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



GOOGLE EXHIBIT 1073 (Part 3 of 3)
Google LLC v. Cardware Inc.
IPR2025-01344

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

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

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,

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

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.

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

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.

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.

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

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

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

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.

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

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

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

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.

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

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

(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.

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.

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.

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

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.

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.

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

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

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.

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.

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

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.

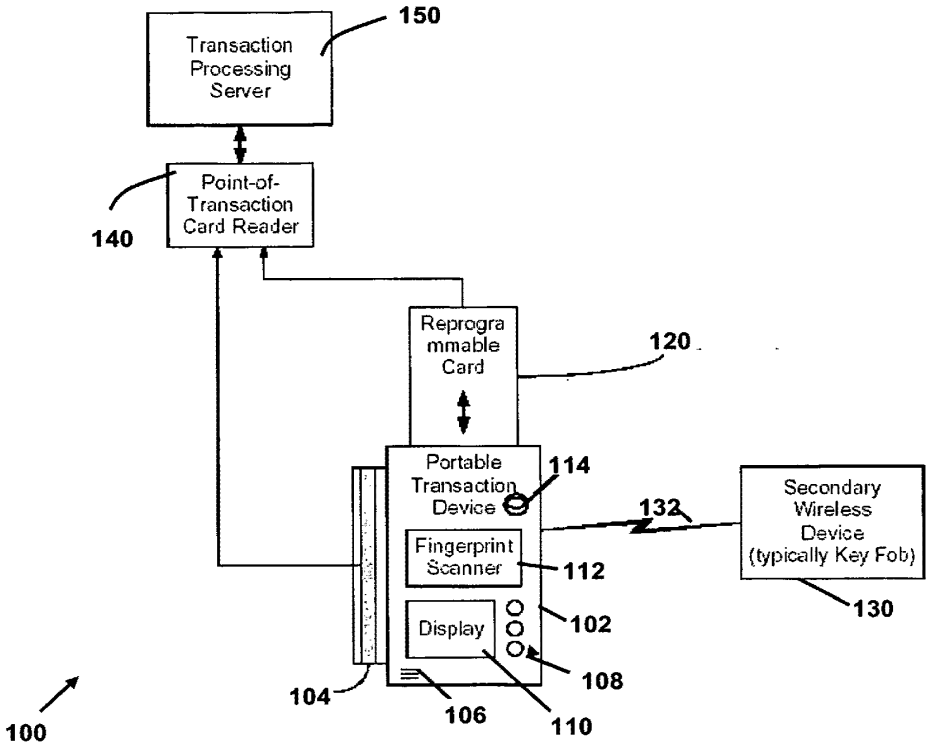

Transaction Processing Server
150
Point-of-Transaction Card Reader
140
Reprogra mmable Card
120
Portable Transaction Device
114
Fingerprint Scanner
112
Display
102
108
104
106
110
100
132
Secondary Wireless Device (typically Key Fob)
130

Fig. 1

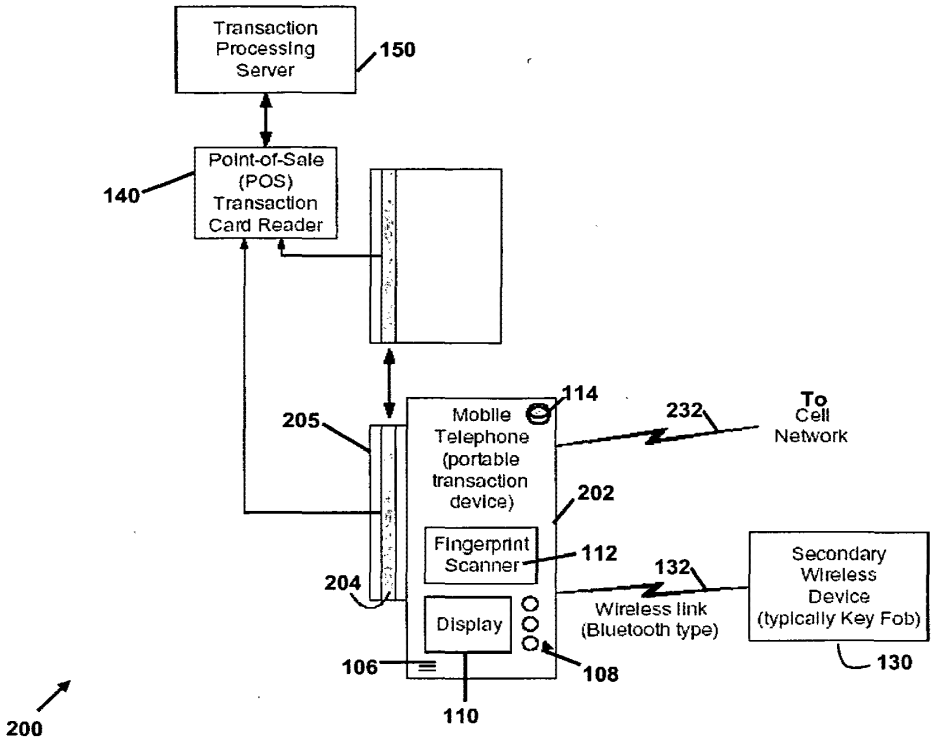

Transaction Processing Server
150
Point-of-Sale (POS) Transaction Card Reader
140
205
Mobile Telephone (portable transaction device)
114
232
To Cell Network
202
Fingerprint Scanner
112
204
132
Secondary Wireless Device (typically Key Fob)
Display
Wireless link (Bluetooth type)
106
108
130
110
200

Fig. 2

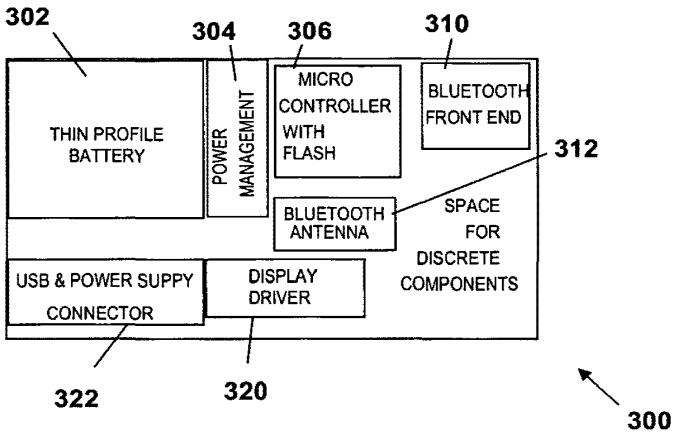

302
304
306
310
THIN PROFILE BATTERY
POWER MANAGEMENT
MICRO CONTROLLER WITH FLASH
BLUETOOTH FRONT END
312
BLUETOOTH ANTENNA
SPACE FOR DISCRETE COMPONENTS
USB & POWER SUPPY CONNECTOR
DISPLAY DRIVER
322
320
300

Fig. 3

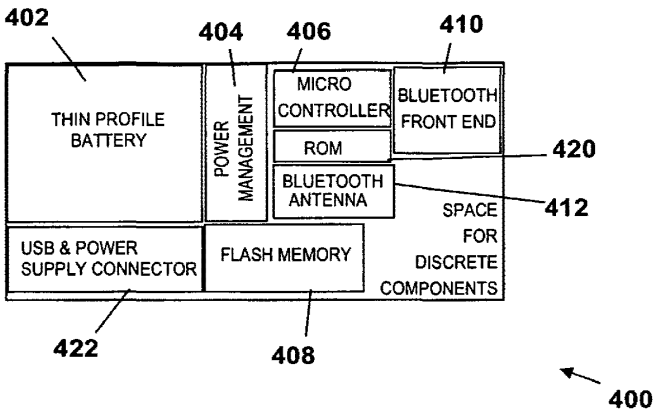

402
404
406
410
THIN PROFILE BATTERY
POWER MANAGEMENT
MICRO CONTROLLER
BLUETOOTH FRONT END
ROM
420
BLUETOOTH ANTENNA
412
SPACE FOR DISCRETE COMPONENTS
USB & POWER SUPPLY CONNECTOR
FLASH MEMORY
422
408
400

Fig. 4

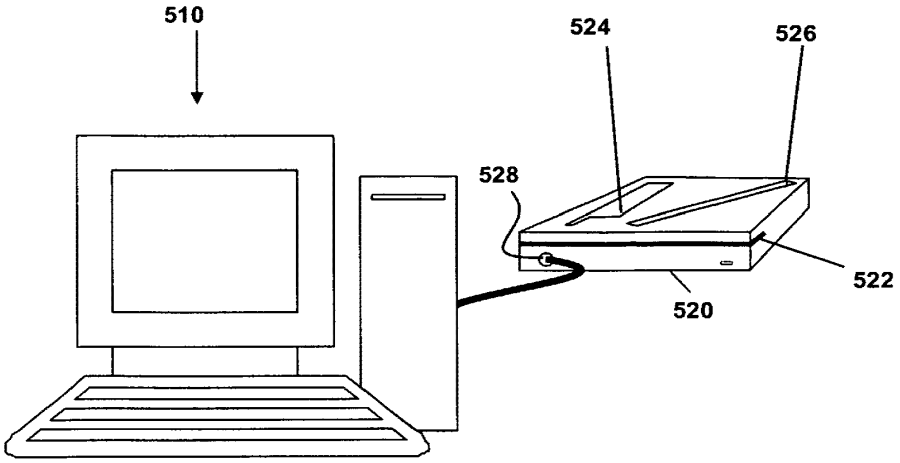



Fig. 5

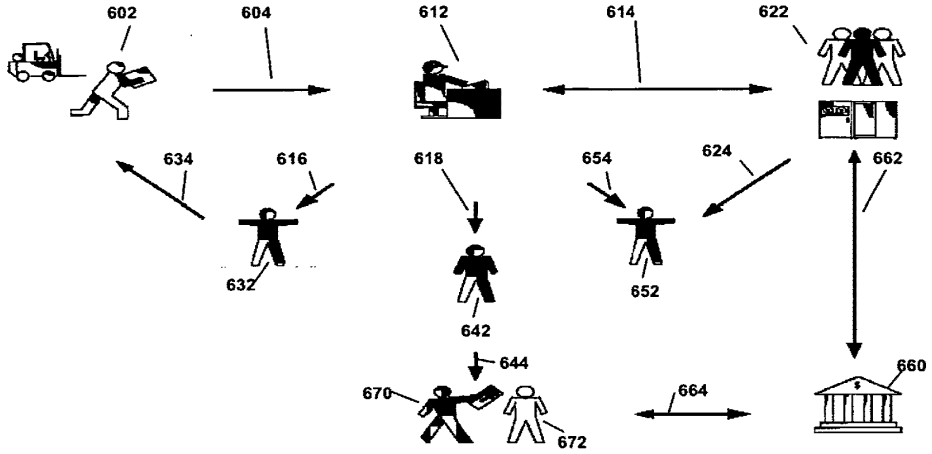

602
604
612
614
622
634
616
618
654
624
662
632
642
652
644
660
670
664
672

Fig. 6

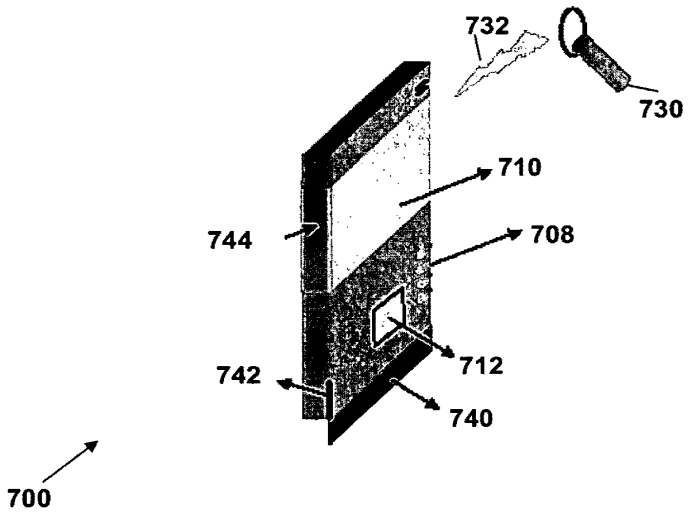



Fig. 7

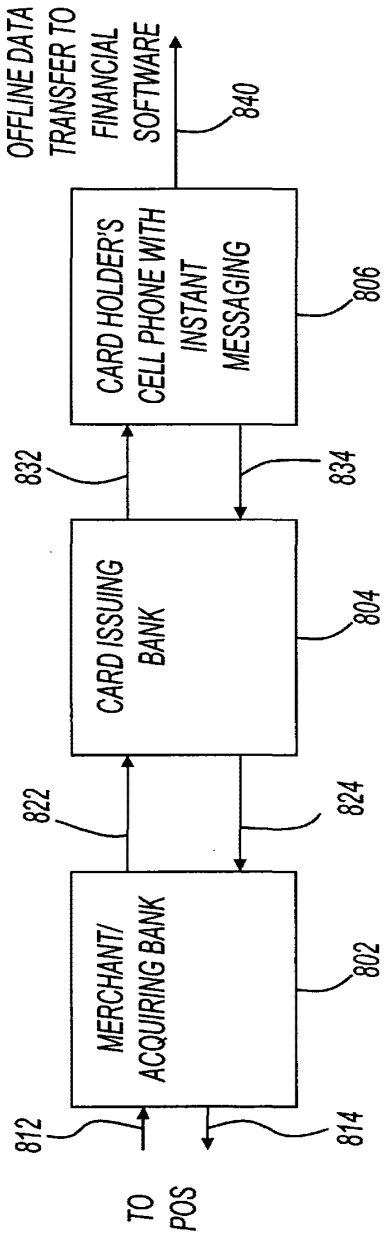

OFFLINE DATA TRANSFER TO FINANCIAL SOFTWARE
840
CARD HOLDER'S CELL PHONE WITH INSTANT MESSAGING
806
832
834
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

