIM.pdf	412CA0030F07729AE1E0C74E6A24C962E33CF30397E768FF63 D3ADEE0EA94F20BCC39E2051F29F663F877639D52BF20A4A3 1376E0B78EC5DD4495927C1382178
Rambus_Press.pdf	333A954C9E71DC993BCDD386494DAB6D5F1C92FD923D4E38 06843911D2A9F98CD7CAD0CA34DB71FE25444833F221BE3F1 325D49EF2A1F72F8C64A42A061D6B67
Securing_Payments_Payments _Tokenization_in_Primetime_S usan_Pandy.pdf	875973E804A5800330E6FFCB7D5FC3E9BB11D2BC66F10838C 7342F8E4E48BA0FC2762F20E1408C6DC2931DFBD824D1A11C 6799593DAECD4DCB09435D707AA4A5

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"EMVCO Publishes Technical Framework for its Payment Tokenisation Specification," EMVCO, March 11, 2014, pp. 1-2.	
	2	"Encryption and Tokenization: Which is best for your business?," Townsend Security, 2010, pp. 1-4.	
	3	MOLEN, "Engadget Primed: What is NFC, and why do we care?," Engadget, June 10, 2011, pp. 1-11.	
	4	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-11.	
	5	"Financial Cryptography," 5th International Conference, FC 2001 Proceedings, Grand Cayman, British West Indies, February 19-22, 2001, Paul F. Syverson (Editor), pp. 1-57.	
	6	"Gemalto to Provide Isis Mobile Commerce Platform with Trusted Service Manager (TSM) Solution," Business Wire, December 12, 2011, pp. 1-3.	
	7	"Google Checkout checks out, replaced by Google Wallet," Android Community, November 17, 2011, page 1.	
	8	"Google Checkout HTML API Short Attribute Reference," Google Checkout, Google Code (archive.org), March 27, 2012, pp. 1-4.	
	9	"Google Commerce: Building one wallet: Google Checkout is transitioning to Google Wallet," commerce.googleblog.com, November 16, 2011, pp. 1-2.	
	10	"Google Prepaid Cards," Wallet Help, Google (archive.org), October 3, 2012, page 1.	
	11	CLARK, "Google Unveils first Android NFC phone - but Nexus S is limited to tag reading only for now," NFC World, December 7, 2010, pp. 1-4.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Google Wallet launches officially on Nexus S 4G," Android Community, September 19, 2011, pp. 1-2.	
	13	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, September 19, 2011, page 1.	
	14	BOULTON, "Google Wallet Mobile Payments Coming to New York, Francisco; Google Wallet will launch this summer to enable consumers to pay for goods by tapping their Samsung Nexus 2 4G Android phones at NFC-fitted sales terminals at Subway, Macy's and other retailers," eWeek.com, May 26, 2011, pp. 1-2.	
	15	FINGAS, "Google Wallet reaches the web, reminds most of us that it exists," Engadget, October 4, 2012, pp. 1-6.	
	16	RAPHAEL, "Google's Eric Schmidt spills clues about Android Gingerbread," ComputerWorld, November 15, 2010, pp. 1-3.	
	17	"Handset makers line up behind Isis NFC payment platform," Old GigaOm, September 27, 2011, pp. 1-2.	
	18	"How it Works," Wallet Help, Google (archive.org), March 12, 2013, page 1.	
	19	"How to find out IMEI number on Google Nexus S phone," Tech Notes Desk, January 10, 2013, page 1.	
	20	"La Caixa," Annual Report, 2010, Barcelona, Spain, pp. 1-190.	
	21	"INSIDE Contactless to Equip KTFMobile Payment Project Mobile Phones; Korean Manufacturer Confirms INSIDE's NFC Maturity by Embedding MicroRead into LG Electronics and Samsung Electronics Mobile Phones for its Mobile Payment Project," Business Wire, July 16, 2007, pp. 1-2.	
	22	CLUCKEY, "Is a contactless ATM inevitable? Bank of America seems to think so; the FI has filed a patent application for a 'Contactless Automated Teller Machine,'" ATM Marketplace, September 20, 2012, pp. 1-3.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Isis™ Launches in Austin and Salt Lake City; As Many as 20 Isis Ready™ Handsets to Be Available by Year End," Business Wire, October 22, 2012, page 1.	
	24	PEREZ, "Isis Revealed: Carrier-Led Mobile Payments Venture Shows Off Its New App, Announces Banking Partners," TechCrunch, February 27, 2012, pp. 1-6.	
	25	SADEWO, "Isis to officially launch on Oct 22, more supported devices announced," androidauthority.com, October 18, 2012, pp. 1-2.	
	26	"MasterCard Approves NFC Phones from HTC, Intel, LG Electronics, Nokia, RIM, Samsung Electronics and Sony," Professional Services Close-Up, May 10, 2012, Close-Up Media, Inc., pp. 1-2.	
	27	"MASTERCARD INC, FORM 10-K (Annual Report)," Filed February 28, 2007, for the Period Ending December 31, 2006, pp. 1-204.	
	28	"MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer," Global Hub, Engagement Bureau, Press Release, October 1, 2013, pp. 1-2.	
	29	"Fact Sheet: Mobile Commerce: A New Way to Pay: MasterCard Mobile Commerce," May 26, 2011, pp. 1-4.	
	30	"McDonald's testing e-payment system," USA Today, May 29, 2001, pp. 1-3.	
	31	"Mobile Contactless Payments Trialled Live at Mobile World Congress 2010; GSMA, Samsung, Telefónica and Visa, with Giesecke & Devrient, Ingenico, ITN International and La Caixa, collaborate across industries to give Congress attendees an opportunity to experience NFC," Business Wire, February 15, 2010, pp. 1-3.	
	32	"Mobile Payment Bringing value to payments on mobile," Gemalto, November 2011, pp. 1-4.	
	33	WOO, "Mobile PayPass Meets Cloud in Google Wallet," Global Hub, August 1, 2012, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	HEUN, "Mobile Wallet Consortium Strives Cautiously In 2012; The telco joint effort proceeded more slowly than expected, but its leaders maintain that the mobile wallet business is big enough for lots of players," Section: MOBILE: ISIS, January 1, 2013, Page 47, Vol. 2, No. 1, SouceMedia LLC d/b/a Arizent, pp. 1-3.
	35	BELL, "Mobile's Gains Prompt More Banks To Move Beyond Cards For ATM Access," Payments Source, Section: DEBIT: Vol. 1, No. 1, May 12, 2011, pp. 1-4.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IPR2025-01150
Apple EX1071 Page 1340

UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 01:46:45 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424625	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 50

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_2.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1237 KB
Global_Hub_Engagement_Bureau.pdf	2	Non Patent Literature	1475 KB
Google Prepaid.pdf	1	Non Patent Literature	376 KB
Google_Checkout.pdf	4	Non Patent Literature	3470 KB
Google_Commerce.pdf	2	Non Patent Literature	732 KB
HEUN.pdf	3	Non Patent Literature	1732 KB

How_it_Works.pdf	1	Non Patent Literature	451 KB
INSIDE.pdf	2	Non Patent Literature	916 KB
Isis.pdf	1	Non Patent Literature	757 KB
Android_Community.pdf	1	Non Patent Literature	467 KB
BELL.pdf	4	Non Patent Literature	1164 KB
BOULTON.pdf	2	Non Patent Literature	906 KB
CLARK.pdf	4	Non Patent Literature	2713 KB
CLUCKEY.pdf	3	Non Patent Literature	1441 KB
EMVCO.pdf	2	Non Patent Literature	1685 KB
Financial_Cryptography.pdf	57	Non Patent Literature	3150 KB
FINGAS.pdf	6	Non Patent Literature	3940 KB
GARSIDE.pdf	1	Non Patent Literature	884 KB
Gemalto.pdf	3	Non Patent Literature	878 KB
GigaOm.pdf	2	Non Patent Literature	1035 KB
La_Caixa_6_of_6.pdf	30	Non Patent Literature	17444 KB
La_Caixa_1_of_6.pdf	32	Non Patent Literature	21513 KB
La_Caixa_2_of_6.pdf	32	Non Patent Literature	22815 KB
La_Caixa_3_of_6.pdf	32	Non Patent Literature	23969 KB
La_Caixa_4_of_6.pdf	32	Non Patent Literature	23751 KB
La_Caixa_5_of_6.pdf	32	Non Patent Literature	22026 KB

MASTERCARD_6_of_10.pdf	23	Non Patent Literature	17955 KB
MASTERCARD_7_of_10.pdf	11	Non Patent Literature	9661 KB
MASTERCARD_8_of_10.pdf	23	Non Patent Literature	22363 KB
MASTERCARD_9_of_10.pdf	11	Non Patent Literature	5409 KB
MASTERCARD_10_of_10.pdf	68	Non Patent Literature	2896 KB
MASTERCARD_1_of_10.pdf	16	Non Patent Literature	15168 KB
MASTERCARD_2_of_10.pdf	18	Non Patent Literature	20531 KB
MASTERCARD_3_of_10.pdf	17	Non Patent Literature	17524 KB
MASTERCARD_4_of_10.pdf	9	Non Patent Literature	8309 KB
MASTERCARD_5_of_10.pdf	8	Non Patent Literature	5521 KB
Nexus.pdf	2	Non Patent Literature	571 KB
Professional_Services.pdf	2	Non Patent Literature	862 KB
RAPHAEL.pdf	3	Non Patent Literature	2247 KB
SADEWO.pdf	2	Non Patent Literature	534 KB
Tech_Notes_Desk.pdf	1	Non Patent Literature	404 KB
TechCrunch.pdf	6	Non Patent Literature	2920 KB
Townsend_Security.pdf	4	Non Patent Literature	3446 KB
WOO.pdf	2	Non Patent Literature	991 KB
McDonald.pdf	3	Non Patent Literature	1042 KB

Mobile_Commerce.pdf	4	Non Patent Literature	934 KB
Mobile_Contactless.pdf	3	Non Patent Literature	1066 KB
Mobile_Payment_Bringing.pdf	4	Non Patent Literature	2643 KB
MOLEN.pdf	11	Non Patent Literature	6042 KB
nelenkov.pdf	11	Non Patent Literature	7576 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_2.pdf	BA5830495ECB05C97C396842A418096913A6E649F75664D3958C60D9CB72FBCD84283D12C381C98A5D1F8300B27A2E65DFB0144E59DDF6C3BEC22FC610CC32E7
Global_Hub_Engagement_Bureau.pdf	1B2860549A9F1865136D4CE3E063C0FE6E3A4FAF018910007863734D65E5C569F0CFECF996FA01A0019C2B9A76CB689B9DEB760C764B665434789199C46603D7
Google Prepaid.pdf	8B959C8B9FF29691DA36109A27CA0546D1E5ED86E05C7C2D718BF7233732E5971CA4EC9838E68135651FD99EE59DFE227D3C1E4BB8953AD92156FEF958C1D03D
Google_Checkout.pdf	DE1F2BCF81860AE1700F454C78CB662CB8F2012C4BF435FBF9386171224F5A2374259149A295785CD3CB53F7CED26AEE8CD6E79BF92FDDC6D0778EABF6EFE3CD
Google_Commerce.pdf	D6A206586977D368963108F750504B9C64DF513A0277AA7DF4443390E8082E29D3CAB008CF227C7954E187BD02E65015A25FF3085AF9872EAE071C681F4D067D
HEUN.pdf	4518A78961CBC9DD99CC0245FA7782798E5599CE9D9FF2C40943E617400FADFB527A60B372B9839BC2CAC96FCD3ED7893CFCBAEB9685E874459A29FAB1558E25

How_it_Works.pdf	6A1075DBE81FC8DFFA36D02EC494923AF1949AF433B4C1ED6C2BDC0F74ED79F0D2D34B51A9E6B84EFC136F91DFD756E1865AE2C1E5BBD6661859ED884D80649B
INSIDE.pdf	06D31CC4E819EDF91CFB310231189A1DA08355775DFCDDF4EE9E253F98B94CEA1756F1296F3400EB146B0C24C3C6B3B87A862FF81C3B98A70D9130AE4190F406
Isis.pdf	0B1F28A30106AC28361C50B4C69409BE601C7A4FFE4A6DA75867F09CC2FC8062DFB32A49C3488C2218D96BBEABA26CCC7631994B1A1E8AB6E97C09378C65514C
Android_Community.pdf	C3BC9C2062C05D56BA3660C9F2D60486B0BEB99D18E73A594875AECC931B2634A7544F3FB23E57F1710789F76019F9AC8DC71F618DF2D18F6D854682C51537EE
BELL.pdf	315832184105E00308AAD8A29B95A000D6749F8CB7C65041F9566C441DD3162D1FC7A19009D00668D356569BBC482284FFFEDCEA7F1CFEE4F075B0AB357DA480
BOULTON.pdf	E6D39974975D00C9AB39E25494338B6DC0EEDB4F1D0D4DF00AB2B703A05F8FCD8D56657CDD2A7A603C4438CBAAFFF69ED36231A0A0679374E351C8B3927C19BA
CLARK.pdf	384376E17AF5B596674C2AC229D494E0F5ACC90454A41EC94C18184774A65C56ECAB0F4172F969E862E0B1544FB152BE402516752757C829747A0E56C46631F2
CLUCKEY.pdf	81DE99B649A5FAB49D3418750A508E9F1F6DF25034531987F96B6D18987D1AF0DEFCF0B7C5ABAC710815DBC8783FDF0530C0D2263CBC4E0E2C172D80D6170DD1
EMVCO.pdf	E49043EA9DE6EAB06874594838EFBF040F38176620AAD582C2EAA7AF1CC9ED9F5EC83021DEF43C8067A779F52D900B042896438A6C9AD9A50226F411ACD7095E
Financial_Cryptography.pdf	8AD5653B2E0B3E6D48A3A006BCDA86D880D9DC1DDDBE9CB2DFCA329662729C3497F2744875FF09CCF031E72EC1116C7F5A4425C24EAA7099CFBEFD6C4B4E0449

FINGAS.pdf	F5F5A38053FDCD7C45275A7CC8F5B1DF3178E0F710A9B443C0367EE949B9D01CF79A1F9440DB7D9444F744C68037ACD0D46841CE792929FD5B6FB364CF179E90
GARSIDE.pdf	CF87ECE84BC9B4ABA95B312829C5F63D0B681E82700761A0D2C40116CEC37B7EAAA27EEDD13D40A2FE6DD20AECD59AF4480F423F9FD46A2C3E1ABAC5E9F6E6F0
Gemalto.pdf	3D6D9B0AB8B7880DC398814B53D29D703969763EA27B3FC1857D3F7751313A5620E42EF0480F18B4B5BA4FBDC76B8CBFE833E9D80C5A11262D0A57D2FBD385A5
GigaOm.pdf	1350964A54E57749A04DF79088AE54D805D398FAD47C2196517DCC1FEB5398916789DE59319492D14578F7DDE32AF54C6931F60D26758A39B5DA607ACEEF0A53
La_Caixa_6_of_6.pdf	B985241C5F6784FC20C29002A7A7AF3D8F612BD40ED122824A6C1F5F6AC598952B6A997280F03FE5C8D815141A6270DF94913BE22320F63B77BC7FE47AAAA789
La_Caixa_1_of_6.pdf	6067EC177712DA341ACE17FCDFC84CC30E24FF87E635F26BF2F96FE9CB3B82FEADD90C94FE02CD9AB91CE35BF932C01D45B0B485DE6D04EB49A3E9CEC1D67FE7
La_Caixa_2_of_6.pdf	EF8BE7810751C2D53CDB859E9D4177268EAD1B4A05C8CD5D559846A1CDF5162D4E3DA4D3124BA3414196118AE05D3532573B91831742F2FDE10A4CCF3F107263
La_Caixa_3_of_6.pdf	9F15E16381D20F1AE4DD17CCCDB4D1B0CF9DA6D7ECB795527A97FA3BA6F4CD299F577DFBB9464B2DE61B074DFDA093258FA720376A3D187AD6D0B71CD55528FE
La_Caixa_4_of_6.pdf	A7403E4E11CFCB0348C4A5E248246A9DC0BCB87466201A2C4DC8EBBDC6335F360E9849235295B6C977A8E636FDE5D13F1E9D18924F010975EB5A01D1FE6CB78B
La_Caixa_5_of_6.pdf	B70D3D3DA9361727698707DD052C2F4379DD4A752D79B0B06737CDC44052618EAB10253E4B9D3D2B03D10ACC61665E930613D1F7A867D924DDE413B1B339A008

MASTERCARD_6_of_10.pdf	FDA16A567C7AD537B8F913F79E9F710BD2FA86F0F28DC3CE5A21546F31B02D24D8A9FD529A74E71006F1346F7726E9BF657A6445606D9BFE87E9A3FAF807DBCC
MASTERCARD_7_of_10.pdf	69B212D15BAC37F3163786A6F720DD1686351F62076E47FA201CD90F441173DBBFDE18B7B5765AD9D3325CCCFBEFD3754A830FFF06CE34C488BE5AB5A9DB0628
MASTERCARD_8_of_10.pdf	F7228FEFE4EB74FA3DB9A137027494961B592F3860A0682849CA771838EDDD45A034B8C008C571D26F5E5DAB54B9A2E93358BC639D9B05F955A5CB28A87BB5EB
MASTERCARD_9_of_10.pdf	C065FE1371A60E2A6C7407E5D8BB6D0394195A54796C70D1FF25CB3CCC99D8BC6B31EABDC6E1B17FCB01FFC11CE432A6BADEBDD85D5CE286C3915394FFCEB0BB
MASTERCARD_10_of_10.pdf	86C8EBC3B75FDCC84C2FE3E2AB2ABEC0DAA1CBF8391C0574D363AFDE5F889CF4149609E0BEE685EA21FC1B965C72417AE78A282C998D6A27C150DC8C267D190B
MASTERCARD_1_of_10.pdf	7AE810B5E952B26E945BED3DFF552935360682F39E99CA6989D99CC20921CB9ABD2D3DC2D9FB80450034F260D9E8E6C1B899847612B9FE06143BA36ACB225013
MASTERCARD_2_of_10.pdf	0E8A605D28CBE07995AE1652D69FCE321DEB5C1307576C42735560DFDF0ED540FCE9B8F637C963C95E9D9782D623A29033DE9FD7C2A9B0BFA6F34FCCEEBC6B69
MASTERCARD_3_of_10.pdf	F5B7FD326B1E4A5C7725ADC75EC7D614C0388311A63F82349A0AB673B98B08AF2C7984649EB4F722A12AC6A611E52615BAF9F34D7A7A8B5604494E4E4E5621B1
MASTERCARD_4_of_10.pdf	24406E095B1C7D490FFE0CB8C1258C03E8752468EDDC38680815988BC9CDCF625828C5E5E6F9AB5846122D9AF6FB82AE3345A24F41EEBF5F336D9EDA1A84950D
MASTERCARD_5_of_10.pdf	4CA7B532789C799CA62C239737A7586FFD2A4DD8AD9999DD8910E659D80CB5E30F37A6C504C810A34E222C893C160913C5713FC996A06605B6FE18816B7EEE94