*FIG. 8*

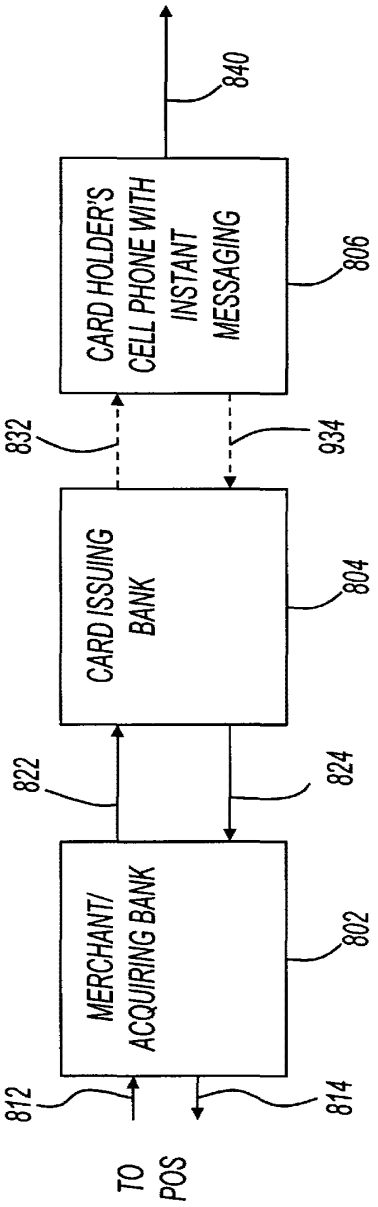

840
CARD HOLDER'S CELL PHONE WITH INSTANT MESSAGING
806
832
934
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 9

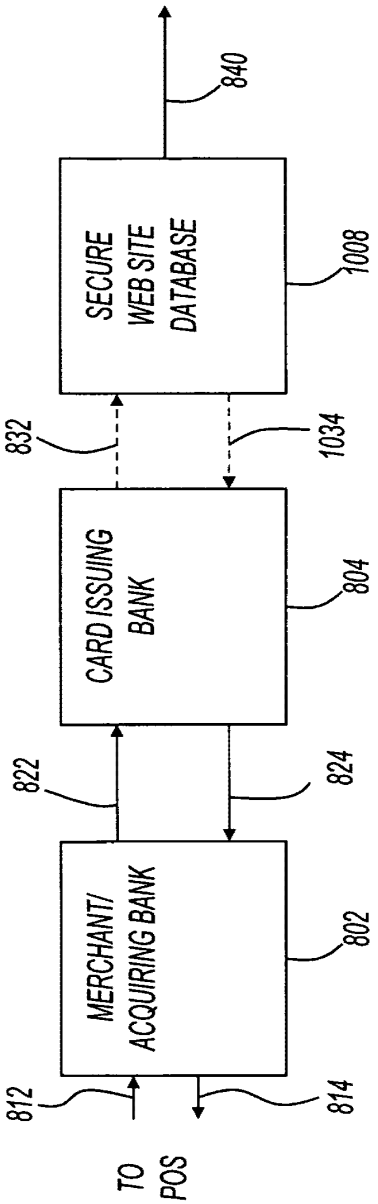

840
SECURE WEB SITE DATABASE
1008
832
1034
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 10

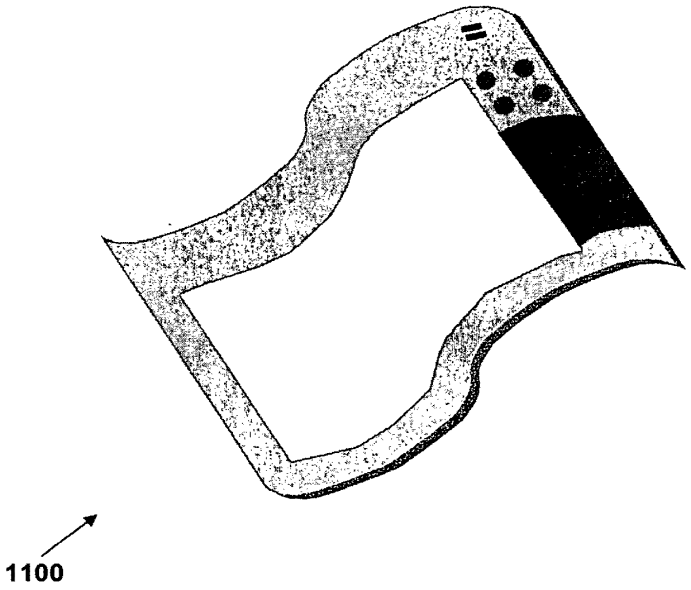



Fig. 11

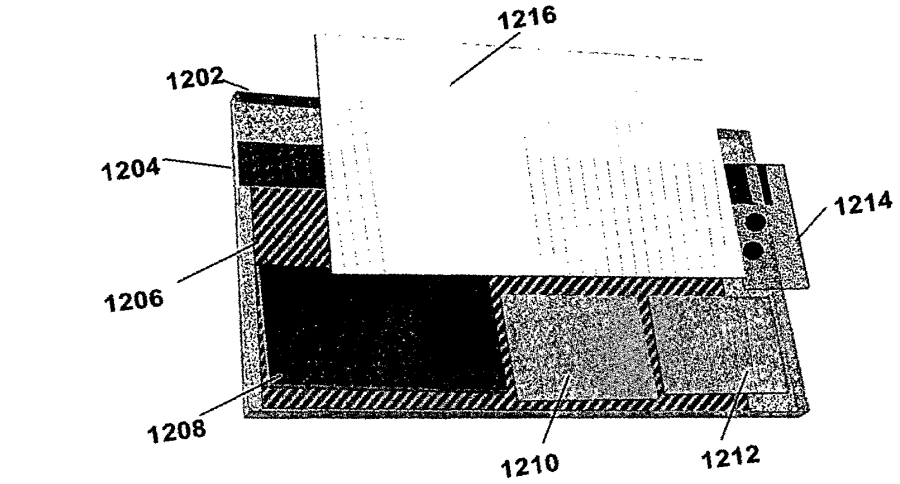



Fig. 12

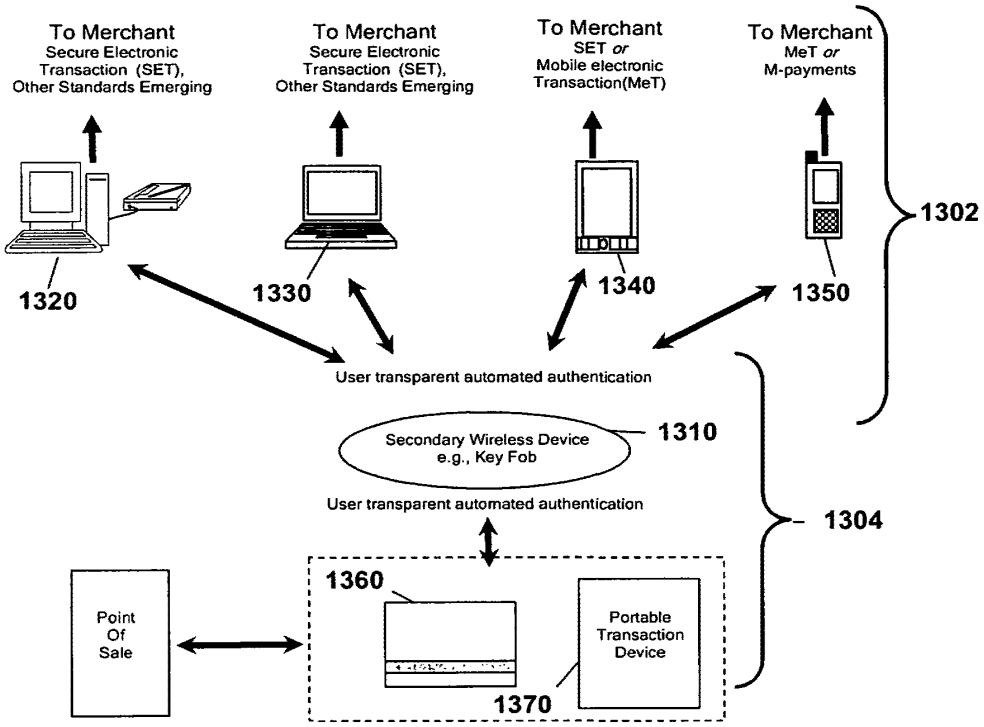

To Merchant
Secure Electronic Transaction (SET), Other Standards Emerging
To Merchant
Secure Electronic Transaction (SET), Other Standards Emerging
To Merchant
SET or Mobile electronic Transaction(MeT)
To Merchant
MeT or M-payments
1302
1320
1330
1340
1350
User transparent automated authentication
Secondary Wireless Device e.g., Key Fob
1310
User transparent automated authentication
1304
Point Of Sale
1360
Portable Transaction Device
1370

Fig. 13

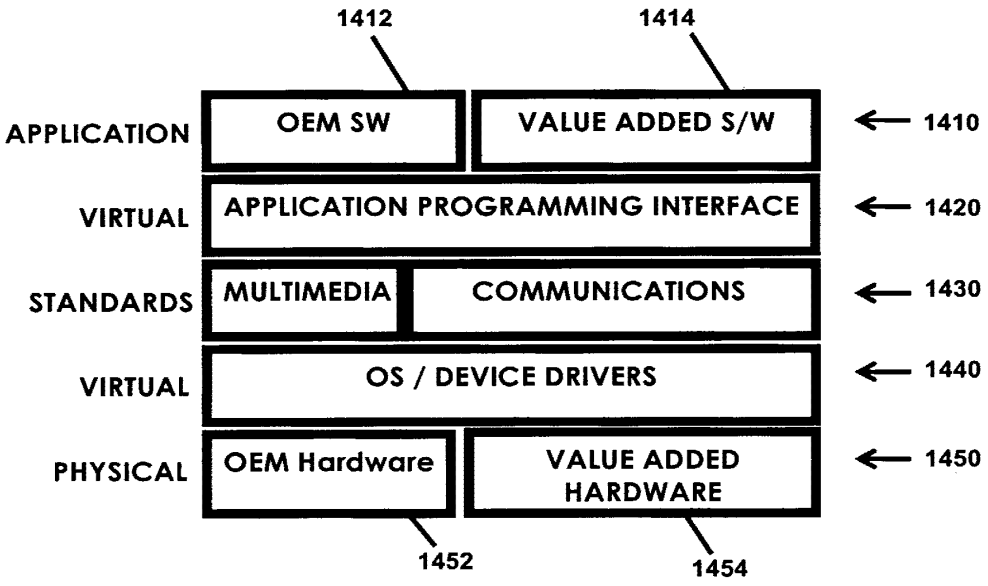

1412
1414
APPLICATION
OEM SW
VALUE ADDED S/W
1410
VIRTUAL
APPLICATION PROGRAMMING INTERFACE
1420
STANDARDS
MULTIMEDIA
COMMUNICATIONS
1430
VIRTUAL
OS / DEVICE DRIVERS
1440
PHYSICAL
OEM Hardware
VALUE ADDED HARDWARE
1450
1452
1454

Fig. 14

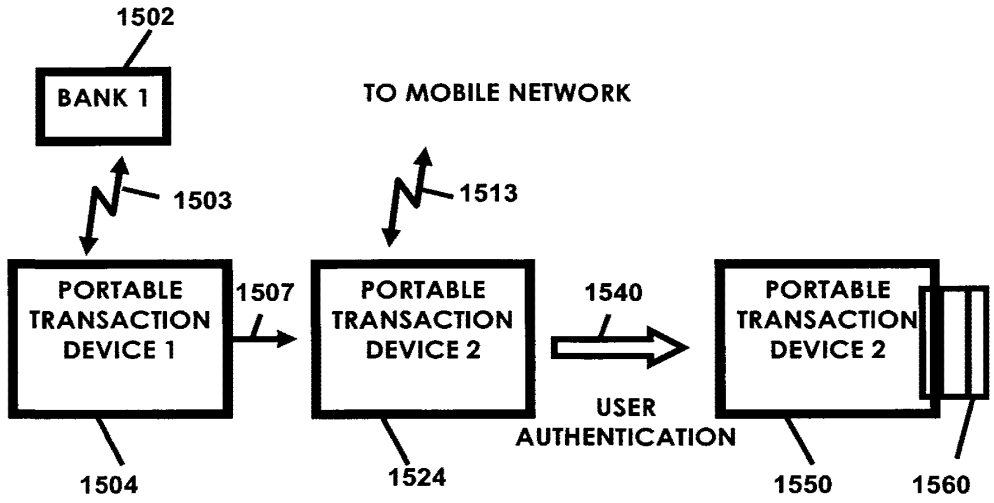

1502
BANK 1
TO MOBILE NETWORK
1503
1513
PORTABLE TRANSACTION DEVICE 1
1507
PORTABLE TRANSACTION DEVICE 2
1540
PORTABLE TRANSACTION DEVICE 2
USER AUTHENTICATION
1504
1524
1550
1560

Fig. 15

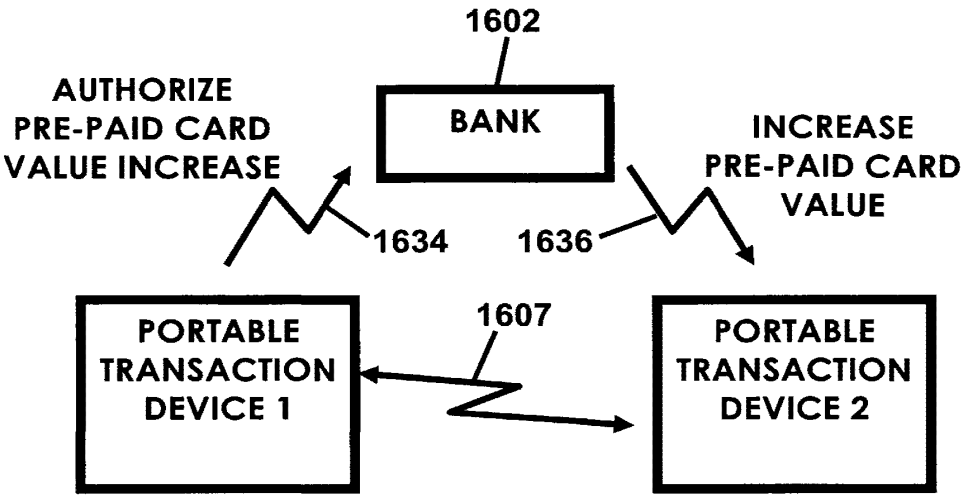

1602
BANK
AUTHORIZE
PRE-PAID CARD
VALUE INCREASE
INCREASE
PRE-PAID CARD
VALUE
1634
1636
1607
PORTABLE
TRANSACTION
DEVICE 1
PORTABLE
TRANSACTION
DEVICE 2

Fig. 16

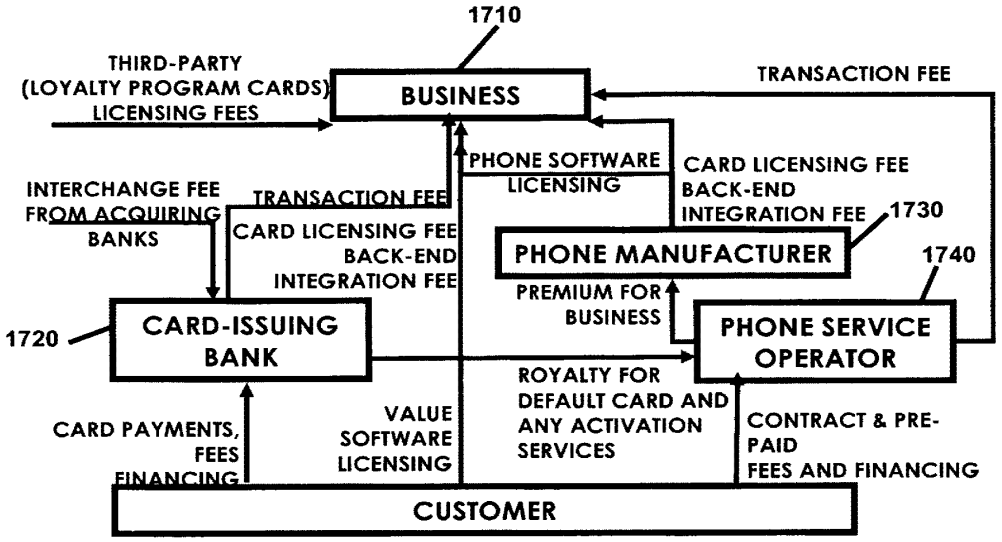

1710
THIRD-PARTY
(LOYALTY PROGRAM CARDS)
LICENSING FEES
BUSINESS
TRANSACTION FEE
PHONE SOFTWARE
LICENSING
CARD LICENSING FEE
BACK-END
INTEGRATION FEE
INTERCHANGE FEE
FROM ACQUIRING
BANKS
TRANSACTION FEE
CARD LICENSING FEE
BACK-END
INTEGRATION FEE
1730
PHONE MANUFACTURER
1740
PREMIUM FOR
BUSINESS
1720
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

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

OC000000136882734

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

**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,

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.

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.**

## 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. _____

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.

## 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

## 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/<br>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

| 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/<br>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

| 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/<br>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

| 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 |

| Search Notes | Application/Control No. | Applicant(s)/Patent Under Reexamination |
|---|---|---|
| | 17/528,073 | WYATT, David |
| | Examiner | Art Unit |
| | SEUNG H LEE | 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 | | | | | | | | |
| 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 | = | | | | | | | | |

| 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 | = | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

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



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] | 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<br>**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

| 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

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

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

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

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

**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

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

**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

## 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 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 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 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 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 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 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 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | "10133979" \|<br>"10217105" \|<br>"20010010723" \|<br>"20010029485" \|<br>"20010034702" \|<br>"20010054003" \|<br>"20020078345" \|<br>"20020093530" \|<br>"20020100808" \|<br>"20020120583" \|<br>"20020152116" \|<br>"20020153424" \|<br>"20020165827" \|<br>"20030023554" \|<br>"20030034873" \|<br>"20030055727" \|<br>"20030078882" \|<br>"20030167350" \|<br>"20030208449" \|<br>"20040015958" \|<br>"20040039919" \|<br>"20040127256" \|<br>"20040215674" \|<br>"20040230799" \|<br>"20050044367" \|<br>"20050075985" \|<br>"20050081038" \|<br>"20050138387" \|<br>"20050156026" \|<br>"20050160049" \|<br>"20050195975" \|<br>"20050247797" \|<br>"20060006230" \|<br>"20060040726" \|<br>"20060041402" \|<br>"20060044153" \|<br>"20060047954" \|<br>"20060085848" \|<br>"20060136334" \|<br>"20060173985" \|<br>"20060174331" \|<br>"20060242698" \|<br>"20060280338" \|<br>"20070033642" \|<br>"20070055630" \|<br>"20070061266" \|<br>"20070061487" \|<br>"20070116292" \|<br>"20070118745" \|<br>"20070197261" \|<br>"20070224969" \|<br>"20070241182" \|<br>"20070256134" \|<br>"20070258594" \|<br>"20070278291" \|<br>"20080008315" \|<br>"20080011831" \|<br>"20080014867" \| | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | "20080035738" \|<br>"20080071681" \|<br>"20080072303" \|<br>"20080086767" \|<br>"20080103968" \|<br>"20080109309" \|<br>"20080110983" \|<br>"20080120711" \|<br>"20080156873" \|<br>"20080162312" \|<br>"20080164308" \|<br>"20080207307" \|<br>"20080209543" \|<br>"20080223918" \|<br>"20080285746" \|<br>"20080308641" \|<br>"20090048026" \|<br>"20090132417" \|<br>"20090143104" \|<br>"20090171682" \|<br>"20090210308" \|<br>"20090235339" \|<br>"20090249077" \|<br>"20090282264" \|<br>"20100023449" \|<br>"20100023455" \|<br>"20100029202" \|<br>"20100030549" \|<br>"20100033310" \|<br>"20100036769" \|<br>"20100078471" \|<br>"20100082491" \|<br>"20100094754").PN.<br>OR ("20100095130" \|<br>"20100100480" \|<br>"20100114731" \|<br>"20100192230" \|<br>"20100207742" \|<br>"20100211797" \|<br>"20100240413" \|<br>"20100257357" \|<br>"20100312634" \|<br>"20100312635" \|<br>"20110035604" \|<br>"20110060631" \|<br>"20110084132" \|<br>"20110101093" \|<br>"20110113245" \|<br>"20110125638" \|<br>"20110131415" \|<br>"20110153437" \|<br>"20110153496" \|<br>"20110208658" \|<br>"20110208965" \|<br>"20110211219" \|<br>"20110218911" \|<br>"20110238564" \|<br>"20110246780" \| | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | "20110258452" \|<br>"20110280406" \|<br>"20110282785" \|<br>"20110294418" \|<br>"20110312271" \|<br>"20120009946" \|<br>"20120024947" \|<br>"20120030047" \|<br>"20120030121" \|<br>"20120047071" \|<br>"20120079281" \|<br>"20120109735" \|<br>"20120143754" \|<br>"20120150737" \|<br>"20120178366" \|<br>"20120196583" \|<br>"20120207305" \|<br>"20120209773" \|<br>"20120238206" \|<br>"20120239560" \|<br>"20120252350" \|<br>"20120254394" \|<br>"20120284194" \|<br>"20120290472" \|<br>"20120296818" \|<br>"20120316992" \|<br>"20120317035" \|<br>"20120317628" \|<br>"20130005245" \|<br>"20130008956" \|<br>"20130026229" \|<br>"20130054474" \|<br>"20130065564" \|<br>"20130080228" \|<br>"20130080229" \|<br>"20130099587" \|<br>"20130104251" \|<br>"20130106576" \|<br>"20130119130" \|<br>"20130130614" \|<br>"20130144793" \|<br>"20130171929" \|<br>"20130179351" \|<br>"20130185772" \|<br>"20130191279" \|<br>"20130200999" \|<br>"20130216108" \|<br>"20130226791" \|<br>"20130226796" \|<br>"20130232082" \|<br>"20130238894" \|<br>"20130282360" \|<br>"20130303085" \|<br>"20130304651" \|<br>"20130312082" \|<br>"20130314593" \|<br>"20130344857" \|<br>"20140002238" \| | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | "20140019352" \|<br>"20140027506" \|<br>"20140032409" \|<br>"20140032410" \|<br>"20140040120" \|<br>"20140040139" \|<br>"20140040147" \|<br>"20140047235" \|<br>"20140067690" \|<br>"20140074637").PN.<br>OR ("20140074655" \|<br>"20140081720" \|<br>"20140095227" \|<br>"20140138435" \|<br>"20140171034" \|<br>"20140171039" \|<br>"20140172700" \|<br>"20140180851" \|<br>"20140208112" \|<br>"20140214674" \|<br>"20140229375" \|<br>"20140245391" \|<br>"20140256251" \|<br>"20140258099" \|<br>"20140258113" \|<br>"20140258125" \|<br>"20140274179" \|<br>"20140279479" \|<br>"20140337235" \|<br>"20140339315" \|<br>"20140346860" \|<br>"20140365780" \|<br>"20140379361" \|<br>"20150012444" \|<br>"20150032635" \|<br>"20150071486" \|<br>"20150088757" \|<br>"20150089586" \|<br>"20150134452" \|<br>"20150140960" \|<br>"20150154595" \|<br>"20150170138" \|<br>"20150178724" \|<br>"20150186871" \|<br>"20150205379" \|<br>"20150235211" \|<br>"20150302409" \|<br>"20150317626" \|<br>"20150332266" \|<br>"20150339474" \|<br>"20150371234" \|<br>"20160012465" \|<br>"20160026997" \|<br>"20160048913" \|<br>"20160055480" \|<br>"20160057619" \|<br>"20160065370" \|<br>"20160087957" \| | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | "20160092696" \|<br>"20160148193" \|<br>"20160232523" \|<br>"20160239672" \|<br>"20160253651" \|<br>"20160255072" \|<br>"20160267486" \|<br>"20160277383" \|<br>"20160277388" \|<br>"20160307187" \|<br>"20160307189" \|<br>"20160314472" \|<br>"20160330027" \|<br>"20160335531" \|<br>"20160379217" \|<br>"20170004502" \|<br>"20170011395" \|<br>"20170011406" \|<br>"20170017957" \|<br>"20170017964" \|<br>"20170024716" \|<br>"20170039566" \|<br>"20170041759" \|<br>"20170068950" \|<br>"20170103388" \|<br>"20170104739" \|<br>"20170109509" \|<br>"20170109730" \|<br>"20170116447" \|<br>"20170124568" \|<br>"20170140379" \|<br>"20170154328" \|<br>"20170154333" \|<br>"20170180134" \|<br>"20170221047" \|<br>"20170230189" \|<br>"20170237301" \|<br>"20170289127" \|<br>"20170295013" \|<br>"20170316696" \|<br>"20170317834" \|<br>"20170330173" \|<br>"20170374070" \|<br>"20180034507" \|<br>"20180039986").PN.<br>OR ("20180068316" \|<br>"20180129945" \|<br>"20180160255" \|<br>"20180191501" \|<br>"20180205712" \|<br>"20180240106" \|<br>"20180254909" \|<br>"20180268132" \|<br>"20180270214" \|<br>"20180294959" \|<br>"20180300716" \|<br>"20180302396" \|<br>"20180315050" \| | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | "20180316666" \|<br>"20180322486" \|<br>"20180359100" \|<br>"20190014107" \|<br>"20190019375" \|<br>"20190036678" \|<br>"20190238517" \|<br>"4683553" \| "4827113" \|<br>"4910773" \| "5036461" \|<br>"5363448" \| "5377270" \|<br>"5533126" \| "5592553" \|<br>"5616901" \| "5666415" \|<br>"5764789" \| "5768373" \|<br>"5778072" \| "5796827" \|<br>"5832090" \| "5883810" \|<br>"5901874" \| "5929413" \|<br>"5960411" \| "6021203" \|<br>"6049328" \| "6058373" \|<br>"6061666" \| "6105013" \|<br>"6199114" \| "6199762" \|<br>"6216227" \| "6227447" \|<br>"6282522" \| "6324271" \|<br>"6342844" \| "6367011" \|<br>"6402028" \| "6438550" \|<br>"6501847" \| "6631197" \|<br>"6641050" \| "6655585" \|<br>"6662020" \| "6721706" \|<br>"6731778" \| "6779115" \|<br>"6792533" \| "6829711" \|<br>"6834271" \| "6834795" \|<br>"6852031" \| "6865547" \|<br>"6873260" \| "6877656" \|<br>"6889198" \| "6905411" \|<br>"6910627" \| "6971031" \|<br>"6990588" \| "7006986" \|<br>"7085931" \| "7127605" \|<br>"7128274" \| "7140550" \|<br>"7152045" \| "7165727" \|<br>"7175076" \| "7202773" \|<br>"7206806" \| "7232073" \|<br>"7246752" \| "7254569" \|<br>"7263507" \| "7270276" \|<br>"7278025" \| "7287692" \|<br>"7290709" \| "7306143" \|<br>"7319986" \| "7325132" \|<br>"7373515" \| "7374099" \|<br>"7375616" \| "7380710" \|<br>"7424977" \| "7453439" \|<br>"7472829" \| "7487357" \|<br>"7568631" \| "7584153" \|<br>"7597250" \| "7628322" \|<br>"7652578" \| "7689832" \|<br>"7703142" \| "7748609" \|<br>"7748617" \| "7748636" \|<br>"7762457" \| "7789302" \|<br>"7793851" \|<br>"7796013").PN. OR<br>("7801799" \| "7801829" | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | \| "7805755" \| "7809643"<br>\| "7827115" \| "7828214"<br>\| "7848746" \| "7882553"<br>\| "7900048" \| "7908216"<br>\| "7922082" \| "7933589"<br>\| "7949559" \| "7954716"<br>\| "7954723" \| "7962369"<br>\| "7993197" \| "8005426"<br>\| "8010405" \| "8041954"<br>\| "8060012" \| "8074877"<br>\| "8082450" \| "8095113"<br>\| "8099332" \| "8103249"<br>\| "8108687" \| "8127143"<br>\| "8135648" \| "8140010"<br>\| "8141136" \| "8150321"<br>\| "8150767" \| "8186602"<br>\| "8196131" \| "8215563"<br>\| "8224753" \| "8232879"<br>\| "8233841" \| "8245292"<br>\| "8249654" \| "8266451"<br>\| "8285329" \| "8302872"<br>\| "8312519" \| "8316237"<br>\| "8332272" \| "8365988"<br>\| "8369960" \| "8371501"<br>\| "8381307" \| "8391719"<br>\| "8417231" \| "8439271"<br>\| "8475367" \| "8489112"<br>\| "8511542" \| "8559872"<br>\| "8566916" \| "8567670"<br>\| "8572386" \| "8577810"<br>\| "8583454" \| "8589335"<br>\| "8594730" \| "8615468"<br>\| "8620218" \| "8667285"<br>\| "8723941" \| "8726405"<br>\| "8740073" \| "8750514"<br>\| "8752189" \| "8794509"<br>\| "8799668" \| "8806592"<br>\| "8807440" \| "8811892"<br>\| "8814039" \| "8814052"<br>\| "8818867" \| "8850538"<br>\| "8861733" \| "8880027"<br>\| "8888002" \| "8898088"<br>\| "8934837" \| "8977569"<br>\| "8994498" \| "9004365"<br>\| "9038894" \| "9042814"<br>\| "9047531" \| "9069976"<br>\| "9081948" \| "9104853"<br>\| "9118663" \| "9122964"<br>\| "9129280" \| "9152832"<br>\| "9203800" \| "9209867"<br>\| "9251330" \| "9251518"<br>\| "9258715" \| "9270337"<br>\| "9306626" \| "9306942"<br>\| "9324066" \| "9324067"<br>\| "9332587" \| "9338622"<br>\| "9373141" \| "9379841"<br>\| "9413430" \| "9413768"<br>\| "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<br>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 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 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 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 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 | 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**