Nexus.pdf	CD282E7EB93402841F3598C1ABF9323875831FC28BC5C38869538B099FF1ADF3251DCBC6944C57CC9DC480032807212CA8A8F1B1A79CA3D20F46D69235B1E282
Professional_Services.pdf	8CF1A963590524130C097DB5B2B4B5890D7A04FC91400CF1D026B4B94C3129C7EE6DFAFA8172F846E40B276760D3EBB7F766E6DD68CF1B40D89908314E08E74F
RAPHAEL.pdf	233867F75F5A66CC2E307DDB2F9454BDDA5CF6276DC1038A2D4CD3750E2CF0E5F746B7801AC979F5D9FAD49C0CE2C638CA5A6D915D2DE75ADA795F4ADC025BA6
SADEWO.pdf	81450CBFEE8BC606808F7CCF9CF2E91DCAC75A91F44CE662E2DFFF88FD5EA7CE429CD3225C048A8A6BBD1689CC3DF3B8AEB788B54F41424C03A4FFA67B926D9A
Tech_Notes_Desk.pdf	6983DE0BBC7E54384E3180638091F493CCB954E76A4CB98A20F4F4D2EF379CCCAB748D6FE86BDBEB4E83A50C2110265A2F6D6BF55F0EE95D3B278A2C479F6266
TechCrunch.pdf	6F15C32BC3889798312969 9DDBA3B8F066B911CF4174D4FCB6DF3D7687D639EDAA4F0AFFA409AFF581AB1ACDAEB42BD27209ABA831831B36FBAB9A54C9EB1473
Townsend_Security.pdf	0FFA78E14FD633D718F240117AD1CDD22780404495877A3F83841834AA4A81C3238E580C9267DF46433445C610657AE1127DAFD4CDDA10B5C46FF1829E99A62C
WOO.pdf	5515199EAF19479E8EB34185F3050DE852A2DABE1D7515C140AD39FA93034B77A9EA3A23A8D1D2B7FD4528CBE2F52CD0F82D8A02ADA1516A5B7CF209B6BF6B50
McDonald.pdf	FF3C99784A6AC857ACEE5F64B2ACB7940FCF7DA7F752A38CFC60EB7773FEFEEC63F34106FC94BF8B5830919C173C73A95A7F2487B673065028807C05C07C09CC
Mobile_Commerce.pdf	0C444481F5FAF77E1A024752C687615FEF5B3540D496D12BBE8F7D9738C6E541B472EC16FC621FF600423C138BA7E5AEBE59185E6BCB6C5891C0D475FDE5809B

Mobile_Contactless.pdf	449F08C62980BE2BE60DA53B29F7A0C80EFC4C85C63A4C595A12836E103D1329E8F0C7B5BEC56DC54634861E264463B535EF6A08A939E4789D74679F9F40DB78
Mobile_Payment_Bringing.pdf	848523007D735C5E54C5F4B4DB6664458D511C4F7F5F803DB695C7B27BD373C155FA94D594FE6B9698B6F40F254D6D3453DB4C64BA64B88A1F91C7D9BBC76A8C
MOLEN.pdf	2DC48712A930C9EEED6A6AE3DF301005B13B3F9A539FFC0B681DFC9D4D613B745FC0FC1D07CA00BCA7CCCC1C731568892D309F5D3154206D8D93CEFB4CB8775E
nelenkov.pdf	F808120F02058F894E7E039FA3136A5EFD52AD3AB88AEA3DD05314D11F36FB64AD149608CB9C76129FE688CF82606CD781000AD235E837E496556926D7A5F43A

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Motorola MotoACTV Smartwatch, http://www.manualplanet.com/pdf/watches/motorola/motorola-motoactv-gpsfitness-tracker-quick-start-guide.pdf, 2012, pp. 1-2.	
	2	PEREZ, "New NFC-Enabled Phones to Hit Europe," ReadWriteWeb, February 18, 2011, pp. 1-3.	
	3	WESTER, "New Samsung Galaxy S4 phone includes NFC, innovative barcode technology; New Samsung smartphone adds a number of features that may spur mobile payment adoption," Mobile Payments Today, March 15, 2013, Networld Media Group, pp. 1-2.	
	4	"NFC Focus: Which Smartphones Have NFC?," International Business Times News, August 9, 2012, pp. 1-3	
	5	"NFC for mobile operators; Maximizing opportunities in the mobile NFC marketplace," Gemalto, November 2009, pp. 1-2.	
	6	CATHELINAIS, "Nice, the first city to switch to contactless payment," 01net.com, May 21, 2010, pp. 1-6.	
	7	CLARK, "Orange to offer Samsung Wave 578 NFC across Europe - but not in the UK," NFC World, February 14, 2011, pp. 1-4.	
	8	CLARK, "Orange to roll out NFC services across Europe in 2011," NFC World, December 16, 2010, pp. 1-3.	
	9	"PayPal Credit Card Tokenization Extension - Magento Connect," Magento Extension Marketplace, http://www.magentocommerce.com/magentoconnect/catalog/product/view/id/18715/s/paypal-credit-card-tokenization-extension-4490/, October 5, 2013, page 1.	
	10	Nanninga, "PayPal Credit Card Tokenization in Magento," SitePoint, September 30, 2013, pp. 1-11.	
	11	"Payment Card Industry (PCI), Data Security Standard, PCI DSS Applicability in an EMV Environment, A Guidance Document, Version 1," PCI Security Standards Council, October 5, 2010, pp. 1-12.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	'Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Version: 1.0, Information Supplement: ATM Security Guidelines," PCI Security Standards Council, January 2013, pp. 1-44.	
	13	'PayPal NVP API Developer Reference Enterprise Edition - eBay," August 28, 2012, pp. 1-382.	
	14	'Rambus' Bell ID to support Android Pay," Rambus, February 18, 2016, page 1.	
	15	'RIM implements Bell ID's Token Manager software for mobile payments," WMI Company News, January 23, 2013, World Market Intelligence Private Ltd., page 1.	
	16	LAI, "Samsung and Visa join forces to enable NFC mobile payment at 2012 Olympics," Engadget, April 1, 2011, pp. 1-6.	
	17	'Samsung and Visa Showcase Mobile Payments at the London 2012 Olympic and Paralympic Games," Business Wire, May 9, 2012, pp. 1-4.	
	18	WARREN, "Samsung and Visa Take NFC Mobile Payments Global," Mashable.com, February 25, 2013, pp. 1-2.	
	19	HASELTON, "Samsung and Visa team up for NFC mobile payments at London 2012 Olympics," Boy Genius Report, March 31, 2011, pp. 1-3.	
	20	'Samsung and Visa to Showcase Mobile Payments @ the London Olympics," Samsung Global Newsroom, May 9, 2012, pp. 1-3.	
	21	'Samsung Announces Launch Dates for Groundbreaking Mobile Payment Service: Samsung Pay," Samsung Global Newsroom, August 14, 2015, pp. 1-2.	
	22	GROTTA, "Samsung Begins to Phase Out Support of MST for Samsung Pay," PaymentsJournal, February 22, 2021, pp. 1-3.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	MURPH, "Samsung cooks up its own NFC module, destined for the Nexus S?," Engadget, December 1, 2010, pp. 1-2.	
	24	MOLEN, "Samsung Galaxy S III for Verizon Wireless review," Engadget, July 9, 2012, pp. 1-10.	
	25	TRENHOLM, "Samsung Galaxy S3 is Olympic phone for no-touch payments," CNET, May 9, 2012, pp. 1-2.	
	26	"Samsung Google Nexus S - Full Phone Specifications, Reviews: Royal droid," GSMArena.com (archive.org), November 2010, pp. 1-2.	
	27	"Samsung Google Nexus S review: Royal droid," GSMArena.com (archive.org), February 11, 2011, pp. 1-2.	
	28	"Samsung partners with FeliCa for Japanese NFC solutions, unveils 2012 Olympics' mobile payment app with Visa," Engadget, February 24, 2012, pp. 1-3.	
	29	CLARK, "Samsung picks NXP for S3," NFCW, May 14, 2012, pp. 1-2.	
	30	"SAMSUNG to Acquire LoopPay, Transformative Digital Wallet Platform," Samsung US Newsroom, February 18, 2015, pp. 1-2.	
	31	HEUN, "Samsung to Unveil NFC Smartwatch - Has Wrist-Payments' Time Come?," Payments Source, September 2, 2013, SourceMedia LLC d/b/a Arizent, pp. 1-2.	
	32	"Samsung's New Secu-NFC Chip Enables Secure Mobile Payment by Enhancing NFC with Security Features," Plus NEWS, November 30, 2011, pp. 1-2.	
	33	NANNINGA, "Save Credit Cards in Magento with Our New Paypal Extension," Classy Llama, August 15, 2013, pp. 1-4.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Shift4 Releases New Technology to Insure the Security of Its Merchants' and Partners' Payment Processing," Hotel Online (archive.org), October 5, 2005, pp. 1-2.	
	35	"S-Pay: What is MST?," Samsung Levant, September 22, 2020, pp. 1-2.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IPR2025-01150
Apple EX1071 Page 1356

UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 02:09:45 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424648	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 49

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_3.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
MURPH.pdf	2	Non Patent Literature	1799 KB
Nanninga.pdf	11	Non Patent Literature	5410 KB
NFC_for_mobile_operators.pdf	2	Non Patent Literature	1832 KB
NFC_Smartwatch.pdf	2	Non Patent Literature	729 KB
NFC_World.pdf	3	Non Patent Literature	1717 KB

NFCW.pdf	2	Non Patent Literature	642 KB
Payment_Card_Industry.pdf	12	Non Patent Literature	7876 KB
Business_Wire.pdf	4	Non Patent Literature	1109 KB
CATHELINAIS.pdf	6	Non Patent Literature	2624 KB
CLARK.pdf	4	Non Patent Literature	2212 KB
Classy_Llama.pdf	4	Non Patent Literature	1389 KB
FeliCa.pdf	3	Non Patent Literature	1019 KB
GROTTA.pdf	3	Non Patent Literature	983 KB
GSMArena.pdf	2	Non Patent Literature	1073 KB
HASELTON.pdf	3	Non Patent Literature	1674 KB
International_Business_Times.pdf	3	Non Patent Literature	970 KB
LAI.pdf	6	Non Patent Literature	1345 KB
LoopPay.pdf	2	Non Patent Literature	561 KB
Magento.pdf	1	Non Patent Literature	388 KB
Mashable.pdf	2	Non Patent Literature	748 KB
PayPal_5_of_13.pdf	30	Non Patent Literature	16398 KB
PayPal_6_of_13.pdf	30	Non Patent Literature	19630 KB
PayPal_7_of_13.pdf	30	Non Patent Literature	12785 KB
PayPal_8_of_13.pdf	30	Non Patent Literature	5647 KB

PayPal_1_of_13.pdf	30	Non Patent Literature	15334 KB
PayPal_2_of_13.pdf	30	Non Patent Literature	17236 KB
PayPal_3_of_13.pdf	30	Non Patent Literature	22001 KB
PayPal_4_of_13.pdf	30	Non Patent Literature	22603 KB
PayPal_11_of_13.pdf	30	Non Patent Literature	16996 KB
PayPal_12_of_13.pdf	30	Non Patent Literature	11931 KB
PayPal_13_of_13.pdf	22	Non Patent Literature	15402 KB
PCI_PTS_POI_1_of_2.pdf	30	Non Patent Literature	18011 KB
PCI_PTS_POI_2_of_2.pdf	14	Non Patent Literature	8792 KB
PayPal_9_of_13.pdf	30	Non Patent Literature	17093 KB
PayPal_10_of_13.pdf	30	Non Patent Literature	16828 KB
Samsung_Pay.pdf	2	Non Patent Literature	964 KB
Shift4.pdf	2	Non Patent Literature	1706 KB
TRENHOLM.pdf	2	Non Patent Literature	1139 KB
WESTER.pdf	2	Non Patent Literature	890 KB
Plus_NEWS.pdf	2	Non Patent Literature	880 KB
Rambus.pdf	1	Non Patent Literature	715 KB
ReadWriteWeb.pdf	3	Non Patent Literature	1647 KB
RIM.pdf	1	Non Patent Literature	563 KB
Samsung_Galaxy.pdf	10	Non Patent Literature	5158 KB

Samsung_Global_Newsroom.pdf	3	Non Patent Literature	1692 KB
Samsung_Google.pdf	2	Non Patent Literature	892 KB
Samsung_Levant.pdf	2	Non Patent Literature	36 KB
Motorola.pdf	2	Non Patent Literature	946 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_3.pdf	E8F9662C840C33CF74178A92BD1829C7645747EB26A802ED12E1CDF6307F71904B95419B294EB20E078BEE49209BD45CE9EDF460301F3A713431337AAB1E019F
MURPH.pdf	3343EC02813F63AA251B29CCB759F410E7DA034EB61509565ACE5C9EFB123AEAF72763AA84F7C49FF21BD23F3C363C889D16EBBF249264F22730C98757B8C2BC
Nanninga.pdf	958C75487F5B101A3DF678BB33ECD2362EC70D1BB1E99FABF60F92FBB86C5E32EBE2ACB431B21C0FC3B99596EE2F29AED38D7D10FDA0D03AB4A851A1998F02A5
NFC_for_mobile_operators.pdf	68894F1EA5E57AFB428276AACEB67DCD87754F069DC06BE8C468402382602E46A6EF22F9B1E56929DAFD6071B57D0DD37C4C736D5ACECEE2C42DBCE88F2A0DFC
NFC_Smartwatch.pdf	7216E6FB9A7DBFA2E8C65E91A93623E3B7768ACBECBA0D1C5ECF5D6AF20D0A3CE3B46805B3AD220580186DA805E4FEA388EBCC888906FB1FF79261D1B2207285
NFC_World.pdf	9990DB3A91B2A162BE8A7131186E480FD515164903DC41D44B691329A44DA8A0148088C7102DFAE24355D1D5DF6C29BDC46067C259515B0A34AE3BCB543F3554
NFCW.pdf	0748C68CB295C0077BE7B8928744DED92BEB79BFA2E6D774

	E908A2AEEF7A4A9D6748A838206FB16F1E5C4295E044E61F2D3048568546686CD73C29BBE8D2FA4
Payment_Card_Industry.pdf	D548536D5AE1478E7351E8AAE2493CF8D203FF8D012F486EF1088DDCF885FBA6E70F5A8836711E8AC61B025E2D344E21F5171B54F1D8EEB7471FB13D2454F217
Business_Wire.pdf	9BBA328F64D067B28C7B507554458C1F8724977B81EA513E7E3BF45B90A68A1589DADA1C06AAFC4548A17BEACD5C3F2FAC9E180D40C6597C5805F8A53473C28F
CATHELINAIS.pdf	6E916ABFEE7615F6351CA0EE2774D195CAA14EABDC8DA1886EC415FC838AFFFFC9E5820F181094913BB9DA254A8E88B27DAB125AA0CB6F79BA313B36AAC3BCC1
CLARK.pdf	5542D017F144811C16CF888D6BBB7BF937D52EE45BAAC79445947646EF2CFEF1E289CE92E82BE16B6D177545AC495DF4B77FF43AF8A77FD40551ED6BB0F2376C
Classy_Llama.pdf	72B58E9ADC9D64B80D65D35E68476DE49AED4236C00680BC8AAC8D9849A6FEB3AFF61528270AAE548588993359408C15EA4DF7E053370311F3A4F8F59FB0CAB6
FeliCa.pdf	670F486FEC047C6C1A05C06ECEE07B5DB59E59999ED5D6F0D07CB42A663BDE44D62BA8124C00805BCCA25D2281511FE9DE077A1B5AE25FFC8BBCAEA458D2BAC7
GROTTA.pdf	FD48510D7BB56CA1A742C865728E869091FC6F2FC95539459F62C2CC299DFE18CFDA1E3CA4CBEBAF9948085D53DD91BEC83E1C4359ED9785F382C4A5EB235D68
GSMArena.pdf	F8AB00D2266A2F0638BF0DEEE9661533D41B7F3F1E02757A19C1E45523B10D894F323DAD77D3898BD9A68647F3614ECD542A905BABC187E19A0C0BC57479A3C7
HASELTON.pdf	3B7D85DE2D57659655D30DCA596E3C15B939FA21061DD1ABAC3031695BF7E0327E2979EE882A950F0C040D0D755A87E015047BF0E8E7FBBE6732B05F1DBFAD4C
International_Business_Times.p	591C8296C7326A16249AA877F4DF77F5FA1222CA14F49ECD1

df	3EEE469437C0869529539DA8E74FC2414298BF01CE7948FEC E28D4747812821499D614FDFE2FA81
LAI.pdf	3059934B176978C6E78F0C0FFC9F3B1CA3369EA0AE1291B518 0D3C009793D862B8B926ACEE4D027671DF0A4DDB46103914F 983126613D4694BAF81337131FFB1
LoopPay.pdf	7039BEEFF390C4B80E8AFFED67475DCDCBE0ECE48239F5B6 9CFEC0AF61457CA3E0CB46D8F2F52FF1B561BF840F17692D6 2D5FE6CB64B830BCD62791A79669F22
Magento.pdf	44AF16EA96332713F7D66853873ABB9F41D01E8CA30EB17FC C35C5F266C03B15DCB10425C21F0B7CDF1A5749813 6A6B343 6772372849322EB77B87F793066A9B
Mashable.pdf	3F0BA00846A5FCA74ECFF125CD4BC670652E67CBB6B4B1EA 4002C91634BBB681D6F408569CE24691BD2877D28667C30B22 6E67D782C07744F978BF9F5B3C2B34
PayPal_5_of_13.pdf	9CACF4F33E2096E277465D5963E5EE84B05C3BD88269101A5 80428F5463D0FC56D7281BEA8A6E6CE2F51BBD4F41317BD6E D333E0071F114AB9F74EBC8CE4C20A
PayPal_6_of_13.pdf	F7914E8F14A46A69FAE5D1B04F73DCD42BD7ECB560AE8C43 5D086A5F3B028D95D65C5151A476EEFD4C42822F609E91AF8 F3EE98A04E830DA6CE21368B5FDB108
PayPal_7_of_13.pdf	7CCBDDA691AB8E566F8B5119FDFE4528C0EE48A5A635BBE2 35EC5D2206E614F17F39EFFC674C7533BEA9F6A4840FFC537 422782BC1C94FD57C17C86E3BF121FC
PayPal_8_of_13.pdf	E27C2390D887B918E317E516BB462556ACFE0EA45F6DCAB50 5CC41F2A33BD16B0B3BD9B1131686908AAE8A7B97F336A92C 1712E183078ADFFF59D583AD575A95
PayPal_1_of_13.pdf	AC0FD0DE7855150CFFD10C179950A71811A00F4DFDDA72C4 1268C12A674B42E3CF9A01DD762BFB289E3678D3F005553396 CE3976FD1DC159820119642FC2E25E
PayPal_2_of_13.pdf	2C310F42691C9572B6CAF696A6AF5ED68CA7BD527685E7337

	58D9116A0DE0018A61402251695C2E458B629EE6367D254EE49ECB5BC8612CB9D9BCFE901D97760
PayPal_3_of_13.pdf	12B535B15206D4E8717E56AA41962AC82240A71075EFE1ADBC603E98753A52884D086476D3D285FEE6219107D844B60C55E1789953D65A10359A436CA290E475
PayPal_4_of_13.pdf	78315A5E792007E6F6142B05ECF1299D45B146C547EBBC14E7D7D841B7B3D298E3F0CE55D092B15951A5391E273194FD7964F6B4C5DE2E976D85BD2E038ECD19
PayPal_11_of_13.pdf	C6AFC974D2D88BF92CA5BBCC165E892141BC05DE02B95B0A327DFA058534261A4D206BCDB03AA724526433D425E4D0F36EC8E40C7B298A9D132BA89781F4FFCF
PayPal_12_of_13.pdf	05F22582C380EF3B605D38128FD1C8F5462123C46CC8227C71CA8C17D2012B87B4BAC78AB07E00A750ACB802CE14C3877CB2F057517D6F0F18745FE6277A86E9
PayPal_13_of_13.pdf	8CF0AB1E777DE8E0816A59757D3642EEC5E42929AF052936E7121818B3FE3868CE959249BE905466FFE8F6EE5F582BE06C83597CBA0BD788D31682B7CB2C4F2B
PCI_PTS_POI_1_of_2.pdf	C0B91A6103A6C07B88004B990A7D414E5913C9396630FC2CC244058EB58000E5B9A37F620883E47023FC67AA34E225EDCD7425793AA2DBD85187DC2BF20A9DA1
PCI_PTS_POI_2_of_2.pdf	FAF8888E206D4EE6F49A7FAC6C9853B5AA76FB6529797A8A98F86EEF5631E8927E3891AD31235B4F5EAC2EA329912C758F0ED8FDA450FAB62F885B76541A64FA
PayPal_9_of_13.pdf	58C0C122AD3BAF6747D0767190E7028CDF21432DDFC39D833FF603B3C868B37CF3E7C004E3EFA57396C5166256AB166F96F1572C029970825F6791858BAC587D
PayPal_10_of_13.pdf	26F5F95BEAB1B6A09781805A16344D399C7651F3CA87790583D7063930B5EE49EC8CD44389E0574DB9A19A1ADE2807D1BD71604358AE2F0787F7F22D4709A05E
Samsung_Pay.pdf	581D5F13A8CB2E23FEA45F0B826823C3CD9E92A8BB5CF3096