**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

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**<br>Substitute for Form PTO-875 | Application or Docket Number<br>17/528,073 | Filing Date<br>11/16/2021 | ☐ To be Mailed |
|---|---|---|---|

**ENTITY:** ☐ LARGE ☑ SMALL ☐ MICRO

## APPLICATION AS FILED - PART I

| FOR | (Column 1)<br>NUMBER FILED | (Column 2)<br>NUMBER EXTRA | | RATE ($) | FEE ($) |
|---|---|---|---|---|---|
| ☐ BASIC FEE<br>(37 CFR 1.16(a), (b), or (c)) | N/A | N/A | | N/A | |
| ☐ SEARCH FEE<br>(37 CFR 1.16(k), (i), or (m)) | N/A | N/A | | N/A | |
| ☐ EXAMINATION FEE<br>(37 CFR 1.16(o), (p), or (q)) | N/A | N/A | | N/A | |
| TOTAL CLAIMS<br>(37 CFR 1.16(i)) | minus 20 = | * | | x $50 = | |
| INDEPENDENT CLAIMS<br>(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

| | | (Column 1) | | (Column 2) | (Column 3) | | | |
|---|---|---|---|---|---|---|---|---|
| AMENDMENT | 04/22/2022 | CLAIMS REMAINING AFTER AMENDMENT | | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA | | RATE ($) | ADDITIONAL FEE ($) |
| | Total<br>(37 CFR 1.16(i)) | * 72 | Minus | ** 20 | = 52 | | x $50 = | 2600 |
| | Independent<br>(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 |

| | | (Column 1) | | (Column 2) | (Column 3) | | | |
|---|---|---|---|---|---|---|---|---|
| AMENDMENT | | CLAIMS REMAINING AFTER AMENDMENT | | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA | | RATE ($) | ADDITIONAL FEE ($) |
| | Total<br>(37 CFR 1.16(i)) | * | Minus | ** | = | | x $0 = | |
| | Independent<br>(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.*

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.

## 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;

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.

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:

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. (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

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;

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;

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.

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.

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,

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.

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

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.

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:

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,

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.

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;

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;

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.

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

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

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:

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;

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.

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.

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

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.

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

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:<br>37 CFR 1.19 (Document supply fees)<br>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<br>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<br>51e693c8b0b73d0b1f55fc5df0ef8df0fd49e46d | no | 1 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 3 | Fee Worksheet (SB06) | fee-info.pdf | 40435<br>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.**

| | |
|---|---|
| **Doc Code: DIST.E.FILE**<br>**Document Description: Electronic Terminal Disclaimer - Filed** | PTO/SB/25<br>PTO/SB/26<br>U.S. Patent and Trademark Office<br>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<br>32f0d2b9f03819f638cc9df5558feb66ad88c444 | no | 3 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 2 | Fee Worksheet (SB06) | fee-info.pdf | 37770<br>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.**

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/

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

**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,

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.

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.L.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<br>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.**

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 | | |

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

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 |

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 |

[Page 2 of 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.

# 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<br>ed1691b6999d3775ccd7d3f96aa1fd4e9586e24d | no | 5 |

**Warnings:**

| | | | | | |
|---|---|---|---|---|---|
| **Information:** | | | | | |
| 2 | Request for Corrected Filing Receipt | WYAT-0002USD1C1C1C1C1C1_aia0041_Request_to_Change_Applicant.pdf | 212116<br>af2eeefc8fd99dad1b6d78ec1f20b7b21570860e | no | 2 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 3 | Assignee showing of ownership per 37 CFR 3.73 | WYAT-0002USD1C1C1C1C1C1_aia0096_Statement_under_3_73c.pdf | 195895<br>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.**

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

OC000000132585386

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

**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,

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.

## 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

AMENDMENT A

| | (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($) | OTHER THAN SMALL ENTITY ADDITIONAL FEE($) |
|---|---|---|---|---|---|---|---|---|---|
| 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 | |

AMENDMENT B

| | (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($) | OTHER THAN SMALL ENTITY ADDITIONAL FEE($) |
|---|---|---|---|---|---|---|---|---|---|
| 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.

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)*: **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(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

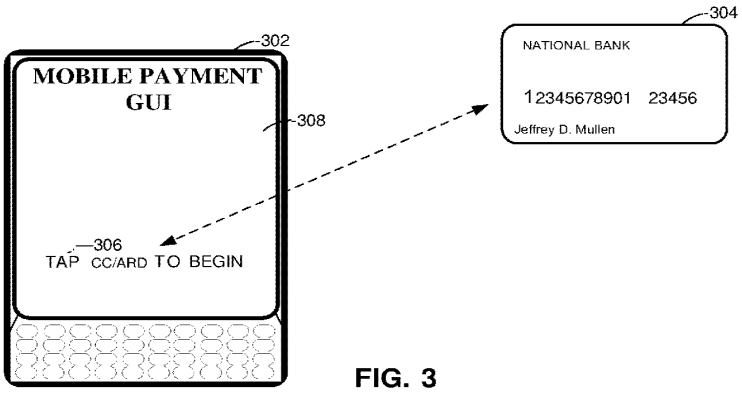



FIG. 3

(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

# 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.

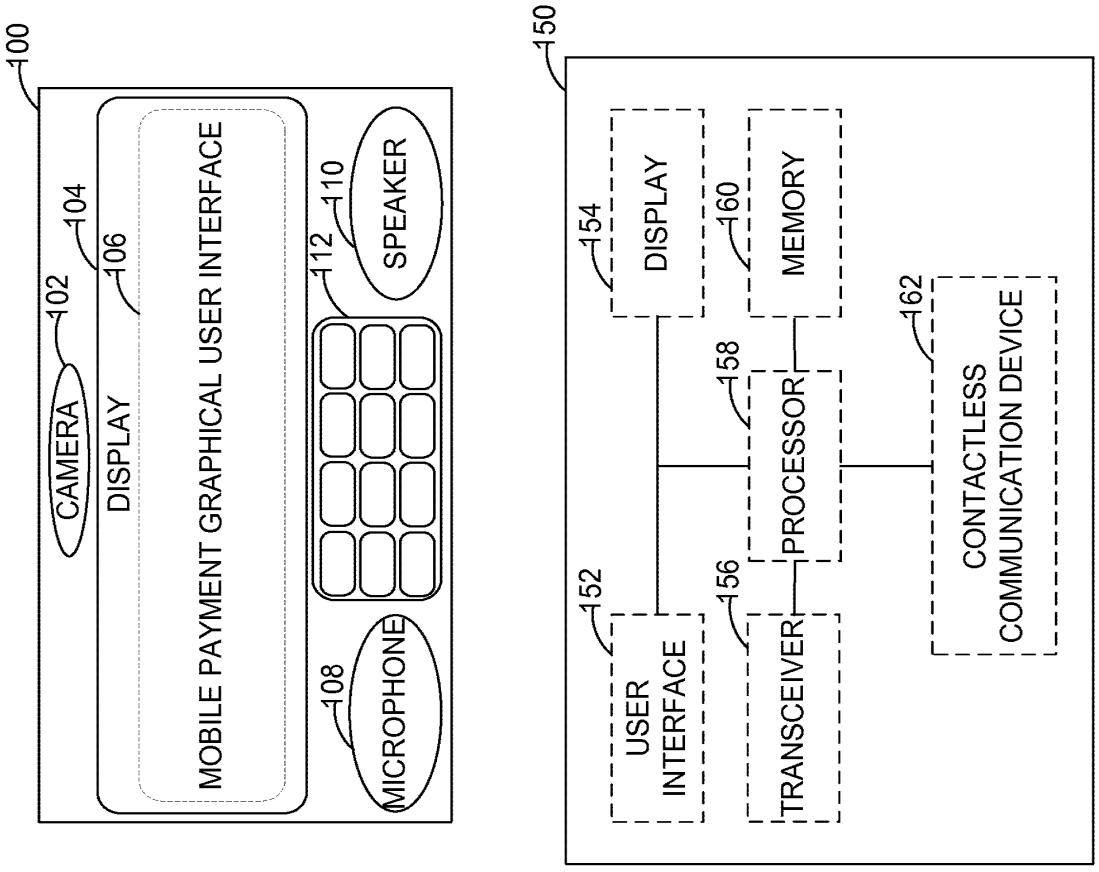

100
CAMERA
102
DISPLAY
104
MOBILE PAYMENT GRAPHICAL USER INTERFACE
106
MICROPHONE
108
SPEAKER
110
112
150
USER INTERFACE
152
TRANSCEIVER
156
PROCESSOR
158
DISPLAY
154
MEMORY
160
CONTACTLESS COMMUNICATION DEVICE
162

FIG. 1

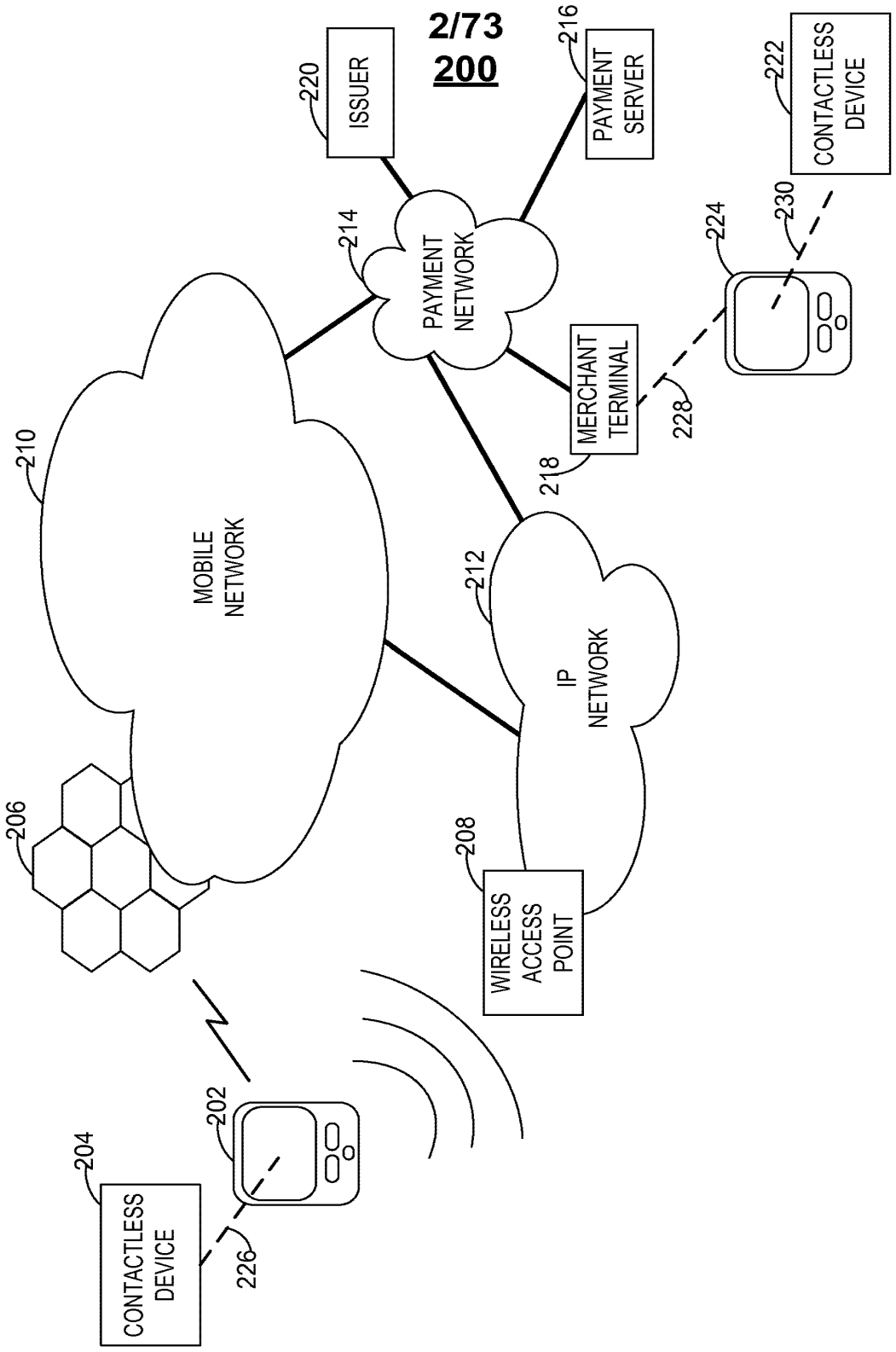

2/73
200
ISSUER
220
PAYMENT SERVER
216
CONTACTLESS DEVICE
222
PAYMENT NETWORK
214
MOBILE NETWORK
210
MERCHANT TERMINAL
218
228
224
230
IP NETWORK
212
206
208
WIRELESS ACCESS POINT
202
204
CONTACTLESS DEVICE
226

FIG. 2

3/73
300

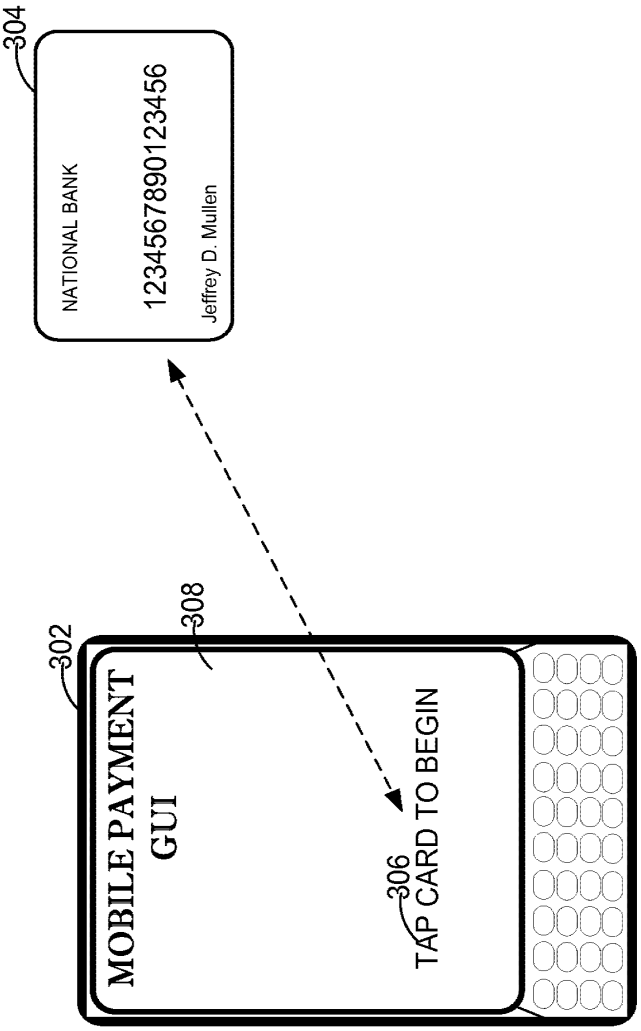

304
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
308
302
MOBILE PAYMENT
GUI
306
TAP CARD TO BEGIN

FIG. 3

4/73

400


CARD DETECTION
AIRLINE CARD
TRAVEL CARD
BANK CARD
404
HEALTHCARE CARD
IDENTIFICATION CARD
REWARDS CARD
BACK
406
CONTINUE
408

FIG. 4

5/73

500

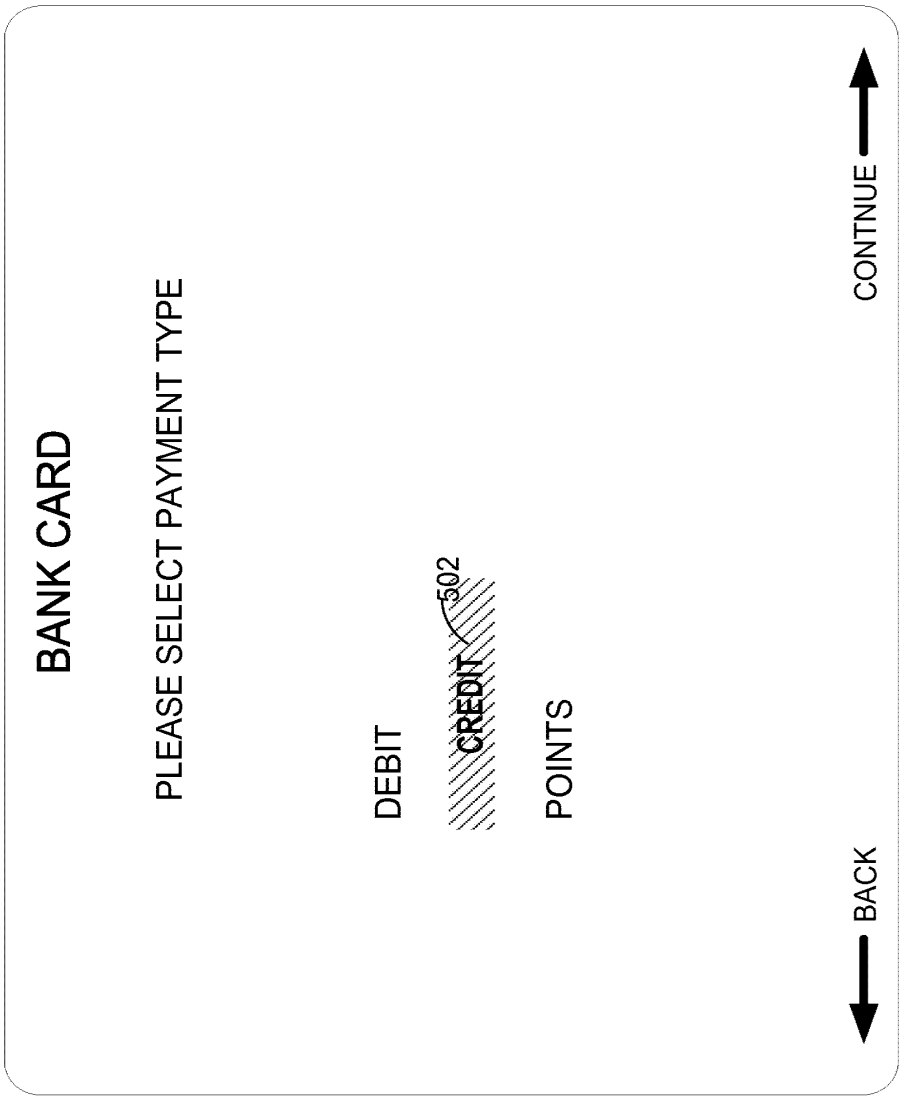

BANK CARD
PLEASE SELECT PAYMENT TYPE
DEBIT
CREDIT
502
POINTS
CONTNUE
BACK

FIG. 5

6/73

600

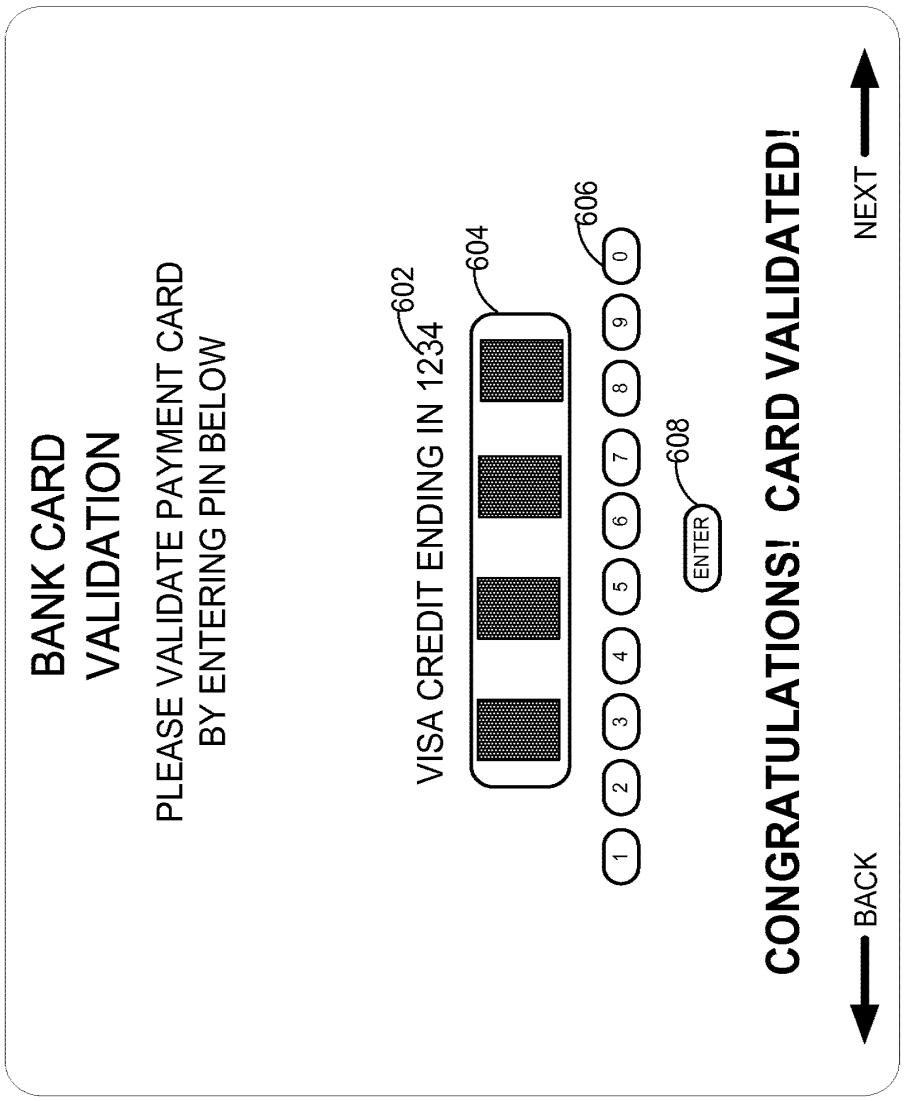

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING PIN BELOW
VISA CREDIT ENDING IN 1234
602
604
606
1
2
3
4
5
6
7
8
9
0
ENTER
608
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 6

7/73
700

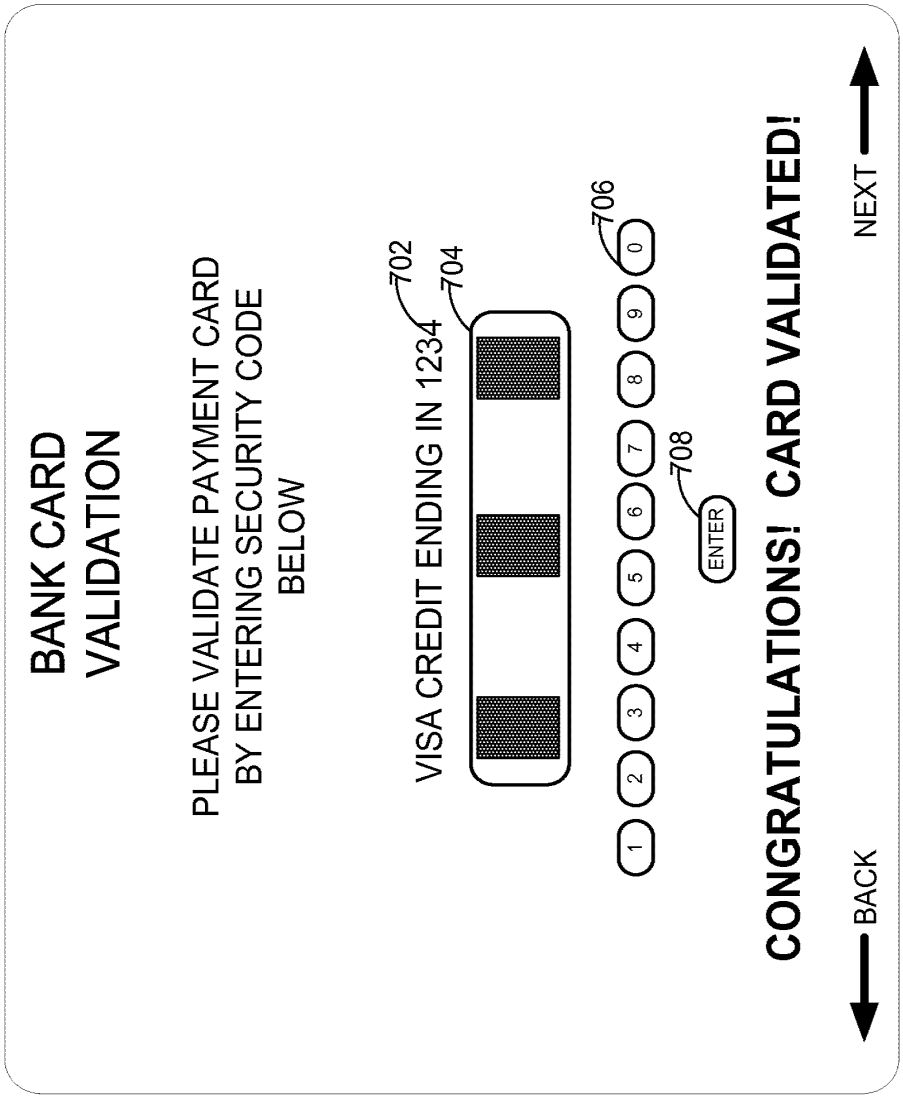

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING SECURITY CODE
BELOW
VISA CREDIT ENDING IN 1234
702
704
706
1
2
3
4
5
6
7
8
9
0
ENTER
708
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 7

8/73

800

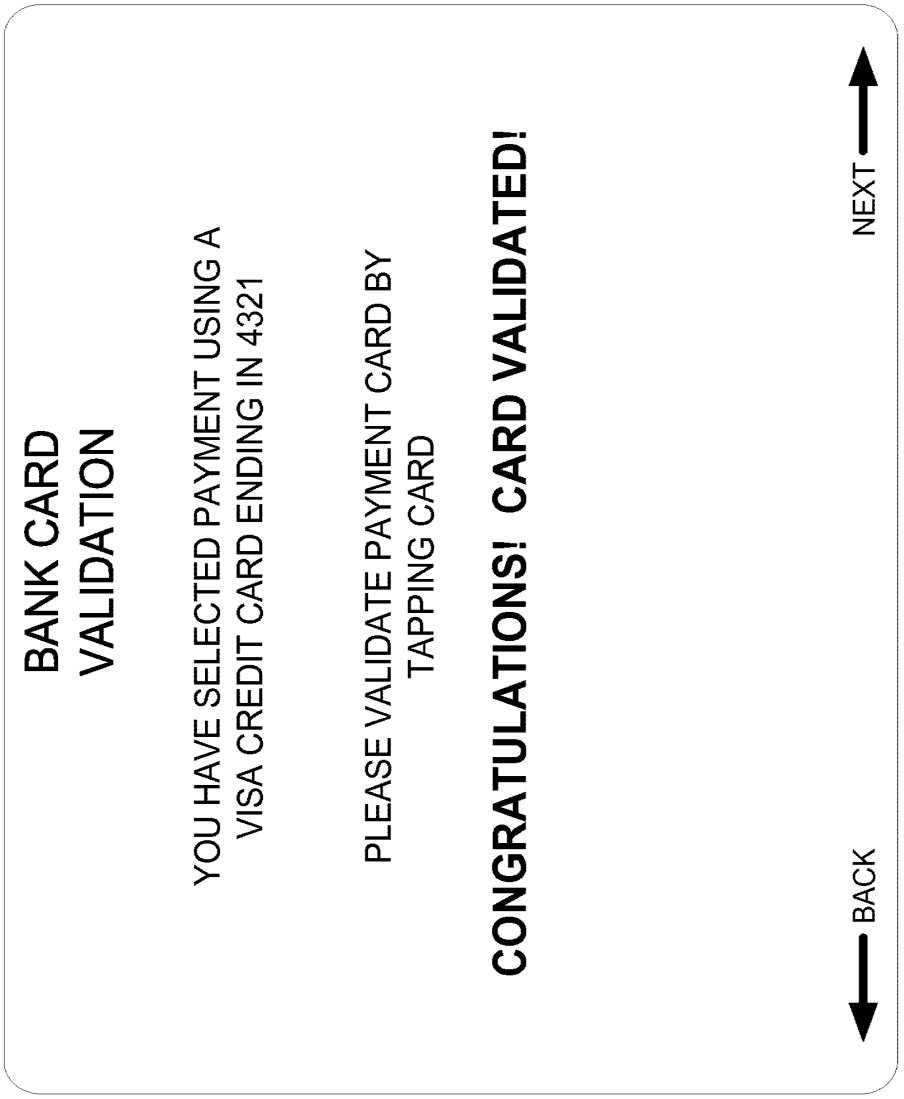

BANK CARD VALIDATION
YOU HAVE SELECTED PAYMENT USING A VISA CREDIT CARD ENDING IN 4321
PLEASE VALIDATE PAYMENT CARD BY TAPPING CARD
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 8

900

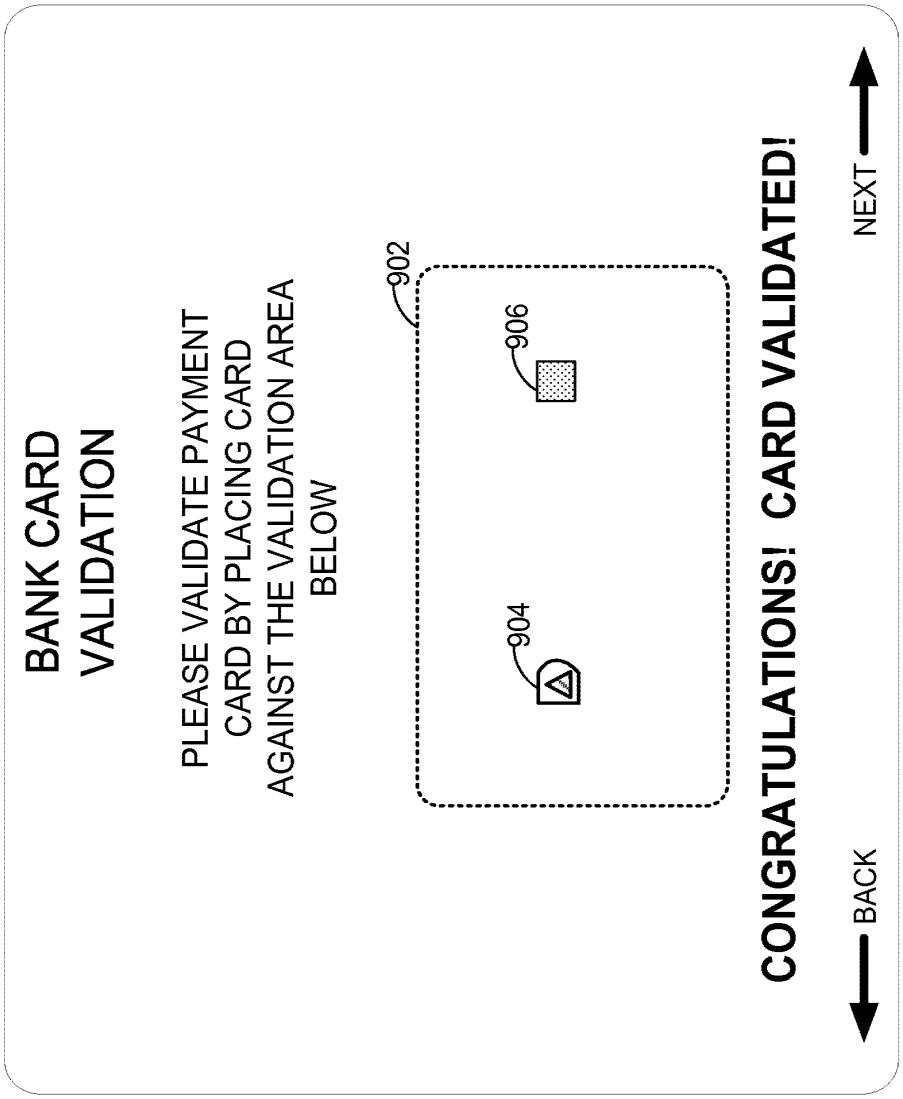

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT
CARD BY PLACING CARD
AGAINST THE VALIDATION AREA
BELOW
902
906
904
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 9