	C014191C7A99AD0CB2F7E15E58EAC39408DECC78B6E3D7EEDB91E85A10F146CC74353CAFD864C4A
Shift4.pdf	42F5EDB83F5B6F24A615A65FAA3075905F49A4E2CA85638BEBB17D75868E3B1431834668DEFD91F71A7AF3394C40A12C75A04DE24C27E8217B073ADEDEFA4D4D
TRENHOLM.pdf	D6E3A1ADDE798B4BE7AE403A39FC5C7FDF4E03AC0CDE0D564D8C1D31FE2204D57836A1DF056739A1AACEAC059539143E7DED32B80660A7DC0144182671042702
WESTER.pdf	206B8E60D15719ADCA9F5EE9A29F7FD7D5C64D261EDE01D91036A255713C93E7E58156E33D49199DFC5D10CE47D1C7D093F572495EE34CBE8CDBF25B6766AD0F
Plus_NEWS.pdf	C94575650FD55ECAE244F014B254DF475D23BECAE1F2BD7201DD5358D224239783AE873112734242B4B9FA6EB44FAEA9D5E4068F24AD36B2CBB106F7703F3506
Rambus.pdf	78310B3329B37D36B4842F7D1393C7792615E1676AB316E49CC95BA4498BDBF7AAFF2ED5D462DFB49AD57F02BF15F0EA0F83FF118C7C581FCFD6B474A501E2C6
ReadWriteWeb.pdf	A2A332300AED6C2E9517C2F7F5FF19ABCBA8C1BAFB15E9FC1A272377B938A7AE9BDBA49CFE1947A74C3543F6BB3647E33D5CC9D9A54876BE2177FA1F63D3CAA9
RIM.pdf	868BF8BE96D1E79F931C1BFC246DE2D6D91525D0962B3945D8D58FF12365DCF695B4F65C4B56B11066F01AB0ACD9CE3BE84C6A4AF7EDFCB3851F16D4487C6E32
Samsung_Galaxy.pdf	4257D3887702AD8610308A665E48511CEA9DE418B3FF3C956C08DFEBDC1B99A9B035708B201F5A369A762319C39CC13C3D713A3E2CB28CC5185386BED95A11C9
Samsung_Global_Newsroom.pdf	02507BBFF5B3F9948C806E2FC305B342085B008CC9A96227F0D10A9F69E401974C2197ADFE9933EC2246B9D92F761C29B101939C3DFA96A873CC7490588EE3C0
Samsung_Google.pdf	22BF35D2C3D91795D664F6742893B3DEB9C280C5297F36CFC

	C913CB022DC48F424F60BB78F13EDF7CAF283E94E1E8B2717780B92E52466261E9D42C1D39ACF0A
Samsung_Levant.pdf	F40563239657AFE4F2C1C636507E74190BE388D0246553B0159F720A82F6EA3F81635B3376E734E25CDEB73C9CC2DD0E0C83FD9F43F663BA811445C01676EFDA
Motorola.pdf	5A43B41EDECA9FCF0F787DA9B737A6E146C77E7B96386C1660EF71BF5BC8BB4F7276BB1055F0D4805B870AEE7DD55E523AFE932BD07E43F54E30407517B9763

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Standing Document (SD1): WG8 Projects: ISO/IEC 14443, Proximity Cards (PICCS)," ISO/IEC JTC1/SC17/WG8 (archive.org), October 25, 2010, pp. 1-6.	
	2	"Telefonica O2 Czech Republic prepares NFC payments," DmEurope, March 25, 2011, page 1.	
	3	MARKKANEN, "Telefonica, Samsung to Pilot SIM-Based NFC Payment Solution in Spain," IHS Global Insight, February 15, 2010, pp. 1-2.	
	4	"The Mobile Payments and NFC Landscape: A U.S. Perspective," Smart Card Alliance, September 2011, pp. 1-53.	
	5	"Tokenization Guidance: How to reduce PCI compliance costs, Version 1.0," Securosis, December 10, 2011, pp. 1-31.	
	6	"Tokenization: What's Next After PCI," RSA, 2012, pp. 1-8.	
	7	SEIFERT, "Verizon won't offer Google Wallet for the Galaxy Nexus because it uses a 'secure element'," The Verge, December 10, 2012, pp. 1-2.	
	8	"Visa and Google Sign Licensing Deal to Boost Mobile Payment Adoption," Visa, September 19, 2011, pp. 1-2.	
	9	"Visa Best Practices for Tokenization Version 1.0," Visa, July 14, 2010, pp. 1-4.	
	10	CROSMAN, "Visa Certifies BlackBerry, Samsung And LG Phones For PayWave NFC Payments," Payments Source, January 10, 2012, pp. 1-2.	
	11	"Visa Completes Acquisition of Rambus Payments Portfolio," Business Wire, October 22, 2019, page 1.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Convenience for customers. Profits for you," Visa PayWave (archive.org), January 2013, pp. 1-2.	
	13	"Verizon User Manual: Samsung Galaxy SIII," Verizon, January 2012, pp. 1-204.	
	14	"World leader in proven and efficient cards for EMV deployment," Gemalto, February 2010, pp. 1-2.	
	15	BECKER, "29C3: A Rambling Walk Through an EMV Transaction (EN)," YouTube, https://www.youtube.com/watch?v=VdNm9JJmCzg, December 30, 2012, pp. 1-2.	
	16	"ARQC and ARPC Generation and Validation," YouTube, https://www.youtube.com/watch?v=I1XTn175FFk, Paragon Application Systems, July 25, 2012, pp. 1-3.	
	17	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	18	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	19	"Credit Card Processing with EPX BuyerWall Tokenization," YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-3.	
	20	"Credit Card Processing with EPX BuyerWall Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-7.	
	21	"Find out how PayPal works," YouTube, https://www.youtube.com/watch?v=dn42Y-2uFQM, March 14, 2012, pp. 1-2.	
	22	"Google checkout," YouTube, https://www.youtube.com/watch?v=-UeYkxePW2c, June 29, 2006, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"See Google I/O 2011: Google Checkout: A Foundation For Payments," YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-2.	
	24	"See Google I/O 2011: Google Checkout: A Foundation For Payments," Transcript of YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-64.	
	25	"Google I/O 2011: How to NFC," YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-2.	
	26	"Google I/O 2011: How to NFC," Transcript of YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-62.	
	27	"Google I/O 2012: Introducing Google Wallet Cloud APIs," YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-3.	
	28	"Google I/O 2012: Introducing Google Wallet Cloud APIs," Transcript of YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-40.	
	29	"Google Nexus S by Samsung at CES 2011," YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	30	"Google Nexus S by Samsung at CES 2011," Transcript of YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	31	"Google Payments Live - Google Wallet updates," YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-2.	
	32	"Google Payments Live - Google Wallet updates," Transcript of YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-40.	
	33	"Google Wallet Demonstration," YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Google Wallet Demonstration," Transcript of YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	
	35	"Google Wallet Hands-On - Engadget," YouTube, https://www.youtube.com/watch?v=5s9wYEkRAgs, May 26, 2011, pp. 1-3.	
	36	"Google Wallet - How to Setup and Use this Exciting NFC Technology," YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-3.	
	37	"Google Wallet - How to Setup and Use this Exciting NFC Technology," Transcript of YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-7.	
	38	"Google Wallet Make Your Phone Your Wallet by Google," YouTube, https://www.youtube.com/watch?v=qRVQTQlJV0g, February 18, 2013, pp. 1-2.	
	39	"Google Wallet Make Your Phone Your Wallet by Google," Transcript of YouTube, https://www.youtube.com/watch?v=qRVQTQlJV0g, February 18, 2013, page 1.	
	40	"Google Wallet Product Launch," YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-3.	
	41	"Google Wallet Product Launch," Transcript of YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-56.	
	42	"Google Wallet Walkthrough," YouTube, https://www.youtube.com/watch?v=xmbRSXYdFFs, February 13, 2012, pp. 1-2.	
	43	"How does Google Wallet work? Really well!," YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	
	44	"How does Google Wallet work? Really well!," Transcript of YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	45	"How Does PayPal Work?," YouTube, https://www.youtube.com/watch?v=MdrPOCCFQ2k, July 24, 2012, pp. 1-2.	
	46	"How To Use Google Wallet On Android," YouTube, https://www.youtube.com/watch?v=6DeiEVBIBcs, October 28, 2011, pp. 1-2.	
	47	"How To Use Google Wallet On Verizon Galaxy Nexus - Pocketnow," YouTube, https://www.youtube.com/watch?v=AZ8t757ZfUs, April 20, 2012, pp. 1-2.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IPR2025-01150
Apple EX1071 Page 1373

UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 02:28:24 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424667	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 50

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_4.pdf	8	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
Google_Wallet_Cloud.pdf	3	Non Patent Literature	1396 KB
Google_Wallet_Demonstration.pdf	2	Non Patent Literature	775 KB
Google_Wallet_Hands.pdf	3	Non Patent Literature	1438 KB
Google_Wallet_updates.pdf	2	Non Patent Literature	807 KB
Google_Wallet_work.pdf	2	Non Patent Literature	22 KB

How_PayPal_Work.pdf	2	Non Patent Literature	789 KB
How_to_NFC.pdf	2	Non Patent Literature	764 KB
MARKKANEN.pdf	2	Non Patent Literature	772 KB
NFC_Technology.pdf	7	Non Patent Literature	124 KB
Paragon.pdf	3	Non Patent Literature	1278 KB
PayPal_works.pdf	2	Non Patent Literature	776 KB
Pocketnow.pdf	2	Non Patent Literature	820 KB
RSA.pdf	8	Non Patent Literature	5143 KB
3Delta.pdf	3	Non Patent Literature	47 KB
BECKER.pdf	2	Non Patent Literature	810 KB
BuyerWall.pdf	7	Non Patent Literature	112 KB
CardVault.pdf	3	Non Patent Literature	1472 KB
CROSMAN.pdf	2	Non Patent Literature	729 KB
DmEurope.pdf	1	Non Patent Literature	515 KB
EPX.pdf	3	Non Patent Literature	1305 KB
Exciting_NFC_Technology.pdf	3	Non Patent Literature	1298 KB
Foundation_For_Payments.pdf	2	Non Patent Literature	810 KB
Google_API.pdf	40	Non Patent Literature	746 KB
Google_checkout.pdf	2	Non Patent Literature	795 KB

Google_Checkout_Foundation.pdf	64	Non Patent Literature	1183 KB
Google_NFC.pdf	62	Non Patent Literature	1150 KB
Google_Payments_Live.pdf	40	Non Patent Literature	751 KB
Wallet work.pdf	2	Non Patent Literature	823 KB
Wallet_by_Google.pdf	1	Non Patent Literature	15 KB
Wallet_Demonstration.pdf	2	Non Patent Literature	28 KB
Wallet_Google.pdf	2	Non Patent Literature	849 KB
Wallet_Launch.pdf	56	Non Patent Literature	1025 KB
Wallet_On_Android.pdf	2	Non Patent Literature	784 KB
Wallet_Product_Launch.pdf	3	Non Patent Literature	1312 KB
Wallet_Walkthrough.pdf	2	Non Patent Literature	754 KB
WG8_Projects.pdf	6	Non Patent Literature	4118 KB
World_leader.pdf	2	Non Patent Literature	1906 KB
Samsung_CES.pdf	2	Non Patent Literature	22 KB
Samsung_CES_2011.pdf	2	Non Patent Literature	823 KB
Securosis.pdf	31	Non Patent Literature	9201 KB
SEIFERT.pdf	2	Non Patent Literature	779 KB
Smart_Card_Alliance.pdf	53	Non Patent Literature	22963 KB
Verizon_1_of_3.pdf	70	Non Patent Literature	15740 KB

Verizon_2_of_3.pdf	70	Non Patent Literature	16395 KB
Verizon_3_of_3.pdf	64	Non Patent Literature	14961 KB
Visa_and_Google.pdf	2	Non Patent Literature	1100 KB
Visa_Best.pdf	4	Non Patent Literature	870 KB
Visa_Completes.pdf	1	Non Patent Literature	709 KB
Visa_PayWave.pdf	2	Non Patent Literature	811 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_4.pdf	5E70D693D28972B92B219403B10E9073E2D866E13075ECCDDC5CD34275B1DF17B0D0E4D22E47620EF11388E751E3BFD6208192E93AD9693CCE61F632BE057297
Google_Wallet_Cloud.pdf	B6F206DBCC53DD0CC7972D397A54DFE1452E43EEED4B4D18CF22D3F5A86D62931990CE2617FA530A9377EE221D5B2D5727435A83D23E2C868EFA1AEC502381A5
Google_Wallet_Demonstration.pdf	CDF5E3E39689FDFF4505A68CE3500BD63A443ACB80E22691EF26505C4ABA564306AF35D24ED429545F39CE392010A9CEB4E87CF3E41BAE1FEE4C0507FFBBAC0B
Google_Wallet_Hands.pdf	F46B216F42A7A7BFBB67B6BCC5DCADFFF3D3F14C9BA313C7089CCAB9627894E56F4A5C9CF32737F1E37D1D5BA899DF765D5109F2228C5955C4749D63150BCEA7
Google_Wallet_updates.pdf	49BA06569961F8F3EB65593933B07CA67589DEEF5D1675BA6BE5DAC44C89C31868B99266E16B789C4966026D2E5B4DEBBA6A30F298BEE6C5D44F206120D19050
Google_Wallet_work.pdf	828A4D631937EBF37AC47EF3141F381AACAD491A908FC6102DE3C565AA3F811538344B6DC29EBAF87A95A8DD18ED5162D

	A0826DB678EBE3029D62A48884D3083
How_PayPal_Work.pdf	035B5005566DB198EC1EDFA5FEFEF19E6DD3E30A3FCB92A1 6305E364F8108AE86EA3670F7ADDD3C4D429D3027CAAE1449 68335248BF3C0D5F80EECD1C1748684
How_to_NFC.pdf	397A3713D95403C73A600EB29202AD7AFF64DAF1F332CAA76 2CFC3042519D9FDED5276A2272107ABB8B3CC1E5BC7C5AC5 564B99E31654C56EC94DEBBB26D40E8
MARKKANEN.pdf	96E9C15ECE817D004BE536A2DBFA538018C936C0232A69C7F 457E555B786240770AF10B69765AF3EE55F436FF16D247759B5 383EA6B935B443F655059407579E
NFC_Technology.pdf	21BDC2275F639A45771600E656F9737AA6B12CF3AE477D4336 FD3CCD80FD8C57D4280900FCE4A4627F6041828B83233105D E5683693D7763CACAB085B5C310B9
Paragon.pdf	0B87C16EFD6DBF194FABA3861A3C19195825F83A5B69DB480 402C8D634F45F38190EF6FB67B133EAF424C5F4892B8D0135A 5386719AD5BB6152DD11189545417
PayPal_works.pdf	A69C192BAE071C5A253C1BE11BC964161F1F67AF1FDD14927 A3B850BF1004FC0871C5E11729E3B4D076B706DDD7B5441CA 1846AD075772412A7C1CF15CAC6618
Pocketnow.pdf	B7010092212F97F7209D641CDE35B9EFBFD4A592CE2AFA9EB A24390B3DDBE059697D4E1C6C8375542DAB76FA247F215D7D B1887DDA59E43B933D1C4AEC8DD3AA
RSA.pdf	7DE349EF70CBE408BD36C605E88072A7640DCFD802E6AF264 B602DA955A58362223E553FB13CE7370DFAC2DC77DEFFA507 71662E378012E3CE2402C0C343AC7A
3Delta.pdf	5F58BF76E0A65E05FC7A09B1DDD2A3C23B2954248DB941337 FC8E7F700F8EC601B7CB134D1774C0A0D1F949B43ADB8282C 809CC9A8C336691BBB15AAB2FA44B5
BECKER.pdf	7AE3168987BC803BF6021F4321284813FB5D5E65C14977C0B5 A6A3CBC5963F29337C1BC0F0DA67626497ECA363C8F97E1F4

	8531217F359EF9BB5EAF0681C1050
BuyerWall.pdf	176A7116AFC2B862606470EE7E266B280E2BD452E21658D1A CB7FA65FBE9B086C8B26C07FB053984CF4D5C65B16F1A0A2 C3C387C43FEF85DBA58F220A87D3B64
CardVault.pdf	3EBC0558D09B9D98E4BB26775641CD309F394C5ACC8C14074 B7FC477E5A544F9463EED1A2AD7C82C3A488AAD6FD5CBCD 0BC039FC5CE6366AE7CDFF1D8E91691D
CROSMAN.pdf	79CE5973DB99844D147A1E6A600283347F9F28F1F464906FA0 CA9251E8B95BE3A12608C11DB3C45970C78C620CCCBC8C88 79CF1DFADFC0339B0991B420277445
DmEurope.pdf	D0193DFD7FF6542DBFD4542CA950AA08BD85C7F7473622E6B 7C3B2CB0A184E12AF18FBA4552611FD51243CFCC04F4484D8 9E1C3C5C1130AD38FACA3684DEEEF2
EPX.pdf	FC2AD534B54D2DD40ADAEDD7EBDA2A9E1DBBC5A8241E2E2 FFAC139EBD828E6C0E282E78C708F322A07AD018E398C49C7 AC2A4C07D8D9848B6A10C2D12E3781DB
Exciting_NFC_Technology.pdf	685F9940825018B8E2341557224608CAF6AA32041B5F13DC6C 26F856E8C64C4C782D5F69FB3654FA417CEC2BD00B156D0E3 1255849B9AEECFFA5C015CB67BFCD
Foundation_For_Payments.pdf	797359B1EF874B7BB1C6C21F0AFE7D10E1C52D3544EF8779B 080A6D9C3EE57F53A484B9741A0568ABC97D23D97D616B084 768B2B6B9D2706EFC600CD3BC3EA4D
Google_API.pdf	D62D83D2418C28439D5D885D267180506669A59785B882A87B 5EA250F2BD43AAA9AD7C764D846A49A9773F57B3754ED8657 A03A38A3B9A68C63C6602F5CEE728
Google_checkout.pdf	8E87C7C4A286876577F861B84EDE72639133271E5DCEB2B4E B2C88EC293024EF2DD27F53137BCE5F1E2CB52FE089AEB45 E8872F6C2160B95E5032F01847A5C7C
Google_Checkout_Foundation.pdf	19C9D87386B08AA4FD0077E52123F86675A593B42E5E287742 C9E431F2B52AD74C21F7BB992AB012AA6D026F79B56225E75