1000

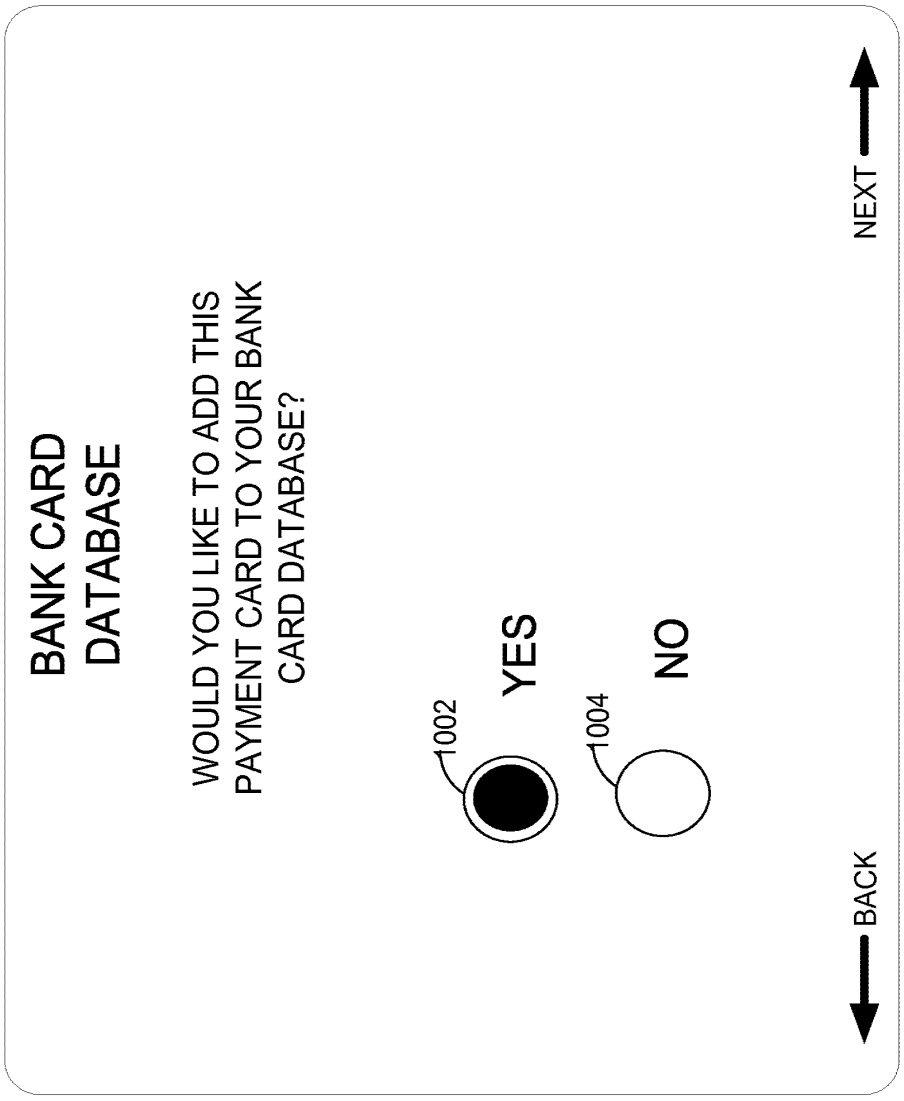

BANK CARD DATABASE
WOULD YOU LIKE TO ADD THIS PAYMENT CARD TO YOUR BANK CARD DATABASE?
1002
YES
1004
NO
NEXT
BACK

FIG. 10

11/73
1100

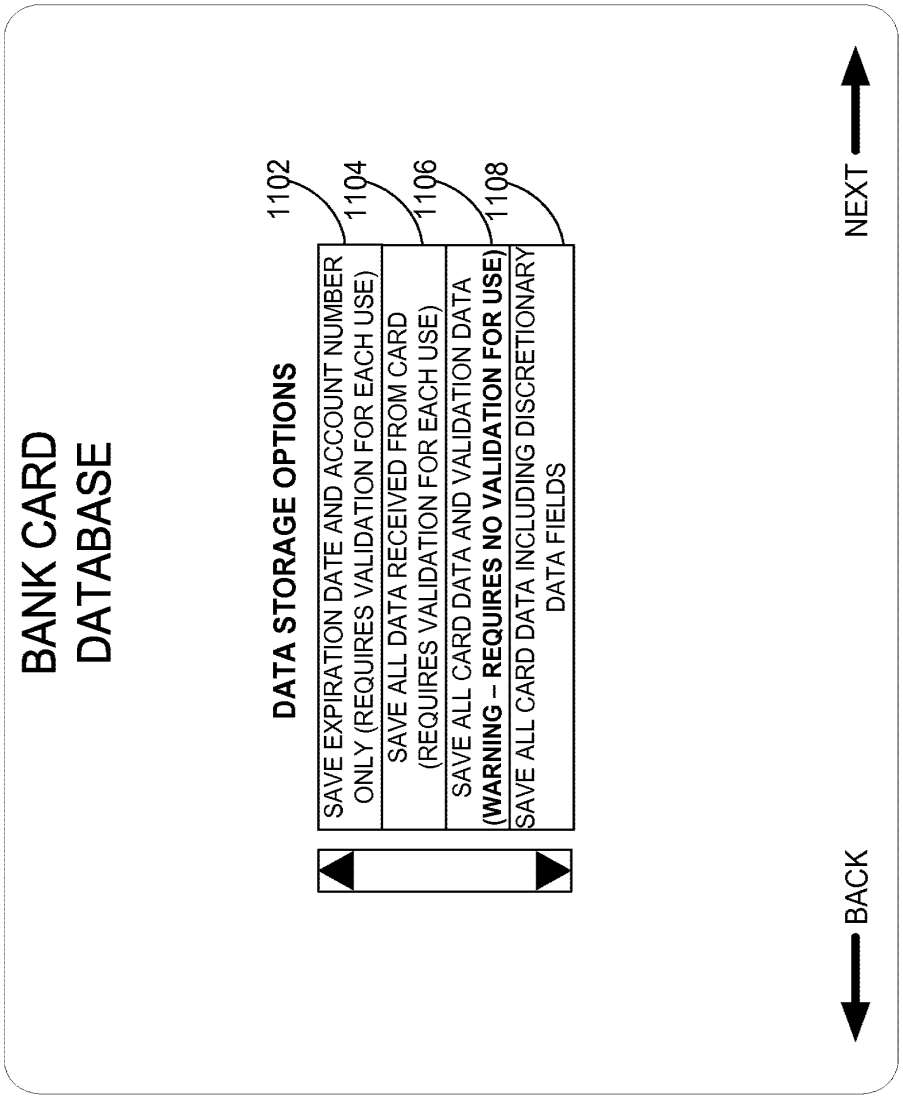



FIG. 11

12/73
1200

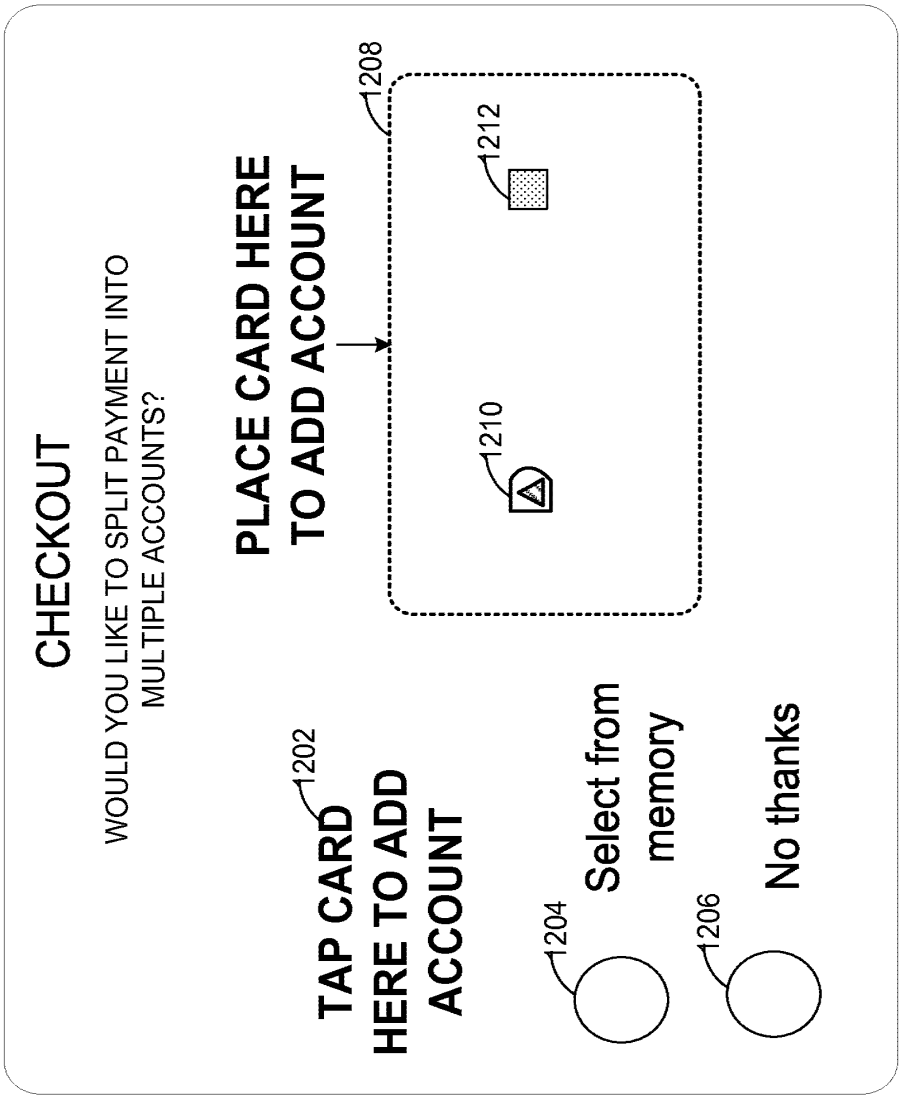



FIG. 12

13/73
1300

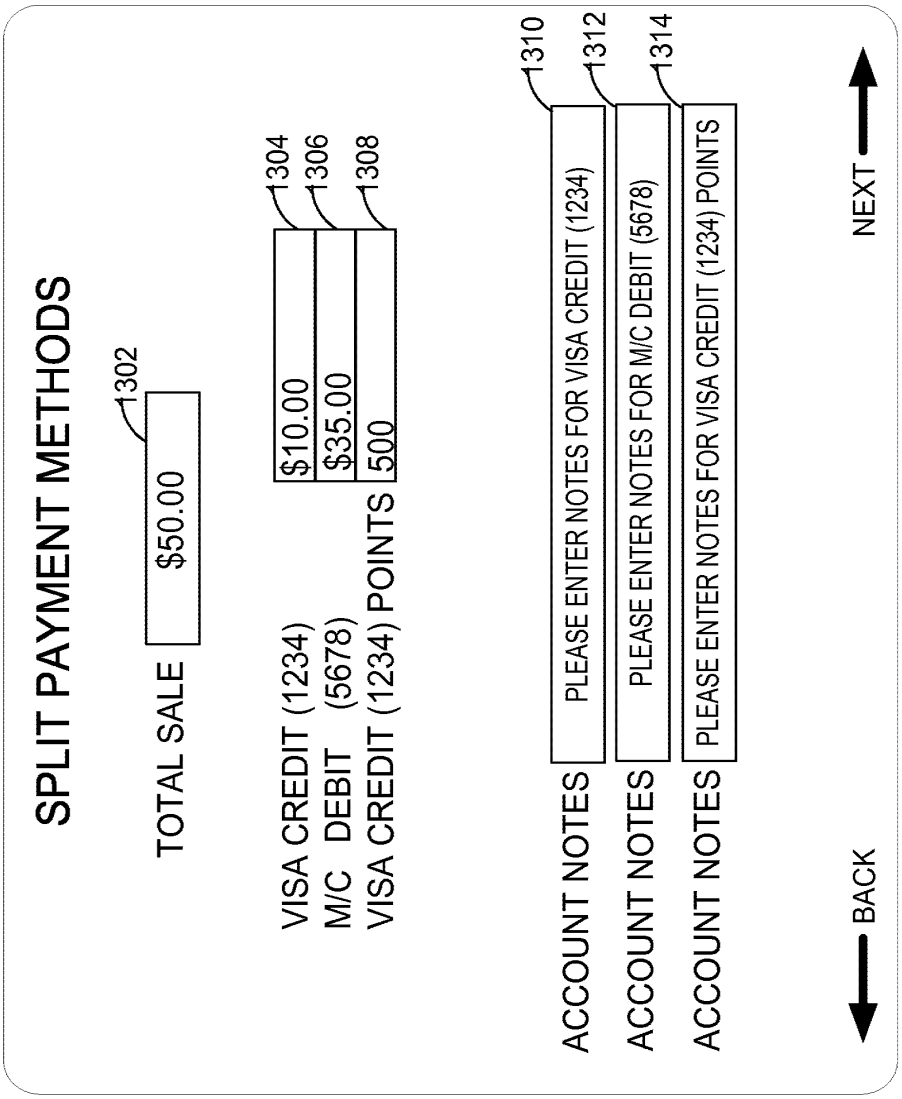



FIG. 13

14/73
1400

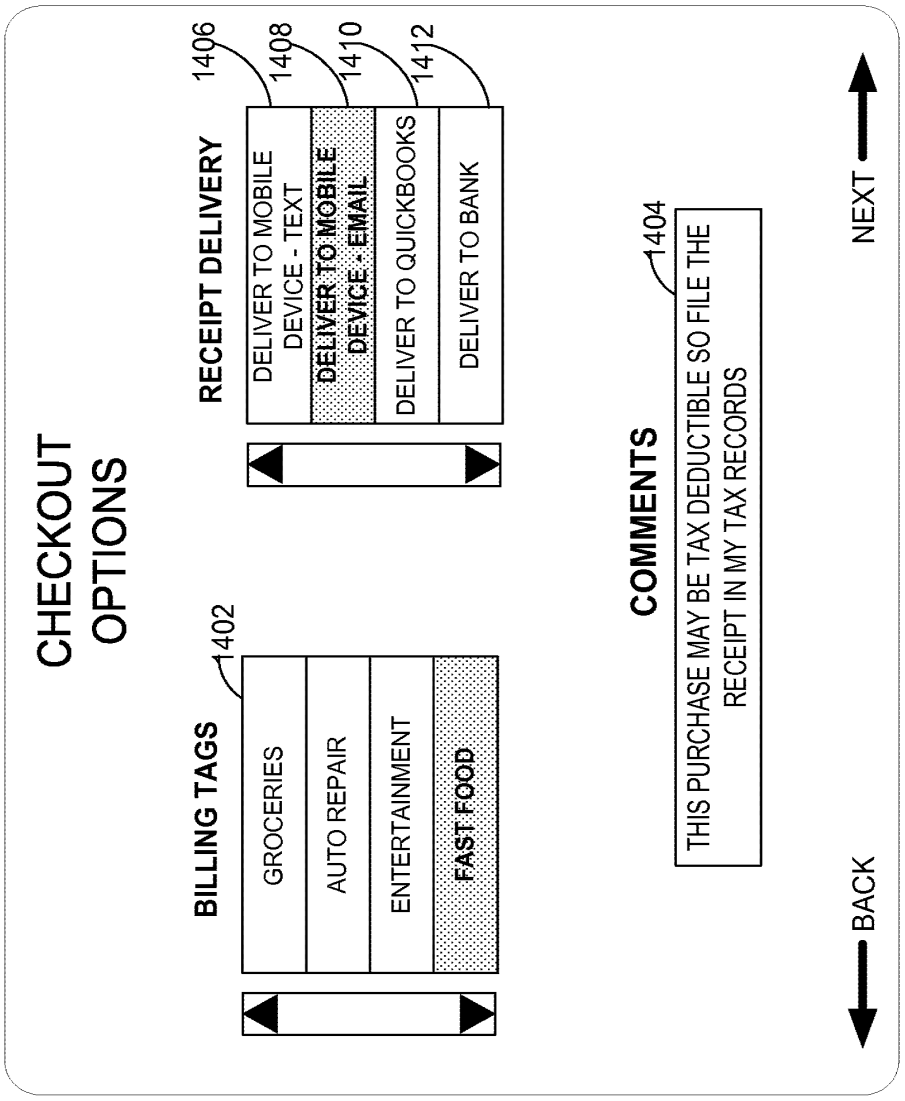



FIG. 14

1500

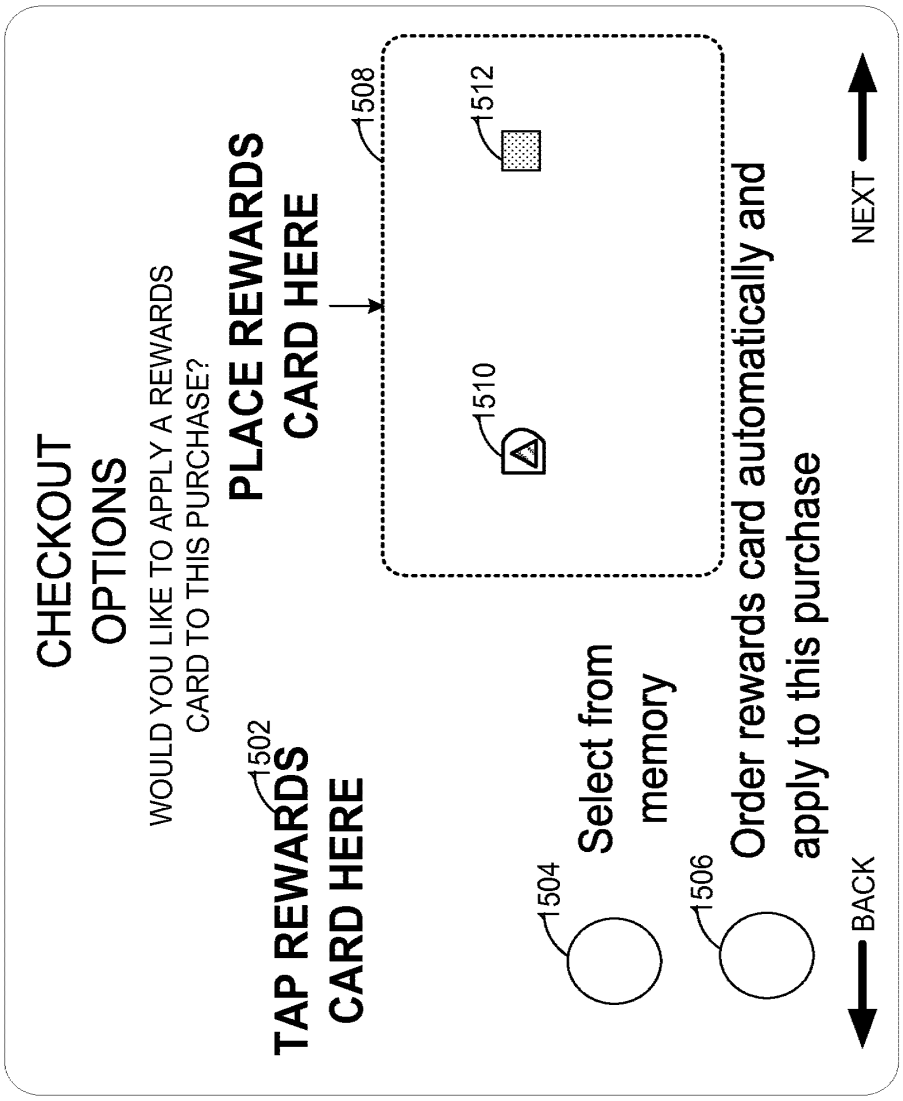

CHECKOUT OPTIONS
WOULD YOU LIKE TO APPLY A REWARDS CARD TO THIS PURCHASE?
TAP REWARDS CARD HERE
1502
PLACE REWARDS CARD HERE
1508
1512
1510
1504
Select from memory
1506
Order rewards card automatically and apply to this purchase
BACK
NEXT