	3302143EA60D805E77492386F4E37
Google_NFC.pdf	0499C68DAD4A7F65FE610E9786FAEF18B8689DCD17EA0012E7BCE20D30283CFC1CC58E1F6A60715EE0E0A2D10ACD5D6EAF30A4F3C708B2CA4CD5BFAC7AA07D99
Google_Payments_Live.pdf	3194CC69D59F5CAF93E304819107E7DAC26C20685EC1E9CF05E8CF2F7C076CA53FB0A94A06FB38725E1FF42F6917C18A13D6C7211968E6360438AB63E625A5A3
Wallet work.pdf	0371B369633DDCA25DD348EEFF0F93A4721B33787F5A8C7C7EBD3892774950A2A7C56DEEE31050321OFC532638958FB3A7A696F2E52A3E8D80CE0C31648F6986
Wallet_by_Google.pdf	847808F7887C8445CC3E7158CCB4BCF0D0C9E4C0AB3F2567025FA20A9DB7033C73D436A3A804BD0132C4C302FA12193E1ACCA290B6340122BF4C03DE53DE24FF
Wallet_Demonstration.pdf	D74DAA4ADDEFAC9E0E2564BCF70DB5D481F036DA823B07190D9A03372B6AE1D251DA2ACC98820453A3B9C4C827EF145DE1613B466764D2D9F92529521A6A3C70
Wallet_Google.pdf	8B79366116A8C3BBC5869EAF1BFE11981BE0DC9DE7C1095C6BCDD35F1B9A69199439A4710F8C2DDFF1FE95B45955A7563B31B1AD5C08CC018A8C68F79636D189
Wallet_Launch.pdf	02083F93DCFB96309CDE6CA1B2343DAAF2D8A2699D47128D4BDA695EACCED01A38782BBFDB6F66EA905BCE240CA596B958D91CFDB0969E26D475486A19449CF9
Wallet_On_Android.pdf	A353DAE20A3767618C03E997A9F5084B775D4FBD3542C83F966A54D655497448A153389B80FF51F3ACB42DD44FD8EB5679A2D5AFBE6652CE0AC65C72DB396B37
Wallet_Product_Launch.pdf	0F61528E884E682744497C155ACCEB542CC9682F9925647683ADF074611828D8A4BA9138E448F059B94BD2454FE96A2EDC6AD65EE291B9C674B38E661A5E437F
Wallet_Walkthrough.pdf	1153C63A606DCB1BC1EBB86C186F5BFE931A6045E00FF3679141B38F9722C2E080746CD2104FEB73F9C269B35A3D380EDF

	DC4BF2DE9729EB675347973D74E4B7
WG8_Projects.pdf	27A492D99A1D0A9086D45D113773E32CDC2BFF721FE98090B3A96A4E32AB61C3AD54782DCD3FE57385E4BC8CA25123C762B2BCF8E6FF82E1D6E3CECA7152ECD8
World_leader.pdf	3D8EB2B23D0F0E8B878986CCB252317CD30F08B9FAA1CC8534DDE7576CD0097EAC59F88FF194DB6B8CF029DC6EA54122FB946BE1BC442A950A17C5CCA0C04CDF
Samsung_CES.pdf	9B9BFD06BD02652E9C098E0B2BAB3AFE53E4FC406E080E2D9C8220383F1EF8784469BD3008C631E129D2E2EE4397C1DA0716E0608EC81E8C894B2339DB86F85F
Samsung_CES_2011.pdf	05BB81954FDB00527DE4D9304A420559ADB891292F2D631FEE6823691998D267072B02FC55B38CD1A7F43763E175586F975C298E22A124DC75B86AE099917667
Securosis.pdf	F270B900A99253A6269E7C36147DB4F6698CBBD29D3EB51BC06E65493EFE4FDB88A6560C77C38036A26A250EC012814A28D4AD20942C4D1140F05260054BB409
SEIFERT.pdf	737CE3D851358447FC0F73A90A454BAED0409CCD60E9FED1E39C2774550B3719D50B2B37A382A33257F5F9FB28E0DD9027EE61ADB12AA08F502923C541D1C053
Smart_Card_Alliance.pdf	98AB0621D0AF0B237C70DA5B48A493B54DE0055FC58CB4EDDCECD53AE2EC17349A36B20E47B33BD367EDDAFF9755346382ABEB2330DAEB44D12D61B56A9A903D
Verizon_1_of_3.pdf	2908F01FEA2A8F32FB71FB9409C7C165767ABD9B2F7743A08E45DABE28530F2E1A991FFA0CE93DA15A123D964B3DD8254345373A954E63D22DE7C21F423958A0
Verizon_2_of_3.pdf	0429CC0F0DBE0B76A1A17BFE6B6A2CAF856FCD71D601B446F3CFD5F2959D51686F0C38A2D452901018E74FF75B0618821A913374D1554C04541930FD7722292A
Verizon_3_of_3.pdf	7EFB00955B6DF940179F345523499EB22385BFC14A53012B223D62ABE4885406AE41F5982E6D8E5AD2C660C3B555CACF383

	6561AF2AEA10A49AD30D2A4CF07D4
Visa_and_Google.pdf	F4F4F8A0FE2734FE22127DBB67A34F8A87CCB77CF25946AF2770B72DC9E6475ABC4FDA422F2989B52BC16D2B359E7009473071B9A1EE3692870EE84615A29AAA
Visa_Best.pdf	092C0EAF5A90E7AFFA4E90C6B979317A42E71C9384C640D736CE76896B6578E186A45089FD790AC5871E2DE152C8B8AA3AB9A071DCDE2E094AAB5730AEAF83B7
Visa_Completes.pdf	61707E6231D3C5DA19A0E989AD084F71611C9DE5E02CCD0B8FAC82E1B056DDE2A63D509D6D0AE27F8791098FD61BE610C1E2F14364EEFA2500C053E9A4EDA94E
Visa_PayWave.pdf	C0FE1C7C3C50168EBCE5C979A38365CEAF943B4C822874DCB0E4248DD2AAABD78E15340ACE90EA1E9C078DDE4EC67E2AFD49CE6FE34C5490BAC0F9C56C4C2844

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

IPR2025-01150
Apple EX1071 Page 1383

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Isis NFC-payment from SXSW 2012," YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 2.	
	2	"Isis NFC-payment from SXSW 2012," Transcript of YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 3.	
	3	"NFC - Google Wallet and More - EE Times - Mobile World Congress," YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-3.	
	4	"NFC - Google Wallet and More - EE Times - Mobile World Congress," Transcript of YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-8.	
	5	"Paying With Google Wallet," YouTube, https://www.youtube.com/watch?v=jTeilSIzBPQ, February 6, 2012, pp. 1-2.	
	6	"Seinfeld - Google Wallet," YouTube, https://www.youtube.com/watch?v=baaCvgTRYsU, June 14, 2013, pp. 1-2.	
	7	"Technology: Google Wallet - The New York Times," YouTube, https://www.youtube.com/watch?v=I8JOT6ban7o, September 23, 2011, pp. 1-2.	
	8	"Using Google Wallet in McDonald's!," YouTube, https://www.youtube.com/watch?v= 1p6co4YIvbA, September 14, 2012, pp. 1-2.	
	9	"Virtual terminal- #1 storing credit card data with tokenization," YouTube, https://www.youtube.com/watch?v=eSXIIGbACew, February 28, 2011, pp. 1-3.	
	10	"What is Google Wallet?," YouTube, https://www.youtube.com/watch?v=iuvyN4iZiP8, August 9, 2011, pp. 1-3.	
	11	"What is Tokenization?," YouTube, https://www.youtube.com/watch?v=ypm5FFfEN34, January 17, 2011, pp. 1-3.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," YouTube, https://www.youtube.com/watch?v=FHD5XzAlKDI, Jul 28, 2009, pp. 1-3.	
	13	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=FHD5XzAlKDI, Jul 28, 2009, pp. 1-12.	
	14	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-3.	
	15	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-12.	
	16	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-3.	
	17	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-8.	
	18	"Caixer contactless lacaixa," YouTube, https://www.youtube.com/watch?v=It2CpMcxQC4, April 4, 2011, pp. 1-2.	
	19	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	20	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, page 1.	
	21	"Understanding Proximity Sensors - T-Mobile," Transcript of YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	22	"Google I/O 2012 - The Sensitive Side of Android," YouTube, https://www.youtube.com/watch?v=Q0V_Id7iNw4, June 29, 2012, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Google Wallet Overview," YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, page 1.	
	24	"Google Wallet Overview," Transcript of YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, pp. 1-2.	
	25	"Android 4.0 APIs | Android Developers," mit.edu, https://stuff.mit.edu/afs/sipb/project/android/docs/about/versions/android-4.0.html, 2011, pp. 1-23.	
	26	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3," EMVCo, November 2011, pp. 1-174.	
	27	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-20.	
	28	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, https://www.theguardian.com/technology/2011/sep/19/google-wallet-available-public, September 19, 2011, pp. 1-5.	
	29	PURDY, "How to grab a screenshot from iPhone, Android, and nearly any other smartphone," Computer World, April 20, 2012, pp. 1-6.	
	30	"Maximum failed passcode attempts in restrictions - what happens?," Apple Community, https://discussions.apple.com/thread/3690633, January 2012, pp. 1-3.	
	31	"Simplify, Organize & Pay with Loop by Will Graylin & George Wallner," Kickstarter, March 2019, pp. 1-13.	
	32	"Hands-on with ISIS Mobile Wallet," YouTube, https://www.youtube.com/watch?v=eOMqvGVKjmM, March 10, 2012, page 1.	
	33	"EMV Solutions," Paragon Application Systems, https://web.archive.org/web/20120818221214/http://www.paragonedge.com/solutions/emv-solutions.html, August 18, 2012, page 1.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	SULLIVAN, "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Economic Review, Federal Reserve Bank of Kansas City, Second Quarter 2010, ProQuest Information and Learning, Vol. 95, No. 2, pp 101-133.
	35	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.3," EMVCo, November 2011, pp. 1-189.
	36	"EMV Contactless Specifications for Payment Systems, Book B, Entry Point Specification, Version 2.1," EMVCo, March 2011, pp. 1-50.
	37	ETHERINGTON, "Android Pay Is Real, And Will Give Developers The Reins As An API," TechCrunch, https://techcrunch.com/2015/03/02/android-pay-is-real-and-will-give-developers-the-reins-as-an-api, March 2, 2015, pp. 1-7.
	38	"PCI DSS Version 2.0 Information Supplement: PCI DSS Tokenization Guidelines," PCI Security Standards Council, pcisecuritystandards.org, https://listings.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf., v 2.0, August 2011, pp. 1-23.
	39	"EMVCo Updates Payment Tokenisation Specification to Introduce 'Payment Account Reference,'" www.emvco.com, March 29, 2016, pp. 1-2.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IPR2025-01150
Apple EX1071 Page 1389

UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 02:47:58 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424685	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 44

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_5.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
Paragon_Application_Systems_EMV.pdf	1	Non Patent Literature	159 KB
passcode_attempts.pdf	3	Non Patent Literature	1011 KB
Paying_Google.pdf	2	Non Patent Literature	746 KB
PCI_Compliance.pdf	3	Non Patent Literature	1345 KB
PCI_Compliance_Stress.pdf	12	Non Patent Literature	204 KB

PCI_Tokenization_Guidelines_Info_Supplement.pdf	23	Non Patent Literature	638 KB
Proximity_Sensors.pdf	2	Non Patent Literature	629 KB
REDUCE_PCI.pdf	3	Non Patent Literature	1473 KB
REDUCE_PCI_STRESS.pdf	12	Non Patent Literature	206 KB
screenshot.pdf	6	Non Patent Literature	1897 KB
Android_API.pdf	23	Non Patent Literature	18175 KB
Android_Pay_Is_Real_TechCrunch.pdf	7	Non Patent Literature	5242 KB
B_Entry_Point_Specification_v2_1_March2011.pdf	50	Non Patent Literature	328 KB
CARD_NUMBER.pdf	3	Non Patent Literature	1439 KB
Changing_Nature_of_US_Card_Payment_Fraud_Industry_and_Public_Policy_Options.pdf	33	Non Patent Literature	446 KB
contactless_lacaixa.pdf	2	Non Patent Literature	634 KB
CREDIT_CARD_NUMBER.pdf	8	Non Patent Literature	135 KB
EMV_v4.3_Book_1_ICC_to_Terminal_Interface.pdf	189	Non Patent Literature	1027 KB
EMVCo_Updates_Payment_Tokenisation_Specification.pdf	2	Non Patent Literature	127 KB
Exploring_Google_Wallet.pdf	20	Non Patent Literature	12200 KB

Google_Wallet_Overview.pdf	1	Non Patent Literature	300 KB
Hands_on_with_ISIS_Mobile_Wallet.pdf	1	Non Patent Literature	205 KB
Isis_NFC.pdf	2	Non Patent Literature	753 KB
Isis_SXSW.pdf	3	Non Patent Literature	42 KB
Mobile_World.pdf	3	Non Patent Literature	1511 KB
Mobile_World_Congress.pdf	8	Non Patent Literature	137 KB
New_York_Times.pdf	2	Non Patent Literature	779 KB
Using_Google_Wallet.pdf	2	Non Patent Literature	782 KB
Virtual_terminal.pdf	3	Non Patent Literature	1469 KB
Wallet_mobile_payments.pdf	5	Non Patent Literature	2498 KB
Wallet_Overview.pdf	2	Non Patent Literature	21 KB
What_Google_Wallet.pdf	3	Non Patent Literature	1334 KB
Will_Graylin.pdf	13	Non Patent Literature	4632 KB
Security_Key_Management_1_of_5.pdf	35	Non Patent Literature	12146 KB
Security_Key_Management_2_of_5.pdf	35	Non Patent Literature	14749 KB
Security_Key_Management_3_of_5.pdf	35	Non Patent Literature	17761 KB
Security_Key_Management_4_of_5.pdf	35	Non Patent Literature	17097 KB

Security_Key_Management_5_of_5.pdf	34	Non Patent Literature	16191 KB
Seinfeld.pdf	2	Non Patent Literature	705 KB
Sensilive_Side.pdf	2	Non Patent Literature	655 KB
T_MOBILE.pdf	1	Non Patent Literature	277 KB
Tokenization.pdf	3	Non Patent Literature	1541 KB
Understanding_Proximity_Sensors.pdf	2	Non Patent Literature	291 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_5.pdf	EB152BE38E8F14A1D1022A1EB20CAAB1E1AFA37556F759B0A9584EC443492165FA65C6C54BB3370D61F79B7C133F06B957104961BE509658FD8D89DD8C146F07
Paragon_Application_Systems_EMV.pdf	AF376E74FC80C73DC8BAEE41F09ECE67605F12E71111098FE1770819CD12E6AE7F3D3FAD34743C6B1D626EFFAB87C3E83C80EA79FB0B00327FCD066DE9DC145A
passcode_attempts.pdf	C9E4FC3CF7D261392F9A86402A2431190D534FB0BC622679C3778154B567459FC03B8D1C85FBB7A3996D61706FD5B413DB69508FABF58BFDD6D6823583D7F483
Paying_Google.pdf	601BCF273175710BE405124C4DA9B46C6B0F2DB06F9739012A31A50FD6B05D4B596410C4DDB111CE7617C7DD681149E95F7A88A60366046E77F0EE18BB7B9643
PCI_Compliance.pdf	3B8B4A36EB201D0FCF1C2CD9CB59D580AD571310E765CB535C92F0B3C2F4ABE94B483FD7C4415735C1EE9C019769056E7D63C98F690B40020D21BF09FA89B196

PCI_Compliance_Stress.pdf	0EF6F246F86CB5B7CAF15CAF7932B0ABDD4E150C8E12D5D158D5F5EA31F0DCD8053D77E85F7B02B59D2F7EF8609BFBAE93CB151CBE115E7A4840E3CA00003FE0
PCI_Tokenization_Guidelines_Info_Supplement.pdf	5FE7C5562730405694C5554CCC5F9926E15C0DFF68F6BB882657326C379CC845C2BD4AEE52DB72E8EF2054D1C3147A934C8F9A1477560D5F6CCEBA9F14B30581
Proximity_Sensors.pdf	8A40C7A3B9DCE6F7446FD7BFA67FF5501E9F023312A4BF6A31FC55C5B4D4BA2C31BB8E29A9A7475FB7016DBA680C459EEAB7FA4D24C5089C003836D525002388
REDUCE_PCI.pdf	4C35268DC06DF30510C90BFF65CB19013F131F06A0B13355B36CF3909DFAF67783EC798BBB6067567EB151467D79D26C37240D9A58CC2F6239B924C3AAE3D471
REDUCE_PCI_STRESS.pdf	A556B8E60973E1948D21AA39563968AF4EA5EAC790150BCE437DC0B84E09E6AB49D4A64D1EFBFB1D1B9816B8BF04E0CB89149B084204A68DC2BCCC067F160113
screenshot.pdf	51EFBD790AF43DBEDF9BD006BD9C8C4D5A30F7F8D54074C173C8AB65E59885C3856E71F2ECE9686E85C792D947408DEBA603B7B9DEE9FD463CF4BE9F7840EE4D
Android_API.pdf	D299177B4ED333463CAB066AA0D24F59369B3E220270A6D3875193983396969C84E68671D3E31574AD90AB6921335A9A265935D8DC368AEB2D1A10277A41CDE0
Android_Pay_Is_Real_TechCrunch.pdf	C4F0DDC061BA696B63644BAADAE8FB6143DEB310A308A251662AB19E27A5D6290BFDC5CCE15140336F3A2CD78F4C5A38FD1167F363C69CBDDC3050ADA5600F00
B_Entry_Point_Specification_v2_1_March2011.pdf	7FEEA416D0E066BECAE398697FDD86EF827441D98F6BFA2089D5A42CB022BA6D0A453CE64DF76899FE54DC01DA10A910829F0657C4D987210B68356098C6EF7D
CARD_NUMBER.pdf	71812AF5700B57C1AB25A8FC556E185FBA6A7C1D79F08A4084821B3BFD3AA958A69D4A1030F0565E8DAB842BDD7215F071E0C7D29B7308A8FAEFB9B20874CFC9

Changing_Nature_of_US_Card_Payment_Fraud_Industry_and_Public_Policy_Options.pdf	327509AF153AD3CB176379B5848415B7119BE7D946D01C4B4C71FD7A1DB0FFA12BB6C383A09297C453AB16193A8C2DEEF43618A3D4BCCA2BCB0CCBDC287F1EE
contactless_lacaixa.pdf	E3B844123B8982BB27C07443F3C9021F2F8DD0271B149B18AB4C1F6F2004281DD7C38BC9002E832E836FF11F20FEB7244753A44CA7C947F3069F1E9251A8B278
CREDIT_CARD_NUMBER.pdf	AEA238B431E2F4108021379775865281863 9BF4DFA2D427A12C39615B250E7C463ED4B0F45B2DD2EF94391D6CBC12DAB7B0C644FDF40910B4E4A347188875ECC
EMV_v4.3_Book_1_ICC_to_Terminal_Interface.pdf	1E687B6A1F33CC017C0C90CE52A3F6D23FFA457B3F58380110635FA9F6901D5295DB5870A7BF949983BD920124FB518B86CC0E53BE978BA8839E7EEBDA0CE20F
EMVCo_Updates_Payment_Tokenisation_Specification.pdf	D15DB971C91EEE5A17D8FBB971D1DDDF748A532293769A462048C1035C798DE0050C186BC230531E097A7B198781AEC0F4BC227CA57A8E88A0D9CBA0C089CB82
Exploring_Google_Wallet.pdf	DF6C87563AFAE759ADE235C519F75F41EF468B3C4296C3FD379529107BBE25B28BAD5D776292C15873110DF15660240FA2D5847DBE5E63C3F036CF898FD99AD3
Google_Wallet_Overview.pdf	6410185709EEBDCCB8059DD7640EFC309FB0569B8EC76EA526E3B05F5EB155133D2D499F820C7A4C6FCA1F41B0BE37849D5EA12831775175ECEC92D07A0F4B8C
Hands_on_with_ISIS_Mobile_Wallet.pdf	F415943E01EFB6E850FBBF782B5A5F1EF50C90105D21552F02F5A9A6AEBC742F2BA54F8C4AE936A10524B4278666B11FA9438499B65E494111E352E7F3F835FA
Isis_NFC.pdf	3AC49AD9FDEF91F9B1200F424AFF6861D51FBB616FCD40D9D1745F7CC702A99311F52D95B575C9FB21046963AE18B3ACCAC1AD832822450828EA37AE753F5E97
Isis_SXSW.pdf	868CC0AECD79D60F8ECCC5DD916C9DC1915F9445B683694A63E3DE618C5EFC7FE56EA44FF6B16F2EE52A18A3966E5AAD340F0D7D759F13D6C2FDC6CAC994C19D

Mobile_World.pdf	74C72C18BD46A49569BDC41192294347FDD95BFEDB7923944CB86A1C2B1FDAC51F1D0FDD122221B2DEFAC0A4D3B3A3969D789A3500CA21BF5D98C2818CDFE558
Mobile_World_Congress.pdf	F0C2B759CB7755B651703DD68FB6460021D1D6518006FB887B5E9C0CFE3E4285C04C16CC18215CBE07A87B1F2998E2A08582DD57756BF544154808020597 0B0C
New_York_Times.pdf	72CE5D91AAD01B131EF53C98BBEC955CD2EBD1AF7297C1F595E9AB46BA36AE475011E0C45841BAC6B0F5F09E3FA526F7A39316402ED1D900C88857F0688339AB
Using_Google_Wallet.pdf	8A4A36DEBDE2D6AC68F5FCA96FD931ED22B2C88244AA20F0D83C4A8BB241BBB02E977D2835BC2A263FCF69DBE6E3B8412C74EBE57FA3EF23BAC2F18981163878
Virtual_terminal.pdf	EA989A5B6BC6A95F36CDA7702AED719D7A246F43D5A584695DB2E844A1DDE5D59E62D67C51BB8D7BBE1823C8A553B862B122F903BE689E9EFC581DD07061D084
Wallet_mobile_payments.pdf	5F86AB0325A6918D7A6BD31D32522099DCC56A90BC7BB6F69BC76E5EB668715CE41BB1BA800C92AFBA9D72DB5B90EF19B3217458650BA447917A02A0D18642E0
Wallet_Overview.pdf	5B74F1AD54B320354499D3E23D8A8C71299C630C78F3BA7F1D075900E338F2C4FFDF0D2A767A9D80D5DD9BD38ADC8B40D2A96FD3E9274FC8636E7E0630B7AA1A
What_Google_Wallet.pdf	ACE563AB3E52C0C2AA5F4DA3E9CA63A28734AEDB88E18B8E61672D5CAA7042BEBDCB6C1C5C42A20904610A1FFDAFEDD02F0F3E9B0522E33C4CAE5E4A8063246F
Will_Graylin.pdf	694DBBA98709129E04A695B85CCE8114D8949DAB0FC559A1DBABE15892053B0C85E5DB7B6306291BA2FD8971082ED5956E2CE41124606BB4B18809FDB04A8AB8
Security_Key_Management_1_of_5.pdf	2B5BE6BB0C5FC5C2AC07582D4C3763E66357010D8BE537D2FF1FC44183A9DCDFCDF962DF5EF39F4E59765AEB8CD6DCA6006620E8DE772057EB655EDD24BFC2CD

Security_Key_Management_2_of_5.pdf	1EE397678DB5A81A51358ADAF5FDE8849D93FE2C91FBB713362BFF56BD8AC5AE7799513A45D6E65C111B2D6E9242C121A953D1B3745DFEF1FDBEBC4CBB8AB89F
Security_Key_Management_3_of_5.pdf	A0733EDB9871753DED2B125B7FEC211EBCBFB1F1DB13A80BE5176A40FB40FF3FFDCB421D495D2178CD30B0BCC98BFA7A385B0D0714527B9869A7D40BB741F58E
Security_Key_Management_4_of_5.pdf	73D99B8583AABAC48C73B6FBAC0770B26FACAE3ACB0A60A48490C27C561BFB0968BD65BF18BA03827C9C67F7B336CC52D173E8C0F01F1D50AE59B2541BA63DE4
Security_Key_Management_5_of_5.pdf	BEEF6C4A4E316E20A91B761441763C8745BDB09D148E846E3F3FCCA69B825B9BD7DF8DC0C843142A2491310C610FEAFC024CAD2ADA84CA3AB6CC1086FD7F7C2D
Seinfeld.pdf	9F449A18E85956D7C28BFCD0CA63FDF6C1D4D5A30DA3DED18069FEAB4EA176ADE7D2BEE52924B3D91D5737F645329B5BF9629FC8617146E3FB53C52B4BC7C516
Sensitive_Side.pdf	317C4948BB4B63F43AEF2357780EDCB4233E3C2998F3A2EC2C57B232D4CCB72B89A04C37A873C83E7FDC20BDA6A8385DFD88A7620169D6D7144D38CB69CD8DC2
T_MOBILE.pdf	BB1994F921DD7982A6B3161056B45A3745BB61B535A92DA705DEEAA25D1C23EB61877914B2EBD91130B8BC525CE1D204E8536E7A0EA034EDC35A027658829317
Tokenization.pdf	7AE63B12CEB14F98A85D4139682F2DCCF49DBBC4AFCDE7AB961760D721D0AF4DA50D5FF7FFAD9A5F088D7A1D2B4E260D005E17DC8A9A9A19B8ABD2C0BC302F0D
Understanding_Proximity_Sensors.pdf	2E181A79CCCF26BD11387AE9D3A466722679EA7119AAEF64560195EC48FC5661D9C9A2F8A2E67DDF24F832EE8C62FDFB4A18B3F388371DA0B6DE3CFF312A7FEB

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

Corrected Application Data Sheet

17528073 : MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

~~Strike through~~ indicates removal of data from existing record Underline indicates new data being added to the application If no data is shown, no data has been corrected

Inventor Information

Data of record	Updated Data
No data change in this section	

Application Information

Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	
Attorney Docket Number	~~WYAT-0002.USD1C1C1C1C1C~~	WYAT-0002-13C12US
Entity Status	Small	

Domestic Benefit/National Stage Information

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c), 386(c), or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

	Updated Data

Data of record

No data change in this section

Foreign Priority Information

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the Application Data Sheet constitutes the claim for priority as required by 35 U.S.C. 119 (b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Data of record	Updated Data

No data change in this section

Applicant Information

The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46.

Data of record	Updated Data
CARDWARE, INC ~~---~~ ~~---~~ ~~San Jose, CA 95130~~ UNITED STATES Phone : --- Email : --- Fax : --- Organization Applicant type : Assignee	111 Congress Ave Suite 500 Austin, TX 78701

Assignee Information including Non-Applicant Assignee Information

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Data of record	Updated Data
No data change in this section	

Signature

NOTE:

This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See CFR 1.4(d) for the manner of making signatures and certifications.

Signature	First name	Last name	Registration #	Date
/Jose S. Garcia/	Jose	Garcia	43628	02/09/2023

Doc Code: R46C.REQ
Document Description: Request under 37 CFR 1.46(c) to correct, update or change the applicant.

PTO/AIA/41 (04-15)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST TO CORRECT OR UPDATE THE NAME OF THE APPLICANT UNDER 37 CFR 1.46(c)(1), OR CHANGE THE APPLICANT UNDER 37 CFR 1.46(c)(2)
(FOR USE ONLY IN APPLICATIONS FILED ON OR AFTER SEPTEMBER 16, 2012)

Application Number	17/528,073
Filing Date	11-16-2021
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Practitioner Docket Number	WYAT-0002-13C12US

To: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Applicant hereby **requests that the name of the applicant be corrected or updated under 37 CFR 1.46(c)(1), or that the applicant be changed under 37 CFR 1.46(c)(2),** in the above-identified application. **Requests under 37 CFR 1.46(c)(1) or (c)(2) cannot be submitted after payment of the issue fee or if the application has been patented.**

Please check the applicable box(es) below.

☐ 1. This request is to **correct or update the name of the applicant** (**under 37 CFR 1.46(c)(1)**) and includes:

☐ An application data sheet (ADS) in accordance with 37 CFR 1.76(c) with the corrected or updated information shown with markings (*e.g.*, underlining for insertions, strikethrough for deletions). A Corrected Web-based ADS may be used.

Note: Requests under 37 CFR 1.46(c)(1) may be filed to correct typographical errors in the name of the § 1.46 applicant, or for updating the name of the § 1.46 applicant (*i.e.*, where there is no change in the applicant itself but just in the applicant's name). See the Manual of Patent Examining Procedure (MPEP) section 605.01.

■ 2. This request is to **change the applicant** (**under 37 CFR 1.46(c)(2)**) and includes:

■ An application data sheet (ADS) in accordance with 37 CFR 1.76(c) that identifies the changes with proper markings (underlining for insertions and strikethrough for deletions). A Corrected Web-based ADS may be used.

■ A Statement Under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent). See MPEP 325.

I am the

☐ applicant* ■ attorney or agent of record Registration number 43628 ☐ attorney or agent acting under 37 CFR 1.34 Registration number _____

Signature /Jose S. Garcia/
Typed or printed name Jose S. Garcia
Date 02/09/2023

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. *Juristic entities must be represented by a patent practitioner (See 37 CFR 1.31, applicable to any paper filed on or after September 16, 2012 that is presented on behalf of a juristic entity, regardless of application filing date). Submit multiple forms if more than one signature is required, see below**.

☐ ** Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.36. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**02/09/2023 10:30:58 PM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61576205	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 3

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
CorrectedADS.pdf	3	Application Data Sheet to update/correct info	71 KB
WYAT-0002-13C12US_aia0041_Request_to_Change_Applicant.pdf	2	Request for Corrected Filing Receipt	235 KB
WYAT-0002-13C12US_aia0096_Statement_under_3_73c.pdf	3	Assignee showing of ownership per 37 CFR 3.73	206 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
CorrectedADS.pdf	1A33C7267A8D023270FD6E2B020D686A5E58F264598F8F5E74485D8388015307249FE1B9D933E1F4A18A864CCCFA682C67C20D59C58BDDC8AE90A1E377648660
WYAT-0002-13C12US_aia0041_Request_to_Change_Applicant.pdf	DDA42D25A1D83DD80DF20D7E4B149C92DD0ECA78949770726B66E1E62C74B42A9BB8AFAB8FB65A6FAF5950AFB55D26501FD947FAF166618D74641441540DE717
WYAT-0002-13C12US_aia0096_Statement_under_3_73c.pdf	ECAA0CB00E24AE36313253321C3465010A67EF77A7BA014A633FF497C86088A2F88E3BB6AFBBBD582D7EFF487B6F41777D07628194C5DFAC8E4AC2366FD3C4E3

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: CARDWARE, INC.

Application No./Patent No.: 17/528,073 Filed/Issue Date: 11-16-2021

Titled: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

CARDWARE, INC., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: David WYATT To: CARDWARE, INC.

   The document was recorded in the United States Patent and Trademark Office at

   Reel 058892, Frame 0036, or for which a copy thereof is attached.

2. From: CARDWARE, INC. To: CARDWARE, INC.

   The document was recorded in the United States Patent and Trademark Office at

   Reel 062030, Frame 0299, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Jose S. Garcia/	02/09/2023
Signature	Date
Jose S. Garcia	attorney for CARDWARE, INC.
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2876	3750	WYAT-0002.USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

Date Mailed: 11/17/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

David WYATT, Austin, TX ~~San Jose, CA~~;

Applicant(s)

CARDWARE, INC, San Jose, CA;

Power of Attorney: The patent practitioners associated with Customer Number 136197

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

IPR2025-01150
Apple EX1071 Page 1409

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

IPR2025-01150
Apple EX1071 Page 1410

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01150
Apple EX1071 Page 1412

UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**02/09/2023 11:19:57 PM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61576291	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
CorrectedADS.pdf	3	Application Data Sheet to update/correct info	70 KB
WYAT-0002-13C12US_Filing_Receipt_Correction.pdf	4	Request for Corrected Filing Receipt	223 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
CorrectedADS.pdf	1B1B34F3B58961AC151A192A146DCB79F1A229C64E171B8698

	63815BCF5E35D68BF7CD747614283FF95034DECCF6FB68366387FFA25A515FACF5A877FA45A29F
WYAT-0002-13C12US_Filing_Receipt_Correction.pdf	4889C75A123B8BA21E4F1CBA3970685B1D3408B25CA12FEEDF9F944657CC26C88CFC0A2D3C0D795E5C25AAECE2DD3CE5632070A46296BCDE6BDEA8AA4A515102

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

Corrected Application Data Sheet

17528073 : MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

~~Strike through~~ indicates removal of data from existing record Underline indicates new data being added to the application If no data is shown, no data has been corrected

Inventor Information

Data of record	Updated Data
David WYATT	
Residence Information US Residency San Jose, CA UNITED STATES	
Mailing Address ~~1314 Vanna Ct~~ ~~—~~ ~~San Jose, CA 95131~~ UNITED STATES	**Mailing Address** 1306 Norwalk Ln Apt 303 Austin, TX 78703

Application Information

Title of Invention	**MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE**	
Attorney Docket Number	**WYAT-0002.USD1C1C1C1C1C**	
Entity Status	**~~Small~~**	**Regular Undiscounted**

Domestic Benefit/National Stage Information

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c), 386(c), or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Data of record	Updated Data
No data change in this section	

Foreign Priority Information

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the Application Data Sheet constitutes the claim for priority as required by 35 U.S.C. 119 (b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Data of record	Updated Data
No data change in this section	

Applicant Information

The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46.

Data of record	Updated Data
No data change in this section	

Assignee Information including Non-Applicant Assignee Information

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Data of record	Updated Data
No data change in this section	

Signature

NOTE:

This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See CFR 1.4(d) for the manner of making signatures and certifications.

Signature	First name	Last name	Registration #	Date
/Jose S. Garcia/	Jose	Garcia	43628	02/09/2023

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

CORRECTED ADS FORM

Application Number	17528073
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Inventor Information

****If no data is shown, no data has been corrected****

	Data of Record	Updated Data
Order Number	1	
Name	David WYATT	
Residence Information		
Residency	us-residency	
City	~~San Jose~~	Austin
State	~~CA~~	TX
Country of Residence	US	
Mailing Address of Inventor		
Address 1	~~1314 Vanna Ct~~	1306 Norwalk Ln
Address 2		Apt 303
City,State/Province, Postal Code	~~San Jose CA 95131~~	Austin TX 78703
Country	US	

Corrected ADS 1.0

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

Application Information

	Data of Record	Updated Data
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	
Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C	
Entity Type	Small	

Domestic Benefit/National Stage Information

****If no data is shown, no data has been corrected****

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121,365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S. C. 119(e) or 120, and 37 CFR 1.78(a).

		Data of Record	Updated Data
	Prior Application Status		
	Application Number		
	Continuity Type		
	Prior Application Number		
	Filing Date (YYYY-MM-DD)		
	Patent Number		
	Issue Date (YYYY-MM-DD)		

Foreign Priority Information

IPR2025-01150
Apple EX1071 Page 1419

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

****If no data is shown, no data has been corrected****

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

		Data of Record	Updated Data
	Application Number		
	Country		
	Filing Date		
	Access Code		

Applicant Information

****If no data is shown, no data has been corrected****
Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

	Data of Record	Updated Data
Applicant Type		
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is		
Name of the Deceased or Legally Incapacitated Inventor		
Applicant is an Organization		
Name		
Organization Name		
Address 1		
Address 2		

Corrected ADS 1.0

City,State/Province,Postal Code		
Country		
Phone Number		
Fax Number		
Email Address		

Assignee Information including Non-Applicant Assignee Information

****If no data is shown, no data has been corrected****
Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office

	Data of Record	Updated Data
Order		
Applicant is an Organization		
Name		
Organization Name		
Mailing Address		
Address 1		
Address 2		
City,State/Province,Postal Code		
Country		
Phone Number		
Fax Number		
Email Address		

IPR2025-01150
Apple EX1071 Page 1421

Signature

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Jose S. Garcia/	Registration Number	43628
First Name	Jose	Last Name	Garcia

IPR2025-01150
Apple EX1071 Page 1422

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2876	3750	WYAT-0002.USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

Date Mailed: 11/17/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Austin, TX
David WYATT, ~~San Jose, CA~~;

Applicant(s)

CARDWARE, INC, San Jose, CA;

Power of Attorney: The patent practitioners associated with Customer Number 136197

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

IPR2025-01150
Apple EX1071 Page 1423

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

IPR2025-01150
Apple EX1071 Page 1424

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01150
Apple EX1071 Page 1426

Electronic Acknowledgement Receipt	
EFS ID:	47512106
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Jose S. Garcia
Filer Authorized By:	
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Receipt Date:	10-FEB-2023
Filing Date:	16-NOV-2021
Time Stamp:	00:42:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet to update/ correct info	CorrectedADS.pdf	102555 87a8012224df8c08385be2eddb0830e64a3b53bd	no	5

Warnings:

Information:					
2	Request for Corrected Filing Receipt	WYAT-0002-13C12US_Filing_Receipt_Correction.pdf	227895 35b0059b8c0e1e5d2d8c0318ee672669d4e8e09d	no	4
Warnings:					
Information:					
			Total Files Size (in bytes):	330450	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

136197 7590 02/13/2023

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

EXAMINER
LEE, SEUNG H

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 02/13/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	05/15/2023

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PTOL-85 (Rev. 02/11)

IPR2025-01150
Apple EX1071 Page 1429

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

136197 7590 02/13/2023
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	05/15/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEE, SEUNG H	2876	235-380000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required) ❑Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

IPR2025-01150
Apple EX1071 Page 1430

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

136197 7590 02/13/2023

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

EXAMINER	
LEE, SEUNG H	

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 02/13/2023

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

IPR2025-01150
Apple EX1071 Page 1431

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 17/528,073	Applicant(s) WYATT, David	
	Examiner SEUNG H LEE	Art Unit 2876	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 1/12/2023.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 15-86 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 6 IDSs filed on 1/12/2023.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/SEUNG H LEE/
Primary Examiner, Art Unit 2876

IPR2025-01150
Apple EX1071 Page 1433

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 12, 2023 has been entered.