FIG. 15

1600

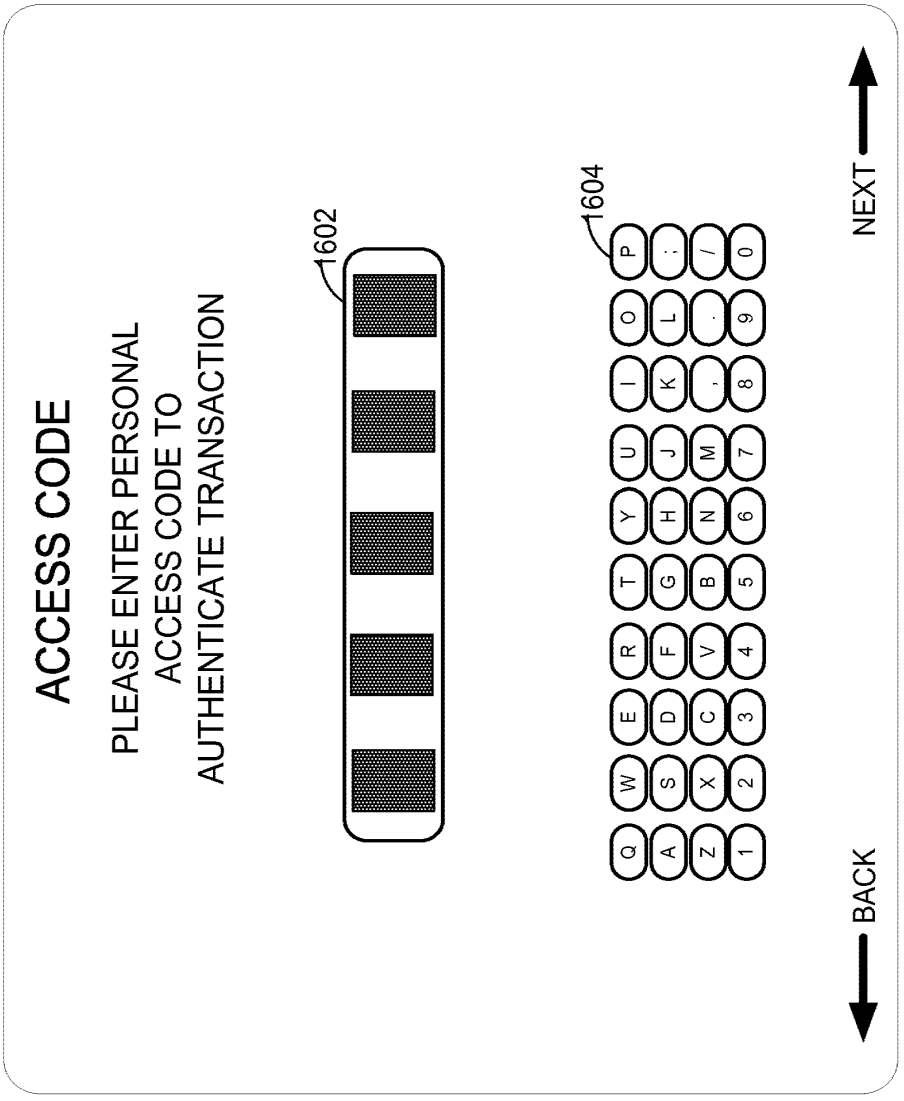

ACCESS CODE
PLEASE ENTER PERSONAL ACCESS CODE TO AUTHENTICATE TRANSACTION
1602
1604
NEXT
BACK
Q A Z 1
W S X 2
E D C 3
R F V 4
T G B 5
Y H N 6
U J M 7
I K , 8
O L . 9
P ; / 0

FIG. 16

17/73
1700

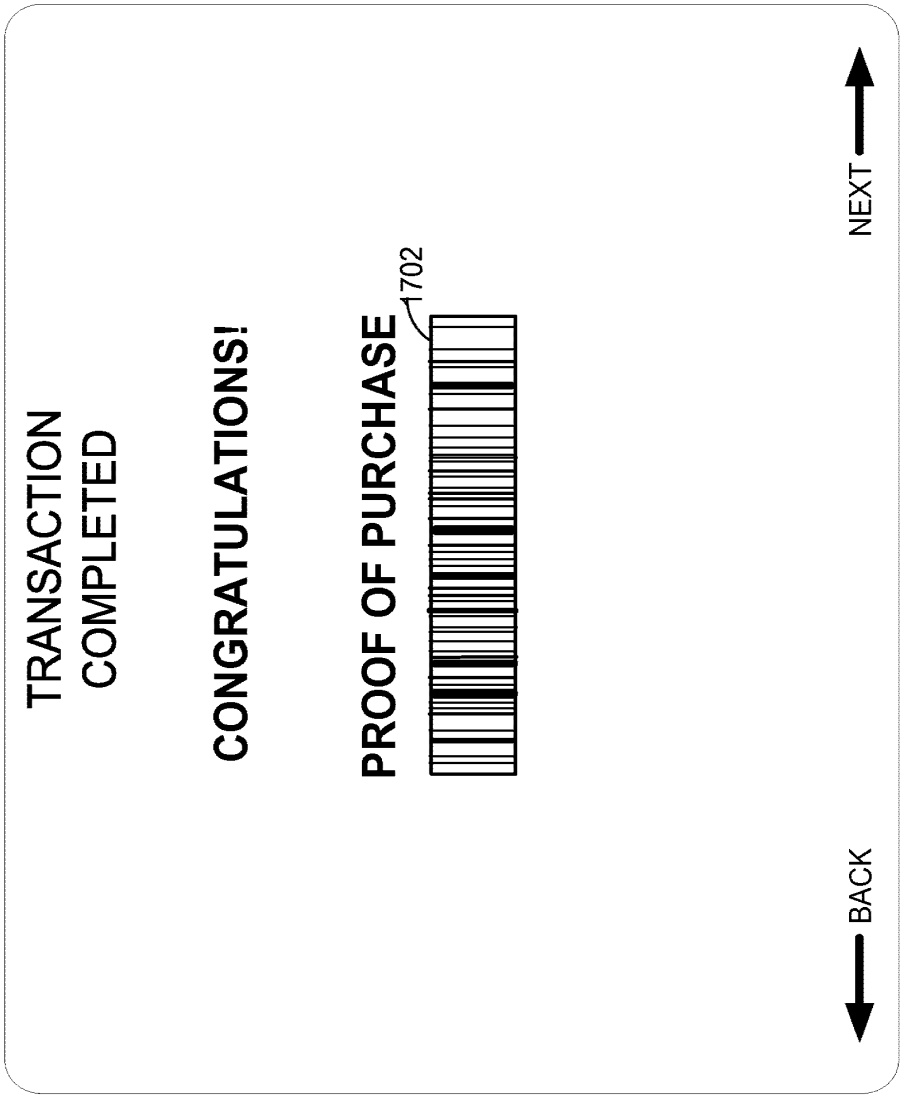



FIG. 17

1800

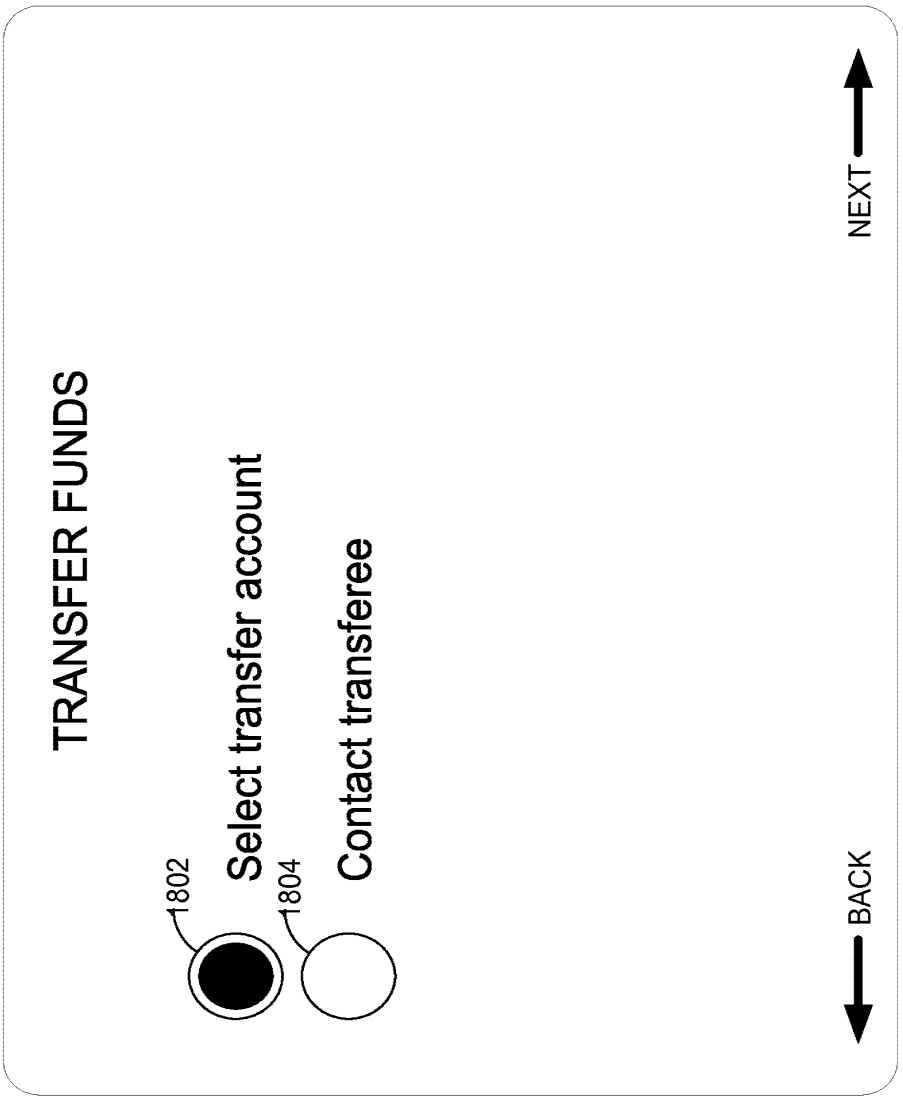

TRANSFER FUNDS
Select transfer account
Contact transferee
1802
1804
NEXT
BACK

FIG. 18

19/73
1900

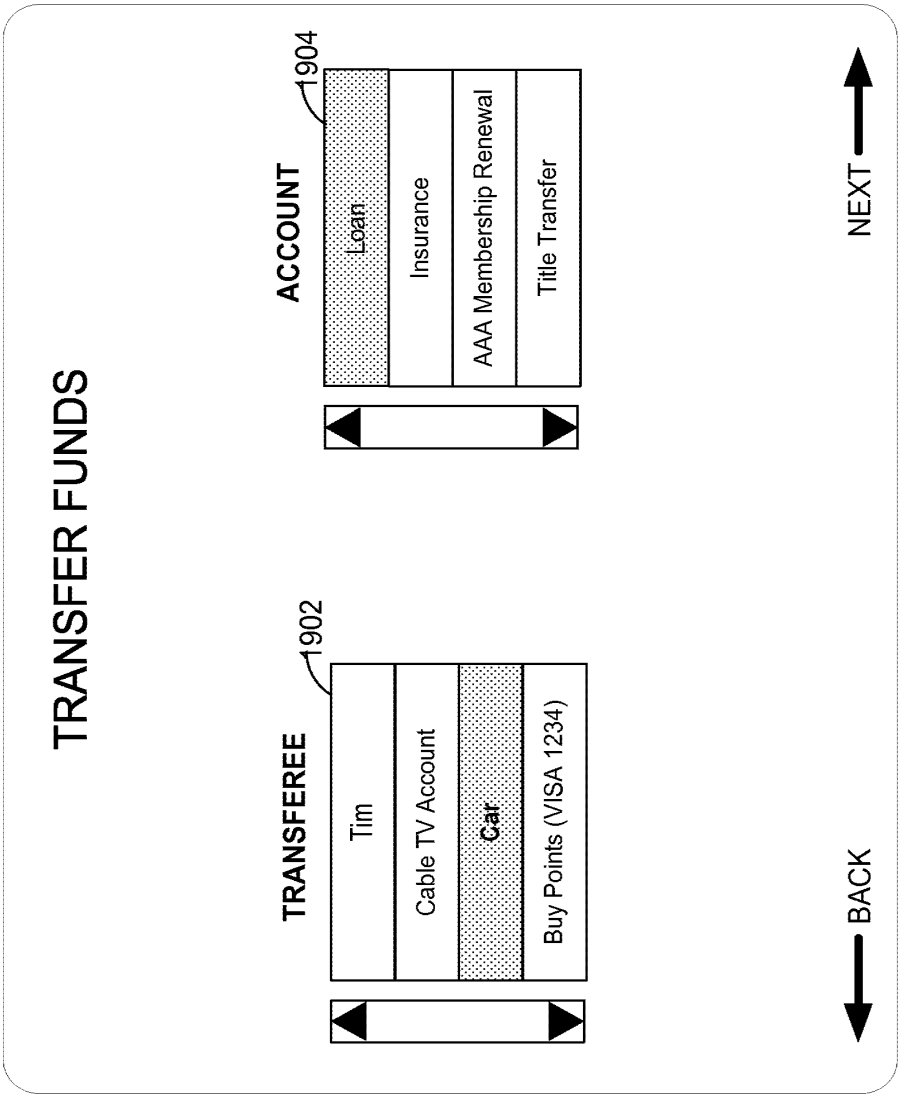



FIG. 19

**20/73**
**2000**

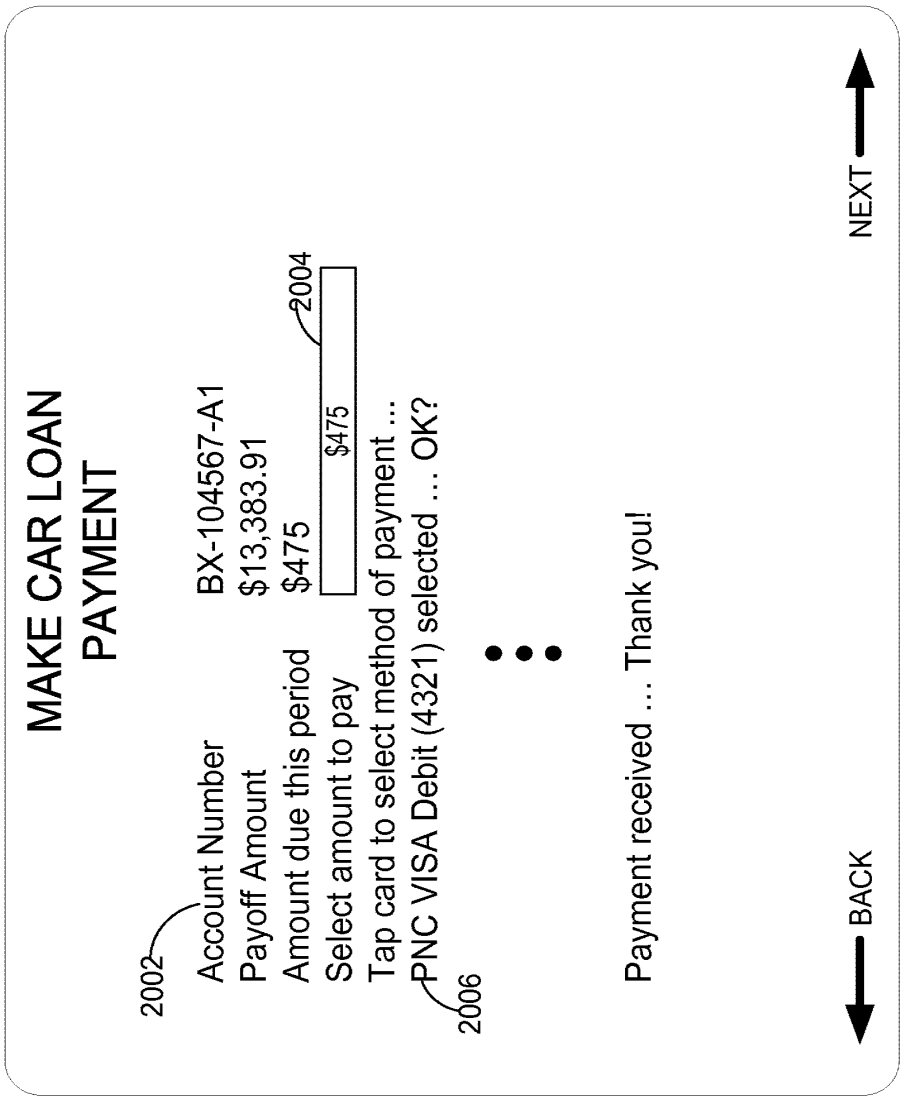



FIG. 20

2100

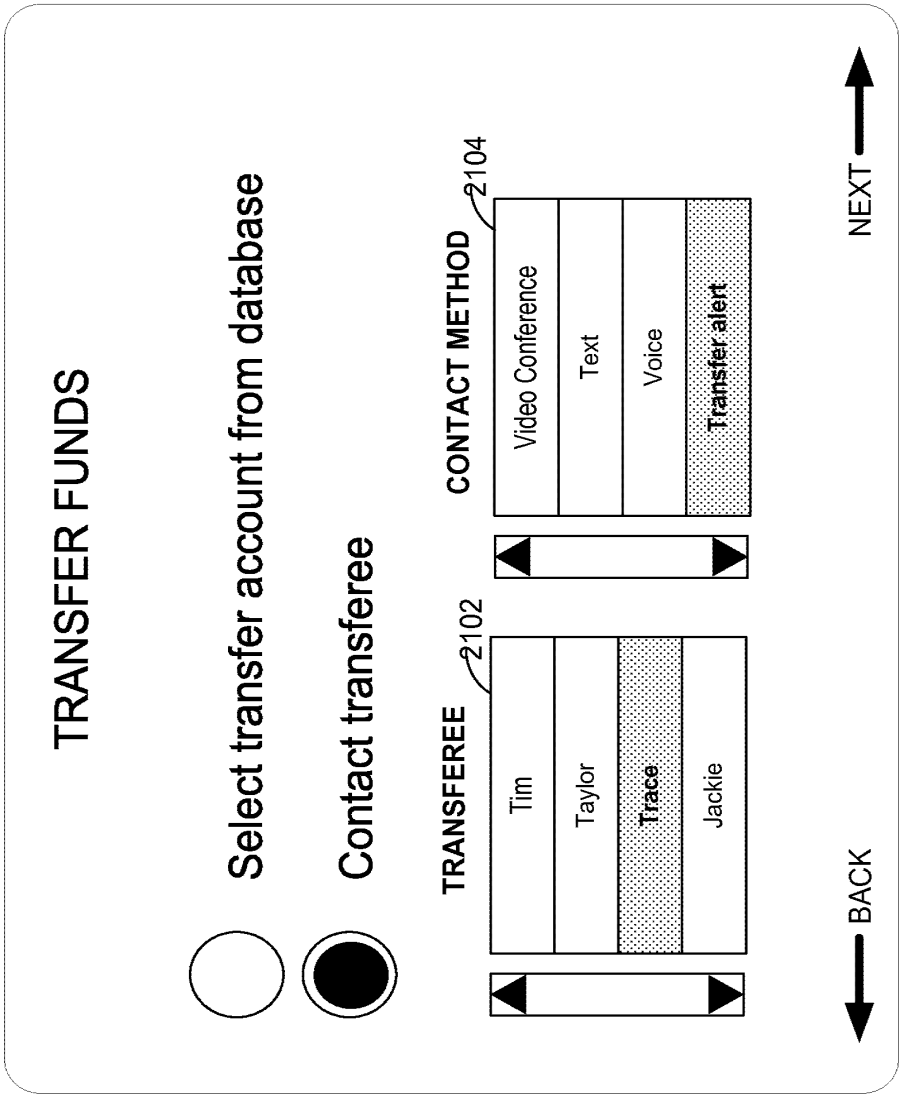

TRANSFER FUNDS
Select transfer account from database
Contact transferee
TRANSFEREE
2102
Tim
Taylor
Trace
Jackie
CONTACT METHOD
2104
Video Conference
Text
Voice
Transfer alert
BACK
NEXT