Allowable Subject Matter

3. Claims 15-86 are allowed.

4. The following is an examiner's statement of reasons for allowance:

None of prior art teaches a method of generating and using limited-use payment information for performing a payment transaction, the method comprising: receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises: a processor; a touch-screen display coupled to the processor; and a near field communications (NFC) interface coupled to the processor; responsive to said priming operation, readying said device to perform a payment transaction by an identified user; receiving a payment request for the payment transaction at said electronic device; displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected

issued payment account; dynamically generating, by the processor, limited-use payment information; wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device; using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account; transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient.; responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display, and a system of the same as set forth in the claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SEUNG H LEE whose telephone number is (571)272-2401. The examiner can normally be reached 7-4:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an

interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steven Paik can be reached on 571-272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SEUNG H LEE/
Primary Examiner, Art Unit 2876

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	11/05/2022	01/28/2023							
1	15	=	=							
2	16	=	=							
7	17	=	=							
8	18	=	=							
9	19	=	=							
10	20	=	=							
11	21	=	=							
12	22	=	=							
13	23	=	=							
14	24	=	=							
15	25	=	=							
16	26	=	=							
17	27	=	=							
23	28	=	=							
24	29	=	=							
25	30	=	=							
26	31	=	=							
3	32	=	=							
18	33	=	=							
4	34	=	=							
27	35	=	=							
28	36	=	=							
21	37	=	=							
22	38	=	=							
5	39	=	=							
6	40	=	=							
19	41	=	=							
20	42	=	=							
29	43	=	=							
30	44	=	=							
31	45	=	=							
32	46	=	=							
33	47	=	=							
34	48	=	=							
35	49	=	=							
36	50	=	=							
38	51	=	=							
37	52	=	=							
39	53	=	=							
40	54	=	=							
41	55	=	=							
44	56	=	=							

IPR2025-01150
Apple EX1071 Page 1437

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

CLAIM		DATE								
Final	Original	11/05/2022	01/28/2023							
42	57	=	=							
43	58	=	=							
45	59	=	=							
46	60	=	=							
47	61	=	=							
48	62	=	=							
49	63	=	=							
50	64	=	=							
51	65	=	=							
52	66	=	=							
53	67	=	=							
54	68	=	=							
55	69	=	=							
56	70	=	=							
57	71	=	=							
60	72	=	=							
61	73	=	=							
58	74	=	=							
59	75	=	=							
62	76	=	=							
63	77	=	=							
64	78	=	=							
65	79	=	=							
66	80	=	=							
67	81	=	=							
68	82	=	=							
69	83	=	=							
70	84	=	=							
71	85	=	=							
72	86	=	=							

IPR2025-01150
Apple EX1071 Page 1438

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

CPC - Searched*		
Symbol	Date	Examiner
G06Q20/341 or G06K19/06206 or G06K19/0716 or G06K19/07749 or G06Q20/06 or G06Q20/065 or G06Q20/223 or G06Q20/24 or G06Q20/346 or G06Q20/347 or G06Q20/352 or G06Q20/3827 or G06Q20/385 or G06Q20/4012 or G06Q20/409 or G07F7/0873 or G07F19/00	01/28/2023	sl

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
PE2E	01/28/2023	sl
14/680979,14/981757,15/701261,16/459150, 17/075637 (parent cases)	01/28/2023	sl
NPL	11/05/2022	sl

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	same as above	01/28/2023	sl

IPR2025-01150
Apple EX1071 Page 1439

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

IPR2025-01150
Apple EX1071 Page 1440

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

CPC						
Symbol					Type	Version
G06Q	/	20	/	341	F	2013-01-01
G07F	/	19	/	00	I	2013-01-01
G06Q	/	20	/	06	I	2013-01-01
G06Q	/	20	/	223	I	2013-01-01
G06Q	/	20	/	347	I	2013-01-01
G06Q	/	20	/	385	I	2013-01-01
G07F	/	7	/	0873	I	2013-01-01
G06K	/	19	/	06206	I	2013-01-01
G06K	/	19	/	0716	I	2013-01-01
G06K	/	19	/	07749	I	2013-01-01
G06Q	/	20	/	24	I	2013-01-01
G06Q	/	20	/	352	I	2013-01-01
G06Q	/	20	/	409	I	2013-01-01
G06Q	/	20	/	065	I	2013-01-01
G06Q	/	20	/	346	I	2013-01-01
G06Q	/	20	/	3827	I	2013-01-01
G06Q	/	20	/	4012	I	2013-01-01

CPC Combination Sets							
Symbol					Type	Set	Ranking	Version
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	28 January 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20230126

IPR2025-01150
Apple EX1071 Page 1441

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06Q20/34	/	20	/	34

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	28 January 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20230126

IPR2025-01150
Apple EX1071 Page 1442

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	15	14	24	18	33	20	42	38	51	46	60	55	69	64	78
2	16	15	25	4	34	29	43	37	52	47	61	56	70	65	79
7	17	16	26	27	35	30	44	39	53	48	62	57	71	66	80
8	18	17	27	28	36	31	45	40	54	49	63	60	72	67	81
9	19	23	28	21	37	32	46	41	55	50	64	61	73	68	82
10	20	24	29	22	38	33	47	44	56	51	65	58	74	69	83
11	21	25	30	5	39	34	48	42	57	52	66	59	75	70	84
12	22	26	31	6	40	35	49	43	58	53	67	62	76	71	85
13	23	3	32	19	41	36	50	45	59	54	68	63	77	72	86

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	28 January 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20230126

IPR2025-01150
Apple EX1071 Page 1443

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Isis NFC-payment from SXSW 2012," YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 2.	
	2	"Isis NFC-payment from SXSW 2012," Transcript of YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 3.	
	3	"NFC - Google Wallet and More - EE Times - Mobile World Congress," YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-3.	
	4	"NFC - Google Wallet and More - EE Times - Mobile World Congress," Transcript of YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-8.	
	5	"Paying With Google Wallet," YouTube, https://www.youtube.com/watch?v=jTeilSlzBPQ, February 6, 2012, pp. 1-2.	
	6	"Seinfeld - Google Wallet," YouTube, https://www.youtube.com/watch?v=baaCvgTRYsU, June 14, 2013, pp. 1-2.	
	7	"Technology: Google Wallet - The New York Times," YouTube, https://www.youtube.com/watch?v=l8JOT6ban7o, September 23, 2011, pp. 1-2.	
	8	"Using Google Wallet in McDonald's!," YouTube, https://www.youtube.com/watch?v= 1p6co4YIvbA, September 14, 2012, pp. 1-2.	
	9	"Virtual terminal- #1 storing credit card data with tokenization," YouTube, https://www.youtube.com/watch?v=eSXIlGbACew, February 28, 2011, pp. 1-3.	
	10	"What is Google Wallet?," YouTube, https://www.youtube.com/watch?v=iuvyN4iZiP8, August 9, 2011, pp. 1-3.	
	11	"What is Tokenization?," YouTube, https://www.youtube.com/watch?v=ypm5FFfEN34, January 17, 2011, pp. 1-3.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul 28, 2009, pp. 1-3.	
	13	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul 28, 2009, pp. 1-12.	
	14	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-3.	
	15	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-12.	
	16	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-3.	
	17	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-8.	
	18	"Caixer contactless lacaixa," YouTube, https://www.youtube.com/watch?v=It2CpMcxQC4, April 4, 2011, pp. 1-2.	
	19	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	20	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, page 1.	
	21	"Understanding Proximity Sensors - T-Mobile," Transcript of YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	22	"Google I/O 2012 - The Sensitive Side of Android," YouTube, https://www.youtube.com/watch?v=Q0V_Id7iNw4, June 29, 2012, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Google Wallet Overview," YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, page 1.	
	24	"Google Wallet Overview," Transcript of YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, pp. 1-2.	
	25	"Android 4.0 APIs | Android Developers," mit.edu, https://stuff.mit.edu/afs/sipb/project/android/docs/about/versions/android-4.0.html, 2011, pp. 1-23.	
	26	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3," EMVCo, November 2011, pp. 1-174.	
	27	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-20.	
	28	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, https://www.theguardian.com/technology/2011/sep/19/google-wallet-available-public, September 19, 2011, pp. 1-5.	
	29	PURDY, "How to grab a screenshot from iPhone, Android, and nearly any other smartphone," Computer World, April 20, 2012, pp. 1-6.	
	30	"Maximum failed passcode attempts in restrictions - what happens?," Apple Community, https://discussions.apple.com/thread/3690633, January 2012, pp. 1-3.	
	31	"Simplify, Organize & Pay with Loop by Will Graylin & George Wallner," Kickstarter, March 2019, pp. 1-13.	
	32	"Hands-on with ISIS Mobile Wallet," YouTube, https://www.youtube.com/watch?v=eOMqvGVKjmM, March 10, 2012, page 1.	
	33	"EMV Solutions," Paragon Application Systems, https://web.archive.org/web/20120818221214/http://www.paragonedge.com/solutions/emv-solutions.html, August 18, 2012, page 1.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	SULLIVAN, "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Economic Review, Federal Reserve Bank of Kansas City, Second Quarter 2010, ProQuest Information and Learning, Vol. 95, No. 2, pp 101-133.
	35	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.3," EMVCo, November 2011, pp. 1-189.
	36	"EMV Contactless Specifications for Payment Systems, Book B, Entry Point Specification, Version 2.1," EMVCo, March 2011, pp. 1-50.
	37	ETHERINGTON, "Android Pay Is Real, And Will Give Developers The Reins As An API," TechCrunch, https://techcrunch.com/2015/03/02/android-pay-is-real-and-will-give-developers-the-reins-as-an-api, March 2, 2015, pp. 1-7.
	38	"PCI DSS Version 2.0 Information Supplement: PCI DSS Tokenization Guidelines," PCI Security Standards Council, pcisecuritystandards.org, https://listings.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf., v 2.0, August 2011, pp. 1-23.
	39	"EMVCo Updates Payment Tokenisation Specification to Introduce 'Payment Account Reference,'" www.emvco.com, March 29, 2016, pp. 1-2.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

IPR2025-01150
Apple EX1071 Page 1450

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"EMVCO Publishes Technical Framework for its Payment Tokenisation Specification," EMVCO, March 11, 2014, pp. 1-2.	
	2	"Encryption and Tokenization: Which is best for your business?," Townsend Security, 2010, pp. 1-4.	
	3	MOLEN, "Engadget Primed: What is NFC, and why do we care?," Engadget, June 10, 2011, pp. 1-11.	
	4	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-11.	
	5	"Financial Cryptography," 5th International Conference, FC 2001 Proceedings, Grand Cayman, British West Indies, February 19-22, 2001, Paul F. Syverson (Editor), pp. 1-57.	
	6	"Gemalto to Provide Isis Mobile Commerce Platform with Trusted Service Manager (TSM) Solution," Business Wire, December 12, 2011, pp. 1-3.	
	7	"Google Checkout checks out, replaced by Google Wallet," Android Community, November 17, 2011, page 1.	
	8	"Google Checkout HTML API Short Attribute Reference," Google Checkout, Google Code (archive.org), March 27, 2012, pp. 1-4.	
	9	"Google Commerce: Building one wallet: Google Checkout is transitioning to Google Wallet," commerce.googleblog.com, November 16, 2011, pp. 1-2.	
	10	"Google Prepaid Cards," Wallet Help, Google (archive.org), October 3, 2012, page 1.	
	11	CLARK, "Google Unveils first Android NFC phone - but Nexus S is limited to tag reading only for now," NFC World, December 7, 2010, pp. 1-4.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Google Wallet launches officially on Nexus S 4G," Android Community, September 19, 2011, pp. 1-2.	
	13	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, September 19, 2011, page 1.	
	14	BOULTON, "Google Wallet Mobile Payments Coming to New York, Francisco; Google Wallet will launch this summer to enable consumers to pay for goods by tapping their Samsung Nexus 2 4G Android phones at NFC-fitted sales terminals at Subway, Macy's and other retailers," eWeek.com, May 26, 2011, pp. 1-2.	
	15	FINGAS, "Google Wallet reaches the web, reminds most of us that it exists," Engadget, October 4, 2012, pp. 1-6.	
	16	RAPHAEL, "Google's Eric Schmidt spills clues about Android Gingerbread," ComputerWorld, November 15, 2010, pp. 1-3.	
	17	"Handset makers line up behind Isis NFC payment platform," Old GigaOm, September 27, 2011, pp. 1-2.	
	18	"How it Works," Wallet Help, Google (archive.org), March 12, 2013, page 1.	
	19	"How to find out IMEI number on Google Nexus S phone," Tech Notes Desk, January 10, 2013, page 1.	
	20	"La Caixa," Annual Report, 2010, Barcelona, Spain, pp. 1-190.	
	21	"INSIDE Contactless to Equip KTFMobile Payment Project Mobile Phones; Korean Manufacturer Confirms INSIDE's NFC Maturity by Embedding MicroRead into LG Electronics and Samsung Electronics Mobile Phones for its Mobile Payment Project," Business Wire, July 16, 2007, pp. 1-2.	
	22	CLUCKEY, "Is a contactless ATM inevitable? Bank of America seems to think so; the FI has filed a patent application for a 'Contactless Automated Teller Machine,'" ATM Marketplace, September 20, 2012, pp. 1-3.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Isis™ Launches in Austin and Salt Lake City; As Many as 20 Isis Ready™ Handsets to Be Available by Year End," Business Wire, October 22, 2012, page 1.	
	24	PEREZ, "Isis Revealed: Carrier-Led Mobile Payments Venture Shows Off Its New App, Announces Banking Partners," TechCrunch, February 27, 2012, pp. 1-6.	
	25	SADEWO, "Isis to officially launch on Oct 22, more supported devices announced," androidauthority.com, October 18, 2012, pp. 1-2.	
	26	"MasterCard Approves NFC Phones from HTC, Intel, LG Electronics, Nokia, RIM, Samsung Electronics and Sony," Professional Services Close-Up, May 10, 2012, Close-Up Media, Inc., pp. 1-2.	
	27	"MASTERCARD INC, FORM 10-K (Annual Report)," Filed February 28, 2007, for the Period Ending December 31, 2006, pp. 1-204.	
	28	"MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer," Global Hub, Engagement Bureau, Press Release, October 1, 2013, pp. 1-2.	
	29	"Fact Sheet: Mobile Commerce: A New Way to Pay: MasterCard Mobile Commerce," May 26, 2011, pp. 1-4.	
	30	"McDonald's testing e-payment system," USA Today, May 29, 2001, pp. 1-3.	
	31	"Mobile Contactless Payments Trialled Live at Mobile World Congress 2010; GSMA, Samsung, Telefónica and Visa, with Giesecke & Devrient, Ingenico, ITN International and La Caixa, collaborate across industries to give Congress attendees an opportunity to experience NFC," Business Wire, February 15, 2010, pp. 1-3.	
	32	"Mobile Payment Bringing value to payments on mobile," Gemalto, November 2011, pp. 1-4.	
	33	WOO, "Mobile PayPass Meets Cloud in Google Wallet," Global Hub, August 1, 2012, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	HEUN, "Mobile Wallet Consortium Strives Cautiously In 2012; The telco joint effort proceeded more slowly than expected, but its leaders maintain that the mobile wallet business is big enough for lots of players," Section: MOBILE: ISIS, January 1, 2013, Page 47, Vol. 2, No. 1, SouceMedia LLC d/b/a Arizent, pp. 1-3.
	35	BELL, "Mobile's Gains Prompt More Banks To Move Beyond Cards For ATM Access," Payments Source, Section: DEBIT: Vol. 1, No. 1, May 12, 2011, pp. 1-4.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Standing Document (SD1): WG8 Projects: ISO/IEC 14443, Proximity Cards (PICCS)," ISO/IEC JTC1/SC17/WG8 (archive.org), October 25, 2010, pp. 1-6.	
	2	"Telefonica O2 Czech Republic prepares NFC payments," DmEurope, March 25, 2011, page 1.	
	3	MARKKANEN, "Telefonica, Samsung to Pilot SIM-Based NFC Payment Solution in Spain," IHS Global Insight, February 15, 2010, pp. 1-2.	
	4	"The Mobile Payments and NFC Landscape: A U.S. Perspective," Smart Card Alliance, September 2011, pp. 1-53.	
	5	"Tokenization Guidance: How to reduce PCI compliance costs, Version 1.0," Securosis, December 10, 2011, pp. 1-31.	
	6	"Tokenization: What's Next After PCI," RSA, 2012, pp. 1-8.	
	7	SEIFERT, "Verizon won't offer Google Wallet for the Galaxy Nexus because it uses a 'secure element'," The Verge, December 10, 2012, pp. 1-2.	
	8	"Visa and Google Sign Licensing Deal to Boost Mobile Payment Adoption," Visa, September 19, 2011, pp. 1-2.	
	9	"Visa Best Practices for Tokenization Version 1.0," Visa, July 14, 2010, pp. 1-4.	
	10	CROSMAN, "Visa Certifies BlackBerry, Samsung And LG Phones For PayWave NFC Payments," Payments Source, January 10, 2012, pp. 1-2.	
	11	"Visa Completes Acquisition of Rambus Payments Portfolio," Business Wire, October 22, 2019, page 1.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Convenience for customers. Profits for you," Visa PayWave (archive.org), January 2013, pp. 1-2.	
	13	"Verizon User Manual: Samsung Galaxy SIII," Verizon, January 2012, pp. 1-204.	
	14	"World leader in proven and efficient cards for EMV deployment," Gemalto, February 2010, pp. 1-2.	
	15	BECKER, "29C3: A Rambling Walk Through an EMV Transaction (EN)," YouTube, https://www.youtube.com/watch?v=VdNm9JJmCzg, December 30, 2012, pp. 1-2.	
	16	"ARQC and ARPC Generation and Validation," YouTube, https://www.youtube.com/watch?v=I1XTn175FFk, Paragon Application Systems, July 25, 2012, pp. 1-3.	
	17	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	18	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	19	"Credit Card Processing with EPX BuyerWall Tokenization," YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-3.	
	20	"Credit Card Processing with EPX BuyerWall Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-7.	
	21	"Find out how PayPal works," YouTube, https://www.youtube.com/watch?v=dn42Y-2uFQM, March 14, 2012, pp. 1-2.	
	22	"Google checkout," YouTube, https://www.youtube.com/watch?v=-UeYkxePW2c, June 29, 2006, pp. 1-2.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"See Google I/O 2011: Google Checkout: A Foundation For Payments," YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-2.	
	24	"See Google I/O 2011: Google Checkout: A Foundation For Payments," Transcript of YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-64.	
	25	"Google I/O 2011: How to NFC," YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-2.	
	26	"Google I/O 2011: How to NFC," Transcript of YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-62.	
	27	"Google I/O 2012: Introducing Google Wallet Cloud APIs," YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-3.	
	28	"Google I/O 2012: Introducing Google Wallet Cloud APIs," Transcript of YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-40.	
	29	"Google Nexus S by Samsung at CES 2011," YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	30	"Google Nexus S by Samsung at CES 2011," Transcript of YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	31	"Google Payments Live - Google Wallet updates," YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-2.	
	32	"Google Payments Live - Google Wallet updates," Transcript of YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-40.	
	33	"Google Wallet Demonstration," YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Google Wallet Demonstration," Transcript of YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	
	35	"Google Wallet Hands-On - Engadget," YouTube, https://www.youtube.com/watch?v=5s9wYEkRAgs, May 26, 2011, pp. 1-3.	
	36	"Google Wallet - How to Setup and Use this Exciting NFC Technology," YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-3.	
	37	"Google Wallet - How to Setup and Use this Exciting NFC Technology," Transcript of YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-7.	
	38	"Google Wallet Make Your Phone Your Wallet by Google," YouTube, https://www.youtube.com/watch?v=qRVQTQlJV0g, February 18, 2013, pp. 1-2.	
	39	"Google Wallet Make Your Phone Your Wallet by Google," Transcript of YouTube, https://www.youtube.com/watch?v=qRVQTQlJV0g, February 18, 2013, page 1.	
	40	"Google Wallet Product Launch," YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-3.	
	41	"Google Wallet Product Launch," Transcript of YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-56.	
	42	"Google Wallet Walkthrough," YouTube, https://www.youtube.com/watch?v=xmbRSXYdFFs, February 13, 2012, pp. 1-2.	
	43	"How does Google Wallet work? Really well!," YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	
	44	"How does Google Wallet work? Really well!," Transcript of YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	45	"How Does PayPal Work?," YouTube, https://www.youtube.com/watch?v=MdrPOCCFQ2k, July 24, 2012, pp. 1-2.	
	46	"How To Use Google Wallet On Android," YouTube, https://www.youtube.com/watch?v=6DeiEVBIBcs, October 28, 2011, pp. 1-2.	
	47	"How To Use Google Wallet On Verizon Galaxy Nexus - Pocketnow," YouTube, https://www.youtube.com/watch?v=AZ8t757ZfUs, April 20, 2012, pp. 1-2.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	30843	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/04/27 12:21 PM
L2	1	nfc same transaction same payment same logo same limited same issuer	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/04/27 12:22 PM
L4	311	monitor$4 same master same node same wireless same sensor	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:55 PM
L5	18	L4.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:55 PM
L6	107	L4 same (slave peripheral)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:56 PM
L7	7	L6.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:56 PM
L8	17	("20030018927"|"9860688"|"20180165568"|"20150154531"|"9189226"|"20100082870"|"20170039666"|"20180046964"|"9824329"|"20080239282"|"9182231"|"20130107770"|"20070049291"|"6614392"|"20100299401"|"20160233927").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:58 PM
L9	9	L6 same (environment$4 temperature)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 01:00 PM
L10	9	("20130250357"|"20150324745"|"7177054"|"8292173"|"7048194"|"7299990"|"7540603"|"8072620"|"20100096181").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 01:04 PM