FIG. 21

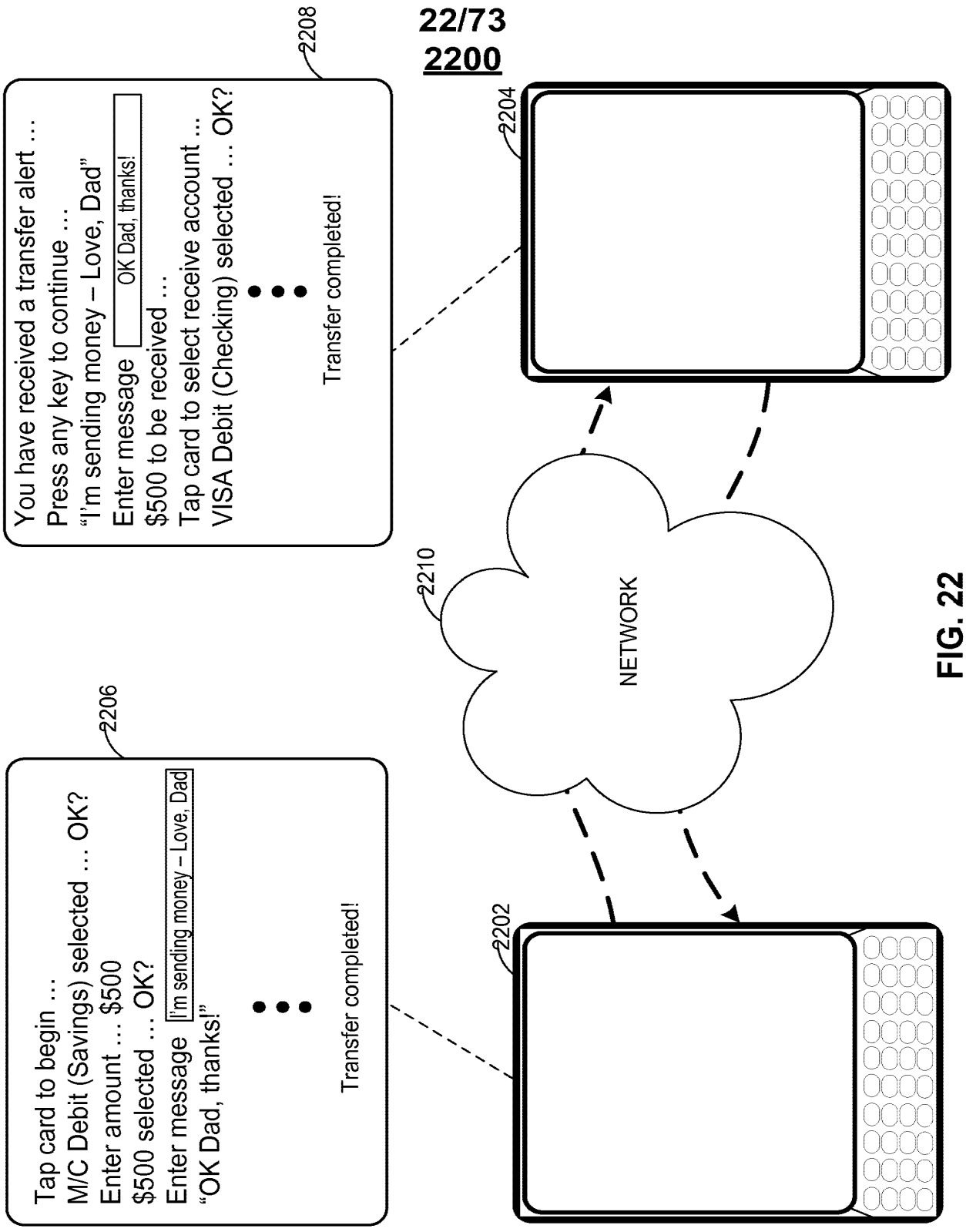

2200
2202
2204
2206
2208
2210
NETWORK
Tap card to begin ...
M/C Debit (Savings) selected ... OK?
Enter amount ... $500
$500 selected ... OK?
Enter message I'm sending money – Love, Dad
"OK Dad, thanks!"
Transfer completed!
You have received a transfer alert ...
Press any key to continue ...
"I'm sending 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!

FIG. 22

2300

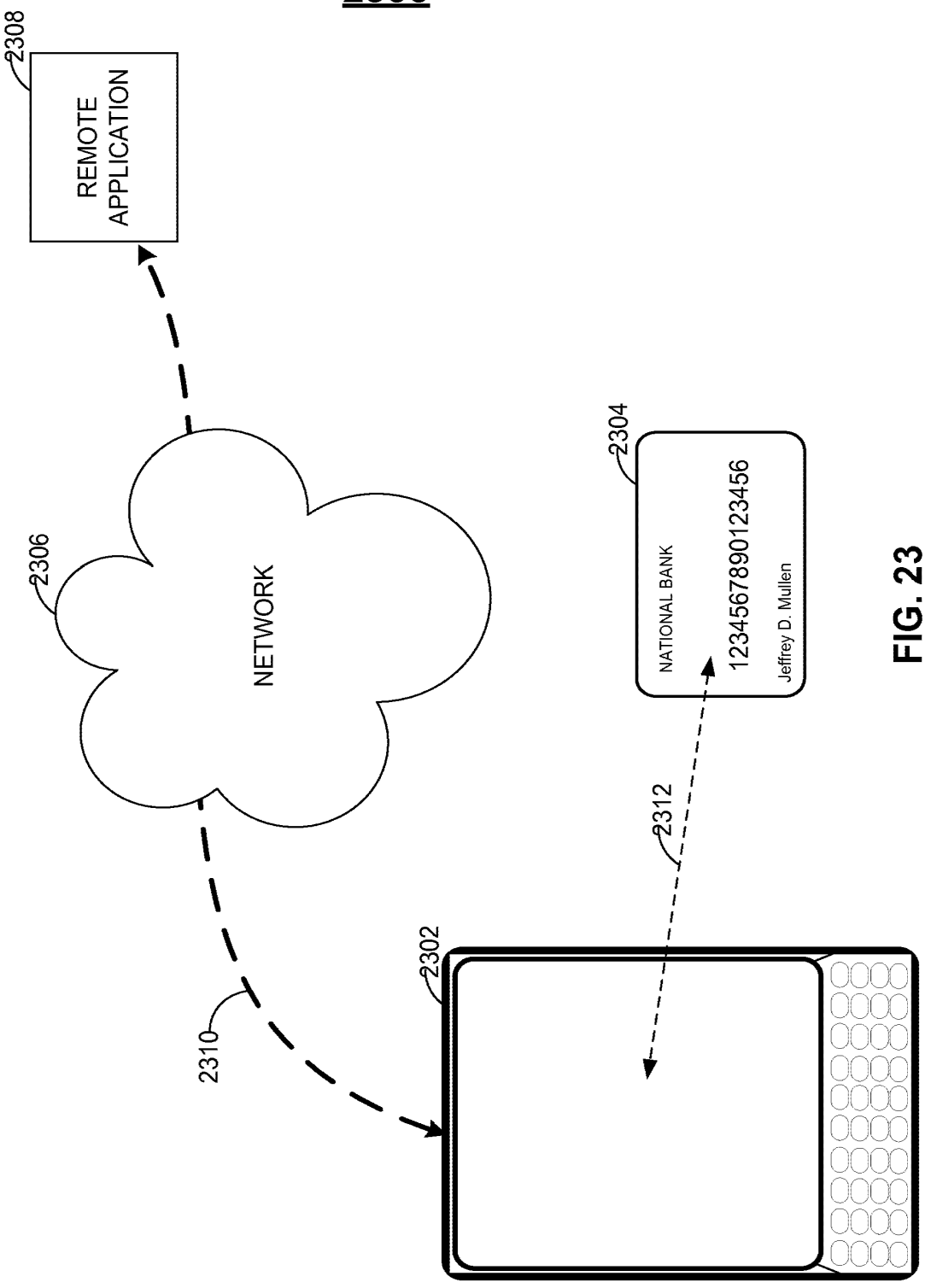

2308
REMOTE APPLICATION
2306
NETWORK
2304
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
2312
2302
2310

FIG. 23

2400

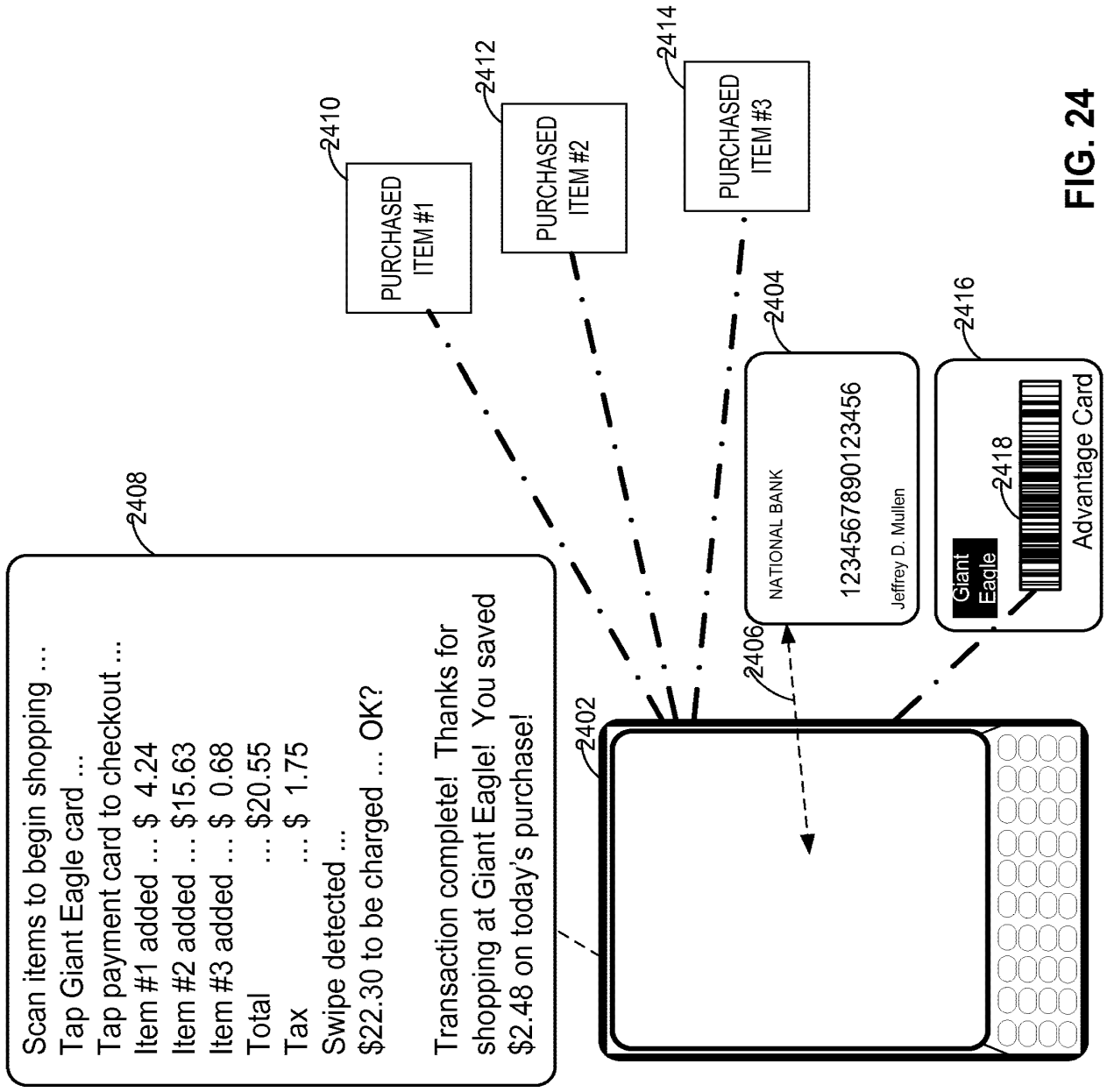

Scan items to begin shopping ...
Tap Giant Eagle card ...
Tap payment card to checkout ...
Item #1 added ... $ 4.24
Item #2 added ... $15.63
Item #3 added ... $ 0.68
Total ... $20.55
Tax ... $ 1.75
Swipe detected ...
$22.30 to be charged .... OK?
Transaction complete! Thanks for shopping at Giant Eagle! You saved $2.48 on today's purchase!
2408
2410
PURCHASED ITEM #1
2412
PURCHASED ITEM #2
2414
PURCHASED ITEM #3
2402
2404
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
2406
2416
Giant Eagle
2418
Advantage Card

FIG. 24

25/73
2500

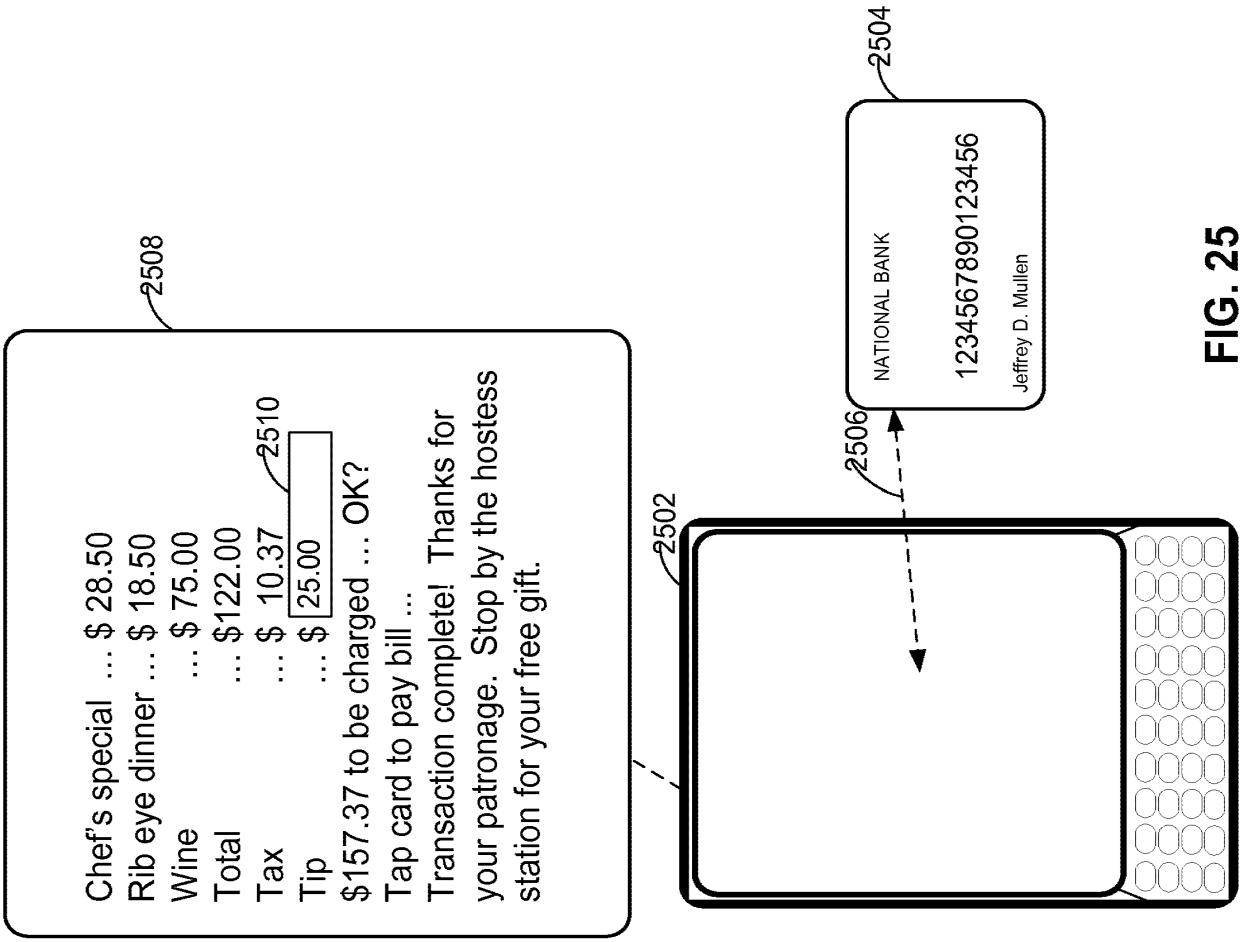



FIG. 25

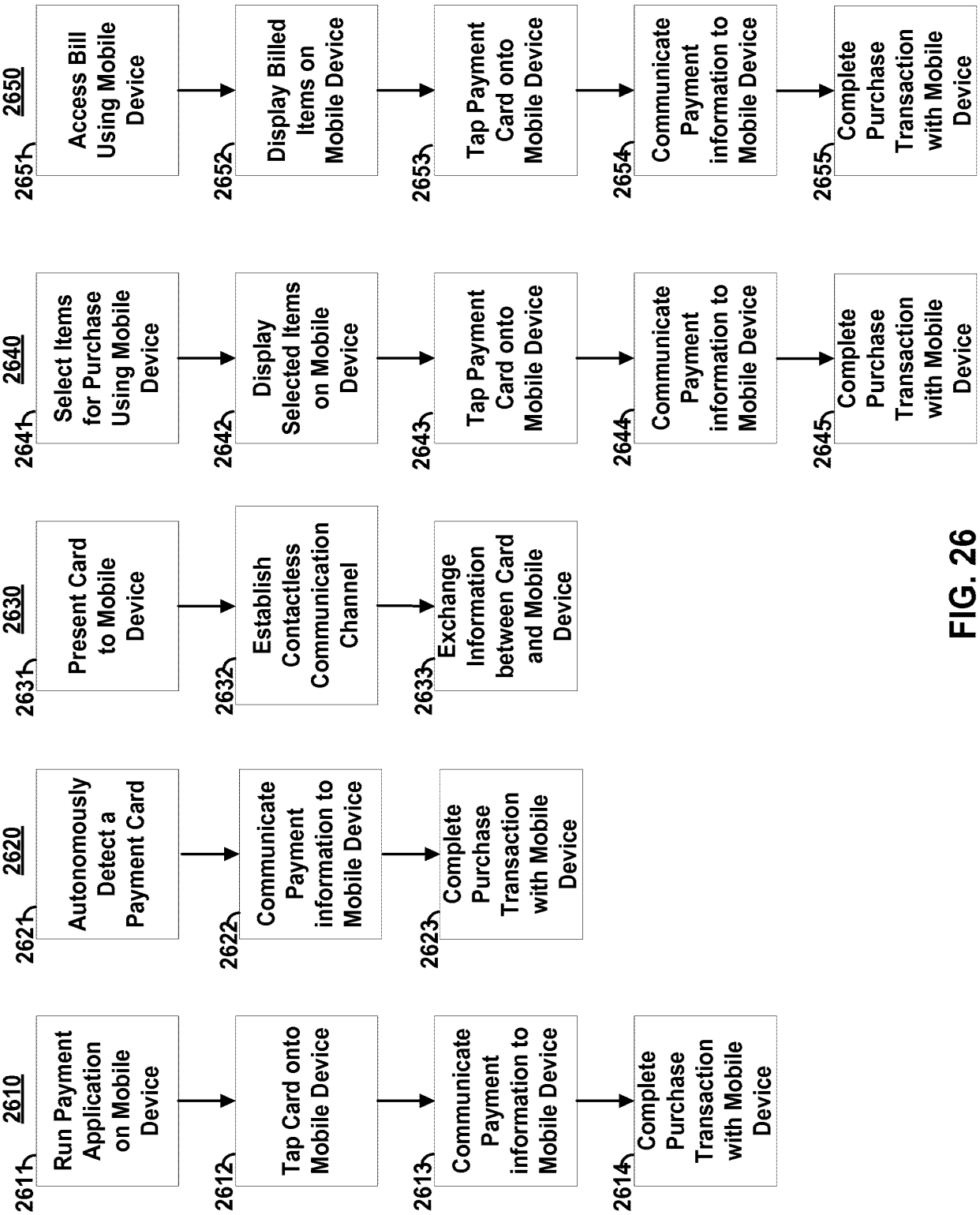

2610
2611
Run Payment Application on Mobile Device
2612
Tap Card onto Mobile Device
2613
Communicate Payment information to Mobile Device
2614
Complete Purchase Transaction with Mobile Device
2620
2621
Autonomously Detect a Payment Card
2622
Communicate Payment information to Mobile Device
2623
Complete 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