IPR2025-01150
Apple EX1071 Page 1466

L11	39	("2015/0324745").URPN.	(USPAT)	OR	OFF	OFF	2020/05/02 08:57 AM
L12	35	label same wireless same master same (slave peripheral)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/02 09:00 AM
L13	39	"517508"	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/02 09:19 AM
L14	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:07 AM
L15	55	nfc same transaction same payment same limited same issuer	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:07 AM
L16	5	L15 same proximity	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:08 AM
L17	30909	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:24 AM
L18	129	L17 and (nfc same select$4 same payment same limit$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:25 AM
L19	43	L17 and (nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:26 AM
L20	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L21	0	L20 and (nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L22	109	(nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L23	94	L22 same (mobile portable)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:34 AM
L24	4186	dynamic same credit	(US-PGPUB; USPAT;	OR	OFF	OFF	2020/05/05

IPR2025-01150
Apple EX1071 Page 1467

		same card	EPO; JPO)				08:35 AM
L25	7	L22 and L24	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:35 AM
L26	23	("20020073025" | "20030101137" | "20070278290" | "20100057553" | "20100082487" | "20110137748" | "20110302089" | "20120006891" | "20140052607" | "20140129422" | "20140143037" | "20140195324" | "20140249941" | "20140279474" | "20150058145" | "20160027005" | "20160086161" | "20160162857" | "20160162887" | "20160335619" | "6633223" | "9292849" | "9489671").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2020/05/05 08:38 AM
L27	6	("20040168067" | "20090276347" | "20110016047" | "20120173311" | "20130159186" | "6163771").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2020/05/05 08:39 AM
L28	4	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2020/05/05 09:39 AM
L29	1	L28 and (respons$4 same nfc same generat$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 09:40 AM
L30	31288	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:19 PM
L31	135	L30 and (nfc same	(US-PGPUB; USPAT;	OR	OFF	OFF	2020/06/21

IPR2025-01150
Apple EX1071 Page 1468

		select$4 same payment same limit$4)	EPO; JPO)				02:19 PM
L32	112	L30 and (nfc same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:20 PM
L33	7	L30 and (nfc same payment same limit$4 same approv$4 same interface)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:20 PM
L34	10	L30 and (nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:28 PM
L35	36	(nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:29 PM
L36	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:30 PM
L37	51	"075637"	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/28 10:02 PM
L38	1	"10810579".pn.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/28 10:03 PM
L39	35569	(G06Q20/341 or G06K19/07749 or G06Q20/347 or G06Q20/06 or G06Q20/409 or G06Q20/4012 or G06Q20/346 or G06Q20/3827 or G06K19/0716 or G07F19/00 or G06Q20/223 or G06Q20/24 or G06Q20/385 or G07F7/0873 or G06K19/06206 or G06Q20/065 or G06Q20/352).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:36 AM
L40	6275	payment same transaction same (limit$4 tempora$6) same generat$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:39 AM
L41	1592	L39 and L40	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:39 AM
L42	862	L40 same issuer same account	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:40 AM
L43	265	L39 and L42	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:40 AM
L44	30	L42 same wireless$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:42 AM

L45	2	("8851370"|"9646301").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:07 AM
L46	31	("10013693" | "20060032908" | "20080223937" | "20100260388" | "20110140841" | "20130048712" | "20130124292" | "20130297509" | "20140052632" | "20140279555" | "20180240106" | "6631849" | "6641050" | "7128274" | "7202825" | "7360688" | "7784692" | "7793851" | "7841539" | "8577813" | "8639629" | "8702007" | "8768838" | "8856539" | "9022286" | "9100826" | "9224083" | "9430765" | "9530137" | "9536238" | "9760884").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2021/09/29 07:08 AM
L47	229	("7128274").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:16 AM
L48	369	("7793851").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:22 AM
L49	77	L40 and L48	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:22 AM
L50	47	L39 and L49	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:22 AM
L51	130	("2013/0159186").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:36 AM
L52	41	(nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L53	1218	(select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L54	267	L39 and L53	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L55	346	L53 same generat$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:49 AM
L56	2785621	L55 sane dynamic$6	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:49 AM
L57	48	L55 same dynamic$6	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:50 AM
L58	11	L55 same static$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:51 AM
L59	543	("10043164" | "10075437" | "10129648" |	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2021/09/29 08:20 AM

IPR2025-01150
Apple EX1071 Page 1470

		"10133979" | "10217105" | "20010010723" | "20010029485" | "20010034702" | "20010054003" | "20020078345" | "20020093530" | "20020100808" | "20020120583" | "20020152116" | "20020153424" | "20020165827" | "20030023554" | "20030034873" | "20030055727" | "20030078882" | "20030167350" | "20030208449" | "20040015958" | "20040039919" | "20040127256" | "20040215674" | "20040230799" | "20050044367" | "20050075985" | "20050081038" | "20050138387" | "20050156026" | "20050160049" | "20050195975" | "20050247797" | "20060006230" | "20060040726" | "20060041402" | "20060044153" | "20060047954" | "20060085848" | "20060136334" | "20060173985" | "20060174331" | "20060242698" | "20060280338" | "20070033642" | "20070055630" | "20070061266" | "20070061487" | "20070116292" | "20070118745" | "20070197261" | "20070224969" | "20070241182" | "20070256134" | "20070258594" | "20070278291" | "20080008315" | "20080011831" | "20080014867" |				

IPR2025-01150
Apple EX1071 Page 1471

		"20080035738" | "20080071681" | "20080072303" | "20080086767" | "20080103968" | "20080109309" | "20080110983" | "20080120711" | "20080156873" | "20080162312" | "20080164308" | "20080207307" | "20080209543" | "20080223918" | "20080285746" | "20080308641" | "20090048026" | "20090132417" | "20090143104" | "20090171682" | "20090210308" | "20090235339" | "20090249077" | "20090282264" | "20100023449" | "20100023455" | "20100029202" | "20100030549" | "20100033310" | "20100036769" | "20100078471" | "20100082491" | "20100094754").PN. OR ("20100095130" | "20100100480" | "20100114731" | "20100192230" | "20100207742" | "20100211797" | "20100240413" | "20100257357" | "20100312634" | "20100312635" | "20110035604" | "20110060631" | "20110084132" | "20110101093" | "20110113245" | "20110125638" | "20110131415" | "20110153437" | "20110153496" | "20110208658" | "20110208965" | "20110211219" | "20110218911" | "20110238564" | "20110246780"					

		"20110258452" | "20110280406" | "20110282785" | "20110294418" | "20110312271" | "20120009946" | "20120024947" | "20120030047" | "20120030121" | "20120047071" | "20120079281" | "20120109735" | "20120143754" | "20120150737" | "20120178366" | "20120196583" | "20120207305" | "20120209773" | "20120238206" | "20120239560" | "20120252350" | "20120254394" | "20120284194" | "20120290472" | "20120296818" | "20120316992" | "20120317035" | "20120317628" | "20130005245" | "20130008956" | "20130026229" | "20130054474" | "20130065564" | "20130080228" | "20130080229" | "20130099587" | "20130104251" | "20130106576" | "20130119130" | "20130130614" | "20130144793" | "20130171929" | "20130179351" | "20130185772" | "20130191279" | "20130200999" | "20130216108" | "20130226791" | "20130226796" | "20130232082" | "20130238894" | "20130282360" | "20130303085" | "20130304651" | "20130312082" | "20130314593" | "20130344857" | "20140002238"				

		"20140019352" | "20140027506" | "20140032409" | "20140032410" | "20140040120" | "20140040139" | "20140040147" | "20140047235" | "20140067690" | "20140074637").PN. OR ("20140074655" | "20140081720" | "20140095227" | "20140138435" | "20140171034" | "20140171039" | "20140172700" | "20140180851" | "20140208112" | "20140214674" | "20140229375" | "20140245391" | "20140256251" | "20140258099" | "20140258113" | "20140258125" | "20140274179" | "20140279479" | "20140337235" | "20140339315" | "20140346860" | "20140365780" | "20140379361" | "20150012444" | "20150032635" | "20150071486" | "20150088757" | "20150089586" | "20150134452" | "20150140960" | "20150154595" | "20150170138" | "20150178724" | "20150186871" | "20150205379" | "20150235211" | "20150302409" | "20150317626" | "20150332266" | "20150339474" | "20150371234" | "20160012465" | "20160026997" | "20160048913" | "20160055480" | "20160057619" | "20160065370" | "20160087957"					

		"20160092696" | "20160148193" | "20160232523" | "20160239672" | "20160253651" | "20160255072" | "20160267486" | "20160277383" | "20160277388" | "20160307187" | "20160307189" | "20160314472" | "20160330027" | "20160335531" | "20160379217" | "20170004502" | "20170011395" | "20170011406" | "20170017957" | "20170017964" | "20170024716" | "20170039566" | "20170041759" | "20170068950" | "20170103388" | "20170104739" | "20170109509" | "20170109730" | "20170116447" | "20170124568" | "20170140379" | "20170154328" | "20170154333" | "20170180134" | "20170221047" | "20170230189" | "20170237301" | "20170289127" | "20170295013" | "20170316696" | "20170317834" | "20170330173" | "20170374070" | "20180034507" | "20180039986").PN. OR ("20180068316" | "20180129945" | "20180160255" | "20180191501" | "20180205712" | "20180240106" | "20180254909" | "20180268132" | "20180270214" | "20180294959" | "20180300716" | "20180302396" | "20180315050"					

		"20180316666" | "20180322486" | "20180359100" | "20190014107" | "20190019375" | "20190036678" | "20190238517" | "4683553"	"4827113" | "4910773"	"5036461" | "5363448"	"5377270" | "5533126"	"5592553" | "5616901"	"5666415" | "5764789"	"5768373" | "5778072"	"5796827" | "5832090"	"5883810" | "5901874"	"5929413" | "5960411"	"6021203" | "6049328"	"6058373" | "6061666"	"6105013" | "6199114"	"6199762" | "6216227"	"6227447" | "6282522"	"6324271" | "6342844"	"6367011" | "6402028"	"6438550" | "6501847"	"6631197" | "6641050"	"6655585" | "6662020"	"6721706" | "6731778"	"6779115" | "6792533"	"6829711" | "6834271"	"6834795" | "6852031"	"6865547" | "6873260"	"6877656" | "6889198"	"6905411" | "6910627"	"6971031" | "6990588"	"7006986" | "7085931"	"7127605" | "7128274"	"7140550" | "7152045"	"7165727" | "7175076"	"7202773" | "7206806"	"7232073" | "7246752"	"7254569" | "7263507"	"7270276" | "7278025"	"7287692" | "7290709"	"7306143" | "7319986"	"7325132" | "7373515"	"7374099" | "7375616"	"7380710" | "7424977"	"7453439" | "7472829"	"7487357" | "7568631"	"7584153" | "7597250"	"7628322" | "7652578"	"7689832" | "7703142"	"7748609" | "7748617"	"7748636" | "7762457"	"7789302" | "7793851" | "7796013").PN. OR ("7801799"	"7801829"					

		| "7805755" | "7809643" | "7827115" | "7828214" | "7848746" | "7882553" | "7900048" | "7908216" | "7922082" | "7933589" | "7949559" | "7954716" | "7954723" | "7962369" | "7993197" | "8005426" | "8010405" | "8041954" | "8060012" | "8074877" | "8082450" | "8095113" | "8099332" | "8103249" | "8108687" | "8127143" | "8135648" | "8140010" | "8141136" | "8150321" | "8150767" | "8186602" | "8196131" | "8215563" | "8224753" | "8232879" | "8233841" | "8245292" | "8249654" | "8266451" | "8285329" | "8302872" | "8312519" | "8316237" | "8332272" | "8365988" | "8369960" | "8371501" | "8381307" | "8391719" | "8417231" | "8439271" | "8475367" | "8489112" | "8511542" | "8559872" | "8566916" | "8567670" | "8572386" | "8577810" | "8583454" | "8589335" | "8594730" | "8615468" | "8620218" | "8667285" | "8723941" | "8726405" | "8740073" | "8750514" | "8752189" | "8794509" | "8799668" | "8806592" | "8807440" | "8811892" | "8814039" | "8814052" | "8818867" | "8850538" | "8861733" | "8880027" | "8888002" | "8898088" | "8934837" | "8977569" | "8994498" | "9004365" | "9038894" | "9042814" | "9047531" | "9069976" | "9081948" | "9104853" | "9118663" | "9122964" | "9129280" | "9152832" | "9203800" | "9209867" | "9251330" | "9251518" | "9258715" | "9270337" | "9306626" | "9306942" | "9324066" | "9324067" | "9332587" | "9338622" | "9373141" | "9379841" | "9413430" | "9413768" | "9420496" | "9426132"					

		| "9432339" | "9455968" | "9473509" | "9491626" | "9553637" | "9619952" | "9635000").PN. OR ("9665858" | "9674705" | "9679286" | "9680942" | "9710804" | "9740342" | "9740988" | "9763097" | "9767329" | "9769662" | "9773151" | "9780953" | "9891823" | "9940571" | "9953323" | "9961194" | "9965756" | "9965911" | "9978058" | "RE42762").PN.					
L60	84	L40 same dynamic$6 same static$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:34 AM
L61	3	L60.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:34 AM
L62	417	("7580898").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 08:37 AM
L63	233	L39 and L62	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:38 AM
L64	87	L63 and nfc	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L65	160	L63 and online	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L66	62	L64 and L65	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L67	43	(Artificial Intelligence) Similar to: 17/528,073 with 0 CPC Selections and 0 Text Selections Text: (US-20210304187-A1 OR US-11176538-B2 OR US-20220207517-A1 OR US-20190325428-A1 OR US-10810579-B2 OR US-20220270077-A1 OR US-20210027276-A1 OR US-11328286-B2 OR US-10339520-B2 OR US-10628820-B2 OR US-20220318784-A1 OR US-20160148190-A1 OR US-20170132616-A1 OR US-9430765-B2 OR US-9760884-B2 OR US-10013693-B2 OR US-20190197520-A1 OR US-20150213351-	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN))	OR	ON	ON	2022/11/05 01:38 PM

IPR2025-01150
Apple EX1071 Page 1478

		A1 OR US-20140263627-A1 OR US-20150213437-A1 OR US-9022286-B2 OR US-20180247300-A1 OR US-9224083-B2 OR US-10332101-B2 OR KR-102395069-B1 OR US-11341470-B1 OR US-20110240745-A1 OR US-10248949-B2 OR WO-2008035174-A3 OR US-20190188687-A1 OR US-5564486-A OR US-20210272091-A1 OR NL-2004464-B1 OR NL-2004464-A OR TW-200705350-A OR US-7328840-B2 OR US-10528941-B2 OR US-9830598-B2 OR WO-2006134545-A3 OR US-10984407-B2 OR US-20170109738-A1 OR US-20180005226-A1 OR US-8998096-B2 OR US-9183480-B1 OR US-20150186877-A1 OR GB-1446170-A OR WO-2018011630-A1 OR EP-3482366-A1 OR CN-111899412-A OR NL-2002671-C2).did.					
L68	35	"528073"	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2022/11/05 01:45 PM
L69	39353	(G06Q20/341 OR G06K19/06206 OR G06K19/0716 OR G06K19/07749 OR G06Q20/06 OR G06Q20/065 OR G06Q20/223 OR G06Q20/24 OR G06Q20/346 OR G06Q20/347 OR G06Q20/352 OR G06Q20/3827 OR G06Q20/385 OR G06Q20/4012 OR G06Q20/409 OR G07F7/0873 OR G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2022/11/05 02:30 PM
L70	336	69 AND dynamic$6 SAME generat$4 SAME nfc	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2022/11/05 03:37 PM
L71	161	card SAME issu$4	(US-PGPUB; USPAT;	OR	OFF	OFF	2022/11/05

IPR2025-01150
Apple EX1071 Page 1479

		SAME dynamic$6 SAME generat$4 SAME nfc	EPO; JPO)				03:38 PM
L72	66	69 AND 71	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2022/11/05 03:38 PM
L73	38	(US-0044510-$ | US-0269005-$ | US-0275761-$ | US-0402811-$ | US-0423942-$ | US-0454728-$ | US-0460314-$ | US-0505277-$ | US-0516208-$ | US-0540647-$ | US-0546291-$ | US-0592893-$ | US-0680322-$ | US-0699266-$ | US-0713646-$ | US-0796299-$ | US-0803452-$ | US-0862718-$ | US-0902390-$ | US-0929851-$ | US-0990954-$ | US-0990959-$ | US-0998620-$ | US-1004075-$ | US-1017399-$ | US-1042855-$ | US-1061698-$ | US-10736322-$ | US-1074581-$ | US-1100431-$ | US-1107047-$ | US-1127010-$ | US-1129018-$ | US-11967211-$ | US-1227278-$ | US-1232339-$ | US-1321701-$ | US-17528073-$ | US-7528073-$ | US-9846866-$).DID.	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2023/01/28 04:09 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

PE2E SEARCH - Search History (Similarity Search)

Ref #	Application Number	Text Selections	CPC Selections
L67	17/528,073	No selections	No selections

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9600808		2017-03-21	Gomez, Sr.; William et al.	
	2	9098846		2015-08-04	Gill; Sara et al.	
	3	7690580		2010-04-06	Shoemaker; Austin William	
	4	8499334		2013-07-30	Doughty; Ralph O. et al.	
	5	11100431		2021-08-24	Mullen; Jeffrey D. et al.	
	6	8255323		2012-08-28	Casey; Brandon J et al.	
	7	8423462		2013-04-16	Amacker; Matthew W. et al.	
	8	10460314		2019-10-29	Hird; Geoffrey R. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	9	9846866		2017-12-19	Royyuru; Vijay	
	10	6736322		2004-05-18	Gobburu; Venkata T. et al.	
	11	7967211		2011-06-28	Challa; Nagesh et al.	
	12	8628012		2014-01-14	Wallner; George	
	13	8690059		2014-04-08	Wallner; George	
	14	8814046		2014-08-26	Wallner; George	
	15	9361613		2016-06-07	Wallner; George	
	16	9454679		2016-09-27	Wallner; George	
	17	9652642		2017-05-16	Wallner; George	
	18	9864994		2018-01-09	Huang; Enyang et al.	
	19	10044510		2018-08-07	Kwon; Eun Young et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	20	10269005		2019-04-23	Lee; Woo-Sup et al.	
	21	10275761		2019-04-30	Lee; Woo-Sup et al.	
	22	10402811		2019-09-03	Park; Yong Man et al.	
	23	10423942		2019-09-24	Lee; Woosup et al.	
	24	10454728		2019-10-22	Huang; Enyang	
	25	10505277		2019-12-10	Lee; Woosup et al.	
	26	10516208		2019-12-24	Lee; Woo-Sup et al.	
	27	10540647		2020-01-21	Park; Yong Man et al.	
	28	10546291		2020-01-28	Kim; Eun Jik et al.	
	29	10592893		2020-03-17	Lee; Hee-Dong et al.	
	30	10680322		2020-06-09	Lee; Woosup et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	31	10699266		2020-06-30	Lee; Hee-Dong et al.	
	32	10713646		2020-07-14	Lee; Hee-Dong et al.	
	33	10796299		2020-10-06	Lee; Woo-Sup et al.	
	34	10803452		2020-10-13	Kim; Eun Jik et al.	
	35	10862718		2020-12-08	Huang; Enyang	
	36	10902390		2021-01-26	Lee; Woosup et al.	
	37	10929851		2021-02-23	Kang; Minkoo et al.	
	38	10990954		2021-04-27	Park; Yong Man et al.	
	39	10990959		2021-04-27	Lee; Woo-Sup et al.	
	40	10998620		2021-05-04	Lee; Woosup et al.	
	41	11004075		2021-05-11	Lee; Je Min et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	42	11017399		2021-05-25	Park; Yong Seok et al.	
	43	11042855		2021-06-22	Kim; Yu Hwan et al.	
	44	11061698		2021-07-13	Rhee; Injong et al.	
	45	11074581		2021-07-27	Kim; In Ho et al.	
	46	11107047		2021-08-31	Kim; Kibong et al.	
	47	11127010		2021-09-21	Cho; Boo Hyun et al.	
	48	11129018		2021-09-21	Kim; Ki Bong et al.	
	49	11227278		2022-01-18	Choi; Hoon et al.	
	50	11232339		2022-01-25	Lee; Woosup et al.	
	51	11321701		2022-05-03	Lee; Hee-Dong et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20130124410		2013-05-16	KAY; Christopher Erin et al.	
	2	20080319905		2008-12-25	CARLSON; Mark	
	3	20100185545		2010-07-22	Royyuru; Vijay K. et al.	
	4	20130262305		2013-10-03	Jones; Andrew R. et al.	
	5	20060089171		2006-04-27	Yoo; Kyung-Min et al.	
	6	20090048971		2009-02-19	Hathaway; Matthew et al.	
	7	20130232083		2013-09-05	SMITH; Theresa L. et al.	
	8	20080126260		2008-05-29	Cox; Mark A. et al.	
	9	20080222047		2008-09-11	Boalt; Adam	
	10	20080172317		2008-07-17	Deibert; Doug et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	11	20090159701		2009-06-25	Mullen; Jeffrey D. et al.	
	12	20120317035		2012-12-13	Royyuru; Vijay K. et al.	
	13	20130166441		2013-06-27	Kobylkin; Egor et al.	
	14	20120310760		2012-12-06	Phillips; Simon et al.	
	15	20080302876		2008-12-11	Mullen; Jeffrey D.	
	16	20110186626		2011-08-04	Manessis; Thomas et al.	
	17	20150147065		2015-05-28	Civelli; Jay Pierre et al.	
	18	20140143785		2014-05-22	Mistry; Pranav et al.	
	19	20050043997		2005-02-24	Sahota, Jagdeep Singh et al.	
	20	20150178724		2015-06-25	Ngo; Hao et al.	
	21	20160132881		2016-05-12	LEE; Yang-Soo et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	22	20160253652		2016-09-01	JE; Seong-Min et al.	
	23	20160253657		2016-09-01	SOHN; Se Chang et al.	
	24	20190026725		2019-01-24	PARK; Yong Seok et al.	
	25	20190172051		2019-06-06	LEE; Hui Jae et al.	
	26	20190173290		2019-06-06	HA; Min Cheol et al.	
	27	20210311752		2021-10-07	Rhee; Injong et al.	
	28	20220005046		2022-01-06	KIM; Inho et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2478712	GB		2011-09-21	JACKSON, DAVID		
	2	2485442	GB		2012-05-16	CUBIC CORP		

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	3	00/62214	WO		2000-10-19	CLEARTOGO.COM et al.		
	4	01/57620	WO		2001-08-09	COMSENSE TECHNOLOGIES LTD et al.		
	5	2007145687	WO		2007-12-21	WEISS, KENNETH P.		
	6	2010043974	WO		2010-04-22	RICHARD, CHRISTIAN		
	7	2012154915	WO		2012-11-15	DYNAMICS INC et al.		
	8	2005119607	WO		2005-12-15	TYFONE INC et al.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Motorola MotoACTV Smartwatch, http://www.manualplanet.com/pdf/watches/motorola/motorola-motoactv-gpsfitness-tracker-quick-start-guide.pdf, 2012, pp. 1-2.	
	2	PEREZ, "New NFC-Enabled Phones to Hit Europe," ReadWriteWeb, February 18, 2011, pp. 1-3.	
	3	WESTER, "New Samsung Galaxy S4 phone includes NFC, innovative barcode technology; New Samsung smartphone adds a number of features that may spur mobile payment adoption," Mobile Payments Today, March 15, 2013, Networld Media Group, pp. 1-2.	
	4	"NFC Focus: Which Smartphones Have NFC?," International Business Times News, August 9, 2012, pp. 1-3	
	5	"NFC for mobile operators; Maximizing opportunities in the mobile NFC marketplace," Gemalto, November 2009, pp. 1-2.	
	6	CATHELINAIS, "Nice, the first city to switch to contactless payment," 01net.com, May 21, 2010, pp. 1-6.	
	7	CLARK, "Orange to offer Samsung Wave 578 NFC across Europe - but not in the UK," NFC World, February 14, 2011, pp. 1-4.	
	8	CLARK, "Orange to roll out NFC services across Europe in 2011," NFC World, December 16, 2010, pp. 1-3.	
	9	"PayPal Credit Card Tokenization Extension - Magento Connect," Magento Extension Marketplace, http://www.magentocommerce.com/magentoconnect/catalog/product/view/id/18715/s/paypal-credit-card-tokenization-extension-4490/, October 5, 2013, page 1.	
	10	Nanninga, "PayPal Credit Card Tokenization in Magento," SitePoint, September 30, 2013, pp. 1-11.	
	11	"Payment Card Industry (PCI), Data Security Standard, PCI DSS Applicability in an EMV Environment, A Guidance Document, Version 1," PCI Security Standards Council, October 5, 2010, pp. 1-12.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Version: 1.0, Information Supplement: ATM Security Guidelines," PCI Security Standards Council, January 2013, pp. 1-44.	
	13	"PayPal NVP API Developer Reference Enterprise Edition - eBay," August 28, 2012, pp. 1-382.	
	14	"Rambus' Bell ID to support Android Pay," Rambus, February 18, 2016, page 1.	
	15	"RIM implements Bell ID's Token Manager software for mobile payments," WMI Company News, January 23, 2013, World Market Intelligence Private Ltd., page 1.	
	16	LAI, "Samsung and Visa join forces to enable NFC mobile payment at 2012 Olympics," Engadget, April 1, 2011, pp. 1-6.	
	17	"Samsung and Visa Showcase Mobile Payments at the London 2012 Olympic and Paralympic Games," Business Wire, May 9, 2012, pp. 1-4.	
	18	WARREN, "Samsung and Visa Take NFC Mobile Payments Global," Mashable.com, February 25, 2013, pp. 1-2.	
	19	HASELTON, "Samsung and Visa team up for NFC mobile payments at London 2012 Olympics," Boy Genius Report, March 31, 2011, pp. 1-3.	
	20	"Samsung and Visa to Showcase Mobile Payments @ the London Olympics," Samsung Global Newsroom, May 9, 2012, pp. 1-3.	
	21	"Samsung Announces Launch Dates for Groundbreaking Mobile Payment Service: Samsung Pay," Samsung Global Newsroom, August 14, 2015, pp. 1-2.	
	22	GROTTA, "Samsung Begins to Phase Out Support of MST for Samsung Pay," PaymentsJournal, February 22, 2021, pp. 1-3.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	MURPH, "Samsung cooks up its own NFC module, destined for the Nexus S?," Engadget, December 1, 2010, pp. 1-2.	
	24	MOLEN, "Samsung Galaxy S III for Verizon Wireless review," Engadget, July 9, 2012, pp. 1-10.	
	25	TRENHOLM, "Samsung Galaxy S3 is Olympic phone for no-touch payments," CNET, May 9, 2012, pp. 1-2.	
	26	"Samsung Google Nexus S - Full Phone Specifications, Reviews: Royal droid," GSMArena.com (archive.org), November 2010, pp. 1-2.	
	27	"Samsung Google Nexus S review: Royal droid," GSMArena.com (archive.org), February 11, 2011, pp. 1-2.	
	28	"Samsung partners with FeliCa for Japanese NFC solutions, unveils 2012 Olympics' mobile payment app with Visa," Engadget, February 24, 2012, pp. 1-3.	
	29	CLARK, "Samsung picks NXP for S3," NFCW, May 14, 2012, pp. 1-2.	
	30	"SAMSUNG to Acquire LoopPay, Transformative Digital Wallet Platform," Samsung US Newsroom, February 18, 2015, pp. 1-2.	
	31	HEUN, "Samsung to Unveil NFC Smartwatch - Has Wrist-Payments' Time Come?," Payments Source, September 2, 2013, SourceMedia LLC d/b/a Arizent, pp. 1-2.	
	32	"Samsung's New Secu-NFC Chip Enables Secure Mobile Payment by Enhancing NFC with Security Features," Plus NEWS, November 30, 2011, pp. 1-2.	
	33	NANNINGA, "Save Credit Cards in Magento with Our New Paypal Extension," Classy Llama, August 15, 2013, pp. 1-4.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Shift4 Releases New Technology to Insure the Security of Its Merchants' and Partners' Payment Processing," Hotel Online (archive.org), October 5, 2005, pp. 1-2.	
	35	"S-Pay: What is MST?," Samsung Levant, September 22, 2020, pp. 1-2.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Susan Pandy, "Securing Payments: Payments Tokenization in Primetime," Federal Reserve Bank of Boston Payments Symposium, January 20, 2016, pp. 1-20.	
	2	"SUMMARY OF ANS X9.119-Part 2 USE OF TOKENS TO PROTECT SENSITIVE CARD DATA," September 2017, pp.1-2.	
	3	Marianne Crowe et al., "Is Payment Tokenization Ready for Primetime?," June 11, 2015, pp. 1-51.	
	4	Terence Spies et al., "ANSI X9.119 Part 2: Using Tokenization Methods," 2013, pp. 1-20.	
	5	ASSORA et al., "A web transaction security scheme based on disposable credit card numbers," Int. J. Electronic Security and Digital Forensics, 2007, Vol. 1, No. 2, Inderscience Enterprises Ltd., pp. 146-155.	
	6	BOYD, "A pragmatic approach to temporary payment cards numbers," Int. J. Electronic Security and Digital Forensics, 2009, Vol. 2, No. 3, pp. 253-268.	
	7	BUCCAFURRI et al., "Implementing disposable credit card numbers by mobile phones," Electronic Commerce Research, Feb. 23, 2011, Vol. 11, Springer Publishing, pp. 271-296.	
	8	JAVANI et al., "A new credit card payment system based on 3D-Secure using one-time-use transaction numbers," Information Assurance and Security Letters, 2010, Vol. 1, Dynamic Publishers, Inc., USA, pp. 060-065.	
	9	KILLORAN et al., "A New Secure Wireless Financial Transaction Architecture," EUROCON 2005, November 22-24, 2005, IEEE, pp. 1060-1063.	
	10	LI et al., "A security-enhanced one-time payment scheme for credit card," Mar. 28-29, 2004, IEEE, pp. 1-11.	
	11	MJØLSNES et al., "On-Line E-Wallet System with Decentralized Credential Keepers," Mobile Networks and Applications, 2003, Vol. 8, Kluwer Academic Publishers, The Netherlands, pp. 87–99.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	NARAYANASWAMI et al., "What Would You Do with a Hundred MIPS on Your Wrist?," RC 22057 (98634) January 22, 2001, IBM Research, pp. 1-10.	
	13	QASIM et al., "Interactive Shopping with Mobile Wallet," World Congress on Sustainable Technologies, 2012, IEEE, pp. 32-36.	
	14	HONIG, "A Week with Google Wallet," Endgadget, September 19, 2011, pp. 1-49.	
	15	KADAMBI et al.,"Near-Field Communication-Based Secure Mobile Payment Service," ICEC'09, August 12–15, 2009, pp. 1-11.	
	16	"A closer look at Google Pay and tokenization," Rambus Press, February 23, 2016, pp. 1-2.	
	17	GHAG et al., "A Comprehensive Study of Google Wallet as an NFC Application," International Journal of Computer Applications, November 2012, Vol. 58, No.16, pp. 37-42.	
	18	"Add any credit or debit card," Google Wallet Help (archive.org), 2012, page 1.	
	19	"Add any credit or signature debit card," Wallet Help, Google Wallet, September 20, 2012, page 1.	
	20	"Allynis Mobile NFC," Gemalto, September 2007, pp. 1-4.	
	21	"Allynis TSM for Transport," Gemalto, October 2009, pp. 1-2.	
	22	ADAMS, "Amex Plays a Major Role in Revamped Isis Mobile Wallet," Payments Source, November 15, 2013, Vol. 1, No. 1, SourceMedia LLC d/b/a Arizent, pp. 1-2.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	PEREZ, "Android Pay, Google's Apple Pay Rival, Arrives Today," DigitalOcean, September 10, 2015, pp. 1-8.	
	24	HEISLER, "Apple Pay: An in-depth look at what's behind the secure payment system," Engadget, October 2, 2014, pp. 1-7.	
	25	FEHR, "Apple Pay: How different is it from other Pay solutions, what role does tokenisation play, and to what degree can Card not Present payment benefit from Apple Pay in future," Technical Report RHUL–ISG–2018–3, April 3, 2018, Egham, Surrey, UK, pp. 1-79.	
	26	"ATMIA publishes contactless ATM best practices," ATM Marketplace, September 27, 2012, pp. 1-2.	
	27	POPPER, "Banks Did It Apple's Way in Payments by Mobile," New York Times, September 11, 2014, pp. 1-2.	
	28	"Bell ID Simplifies EMV Smart Card and NFC Application Management with Versatile New Platform," eBanking & Payment News, May 5, 2011, page 1.	
	29	"BofA pursuing contactless ATM patent," Mobilepaymentstoday.com News, September 20, 2012, Newstex LLC, pp. 1-2.	
	30	"Chip Advisory #20, Visa Recommended Practices for EMV Chip Implementation in the U.S," July 11, 2012, pp. 1-10.	
	31	"Commbank, Mastercard and Samsung collaborate to launch NFC payment service," MarketLine NewsWire (Formerly Datamonitor), December 13, 2013, pp. 1-2.	
	32	"Contactless Payment: Secure Enough?," Card Technology, September 1, 2005, SourceMedia, Inc., Section: SPECIAL ISSUE: CONTACTLESS TECHNOLOGY, Vol. 10, No. 8, page 36.	
	33	"Eligible Devices," Google Wallet Help (archive.org), November 18, 2012, page 1.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	MOTT, "EMV and Mobile Payments, Questions abound, answers divide," Payments Summit Workshop, February 4, 2013, pp. 1-22.
	35	"EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management Version 4.1," May 2004, pp. 1-187.
	36	"EMV Integrated Circuit Card Specifications for Payment Systems. Book 2, Security and Key Management, Version 4.3," November 2011, pp. 1-174.
	37	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.3," November 2011, pp. 1-230.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

IPR2025-01150
Apple EX1071 Page 1506

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ACKNOWLEDGEMENT OF CHANGE TO SMALL ENTITY STATUS

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
17/528,073	11/16/2021	David WYATT	WYAT-0002-USD1C1C1C1C1C	64260

The entity status change request below filed through Patent Center on 02/13/2023 has been accepted.

Certifications

APPLICANT ASSERTING SMALL ENTITY STATUS. See 37CFR 1.27.

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Jose S. Garcia/	Jose Garcia	43628

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2876	3750	WYAT-0002-USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

OC000000157392572

Date Mailed: 02/14/2023

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

David WYATT, Austin, TX;

Applicant(s)

CARDWARE, INC, Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number 136197

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

IPR2025-01150
Apple EX1071 Page 1508

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

IPR2025-01150
Apple EX1071 Page 1509

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01150
Apple EX1071 Page 1511

PART B – FEE(S) TRANSMITTAL

Complete and send this form, together with the applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By fax, send to: (571) 273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

David Wyatt c/o Murabito, Hao & Barnes LLP
111 North Market Steet
Suite 700
San Jose, CA 95113

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

Mina Oliveri	(Typed or printed name)
/Mina Oliveri/	(Signature)
2-14-2023	(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO	CONFIRMATION NO
17/528,073	11/16/2021	David Wyatt	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	05/15/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363)

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1.

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2. 3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE or COUNTRY)
CARDWARE, INC.	AUSTIN, TEXAS

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees Submitted: ☑ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment (*Please first reapply any previously paid fee shown above*):

☑ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 504160

5. Change of Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29. NOTE: Absent a valid Certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27. NOTE: If the application was previously under micro entity status, checking this box will be taken as a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status. NOTE: Checking this box will be taken as a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Anthony C. Murabito/ Date 2-14-2023

Typed or printed name Anthony C. Murabito Registration No. 35,295

IPR2025-01150
Apple EX1071 Page 1512

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:	17528073			
Filing Date:	16-Nov-2021			
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE			
First Named Inventor/Applicant Name:	David WYATT			
Filer:	Anthony C. Murabito/Mina Oliveri			
Attorney Docket Number:	WYAT-0002-13C12US			
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt	
EFS ID:	47531835
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Anthony C. Murabito/Mina Oliveri
Filer Authorized By:	Anthony C. Murabito
Attorney Docket Number:	WYAT-0002-13C12US
Receipt Date:	14-FEB-2023
Filing Date:	16-NOV-2021
Time Stamp:	15:28:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	EFT
Payment was successfully received in RAM	$480
RAM confirmation Number	E20232DF29188730
Deposit Account	504160
Authorized User	Mina Oliveri
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.19 (Document supply fees)	

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	WYAT-0002-USD1C1C1C1C1C_IssueFee_Tran_2-14-2023.pdf	296037 42f56887661a1a626d828d80618bf2d84b591e2e	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38083 9be0bc43f8aeafb866a9db489893a13bcfeb6807	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	334120		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	04/04/2023	11620634	WYAT-0002-13C12US	4809

136197 7590 03/15/2023

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PAIR WEB site http://pair.uspto.gov for additional inventors):

David WYATT, Austin, TX;

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

CARDWARE, INC, Austin, TX;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ACKNOWLEDGEMENT OF LOSS OF ENTITLEMENT TO ENTITY STATUS DISCOUNT

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
17/528,073	11/16/2021	David WYATT	WYAT-0002-13C12US	267402

The entity status change request below filed through Patent Center on 08/29/2024 has been accepted.

Certifications

APPLICANT CHANGING TO REGULAR UNDISCOUNTED FEE STATUS

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Anthony C. Murabito/	Anthony Murabito	35295

AO 120 (Rev. 08/10)

TO:	**Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:23-CV-00187	4/24/2023	Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
CardWare Inc.	Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	11,620,634	4/4/2023	CARDWARE INC.
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Print Save As... Reset