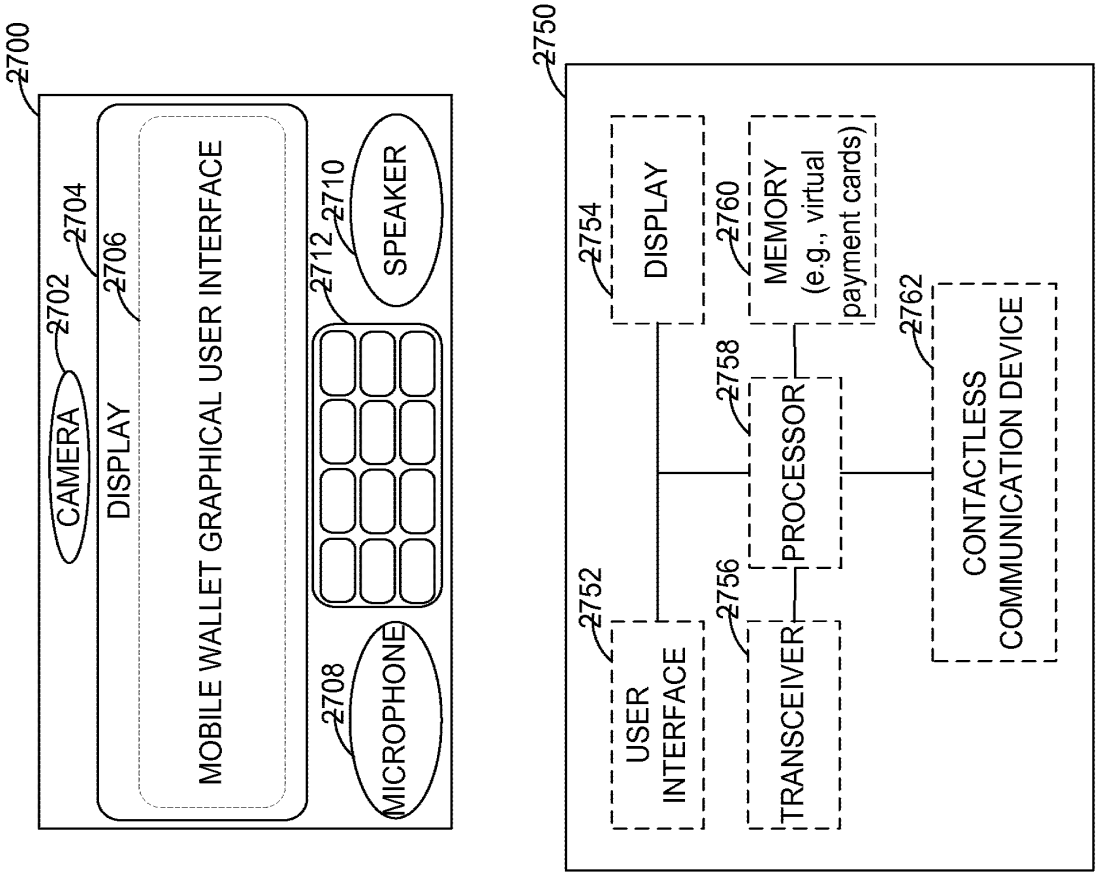

2700
CAMERA
2702
2704
DISPLAY
2706
MOBILE WALLET GRAPHICAL USER INTERFACE
2712
2710
SPEAKER
2708
MICROPHONE
2750
2754
DISPLAY
2760
MEMORY
(e.g., virtual
payment cards)
2752
USER
INTERFACE
2758
PROCESSOR
2756
TRANSCEIVER
2762
CONTACTLESS
COMMUNICATION DEVICE

FIG. 27

28/73

2800

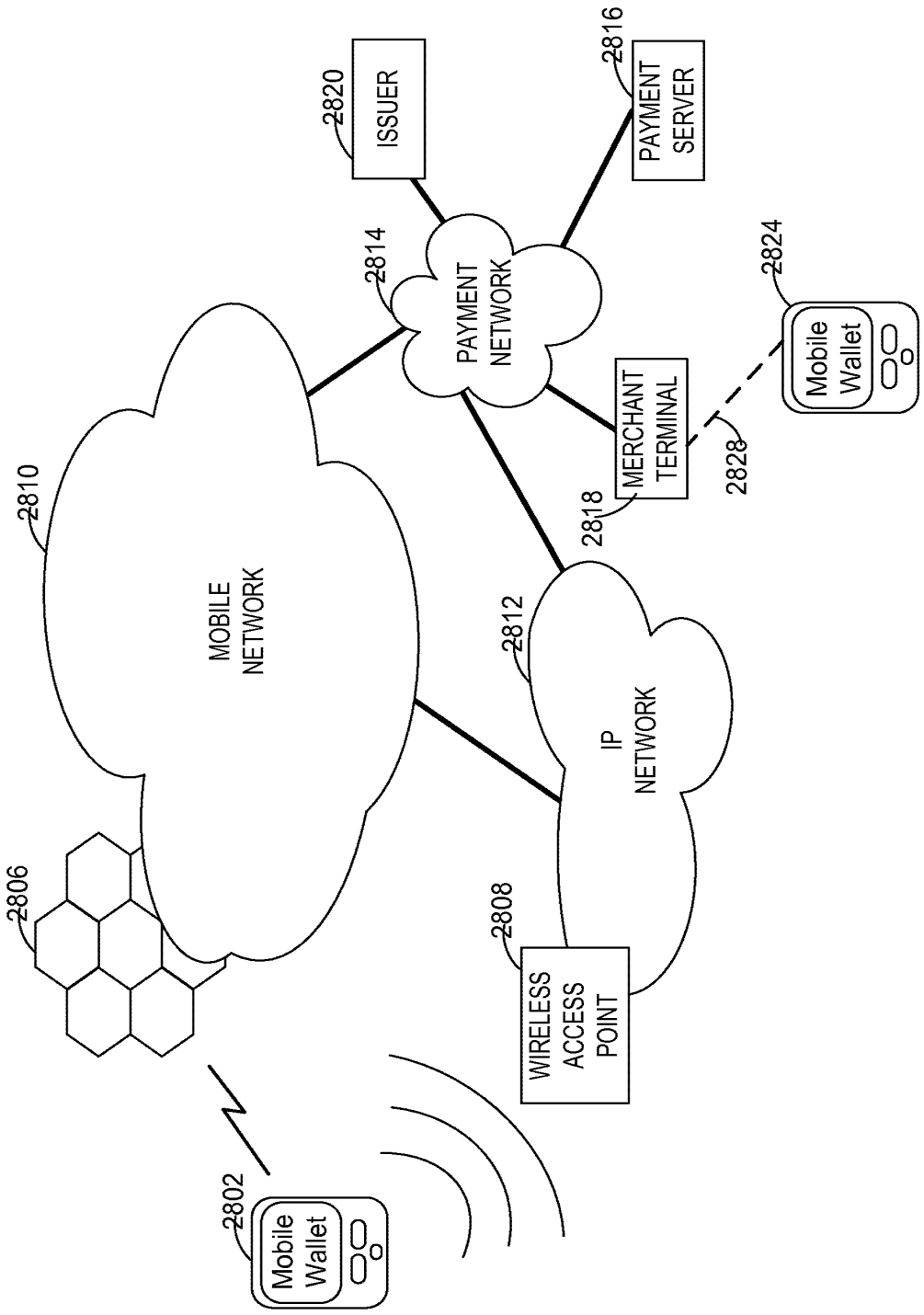



FIG. 28

2900

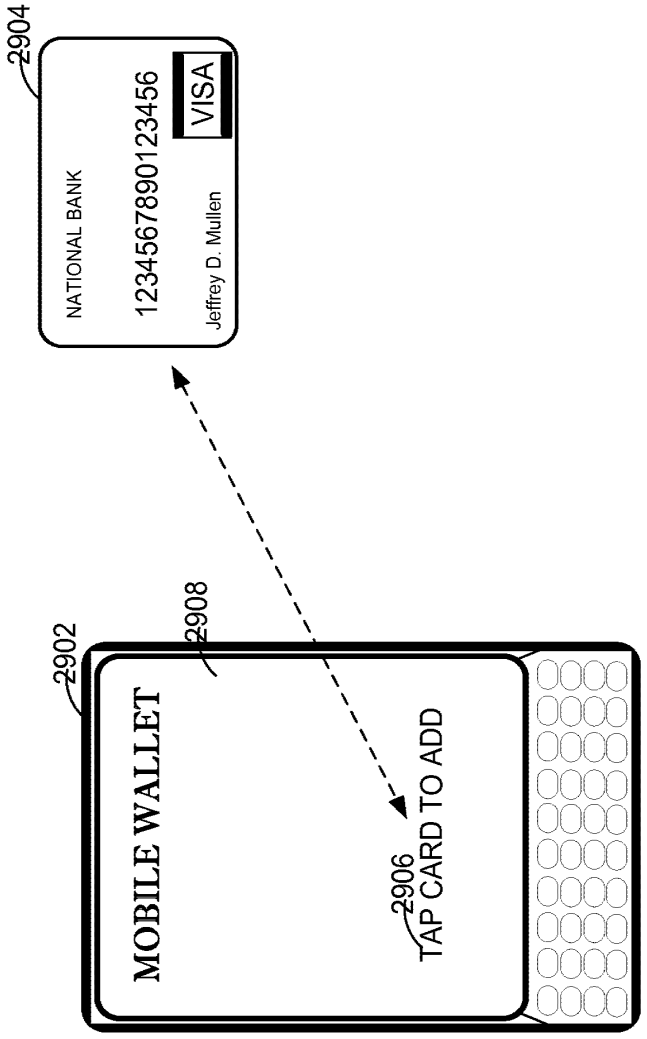

2904
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
2902
2908
MOBILE WALLET
2906
TAP CARD TO ADD

FIG. 29

30/73
3000

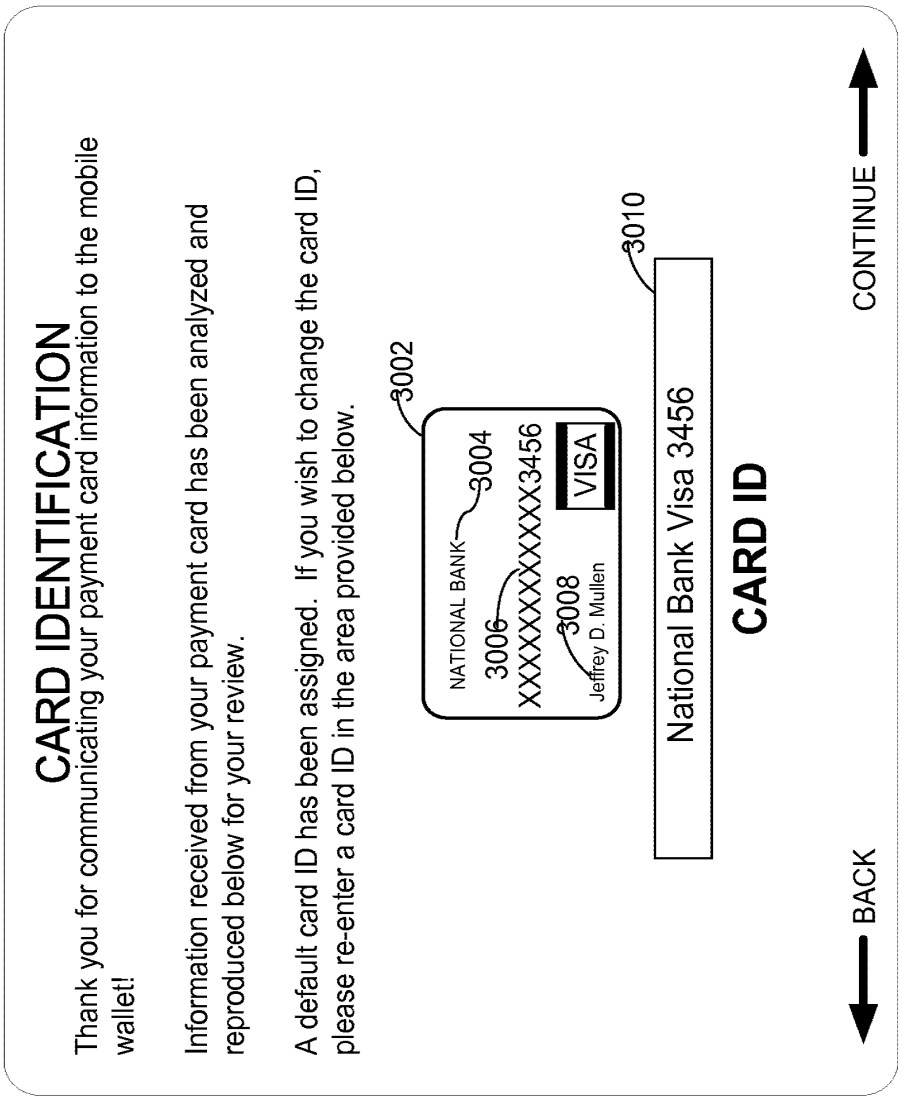



FIG. 30

31/73
3100

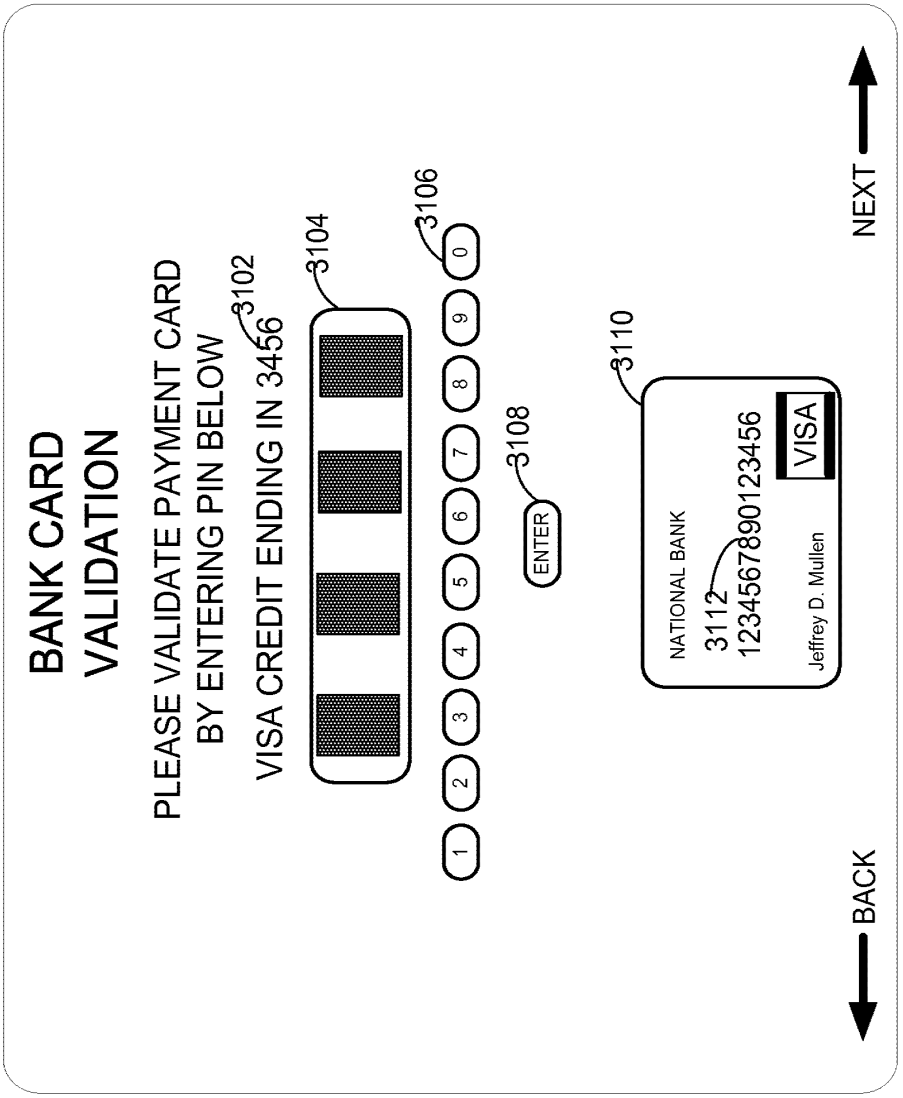



FIG. 31

3200

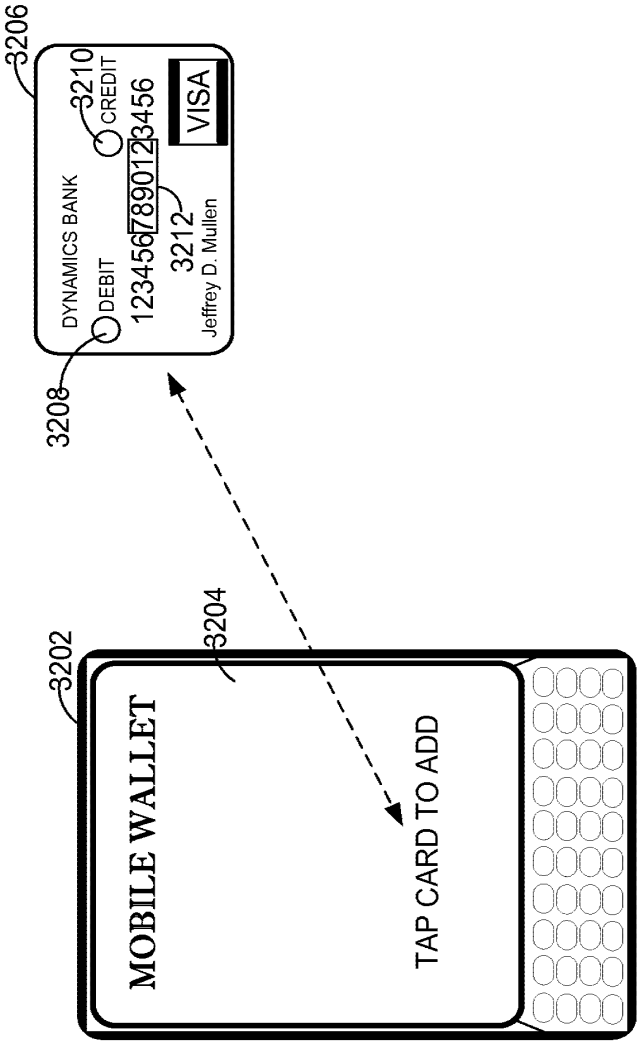

3206
3210
CREDIT
DYNAMICS BANK
DEBIT
123456789012 3456
VISA
3212
Jeffrey D. Mullen
3208
3204
3202
MOBILE WALLET
TAP CARD TO ADD

FIG. 32

3300

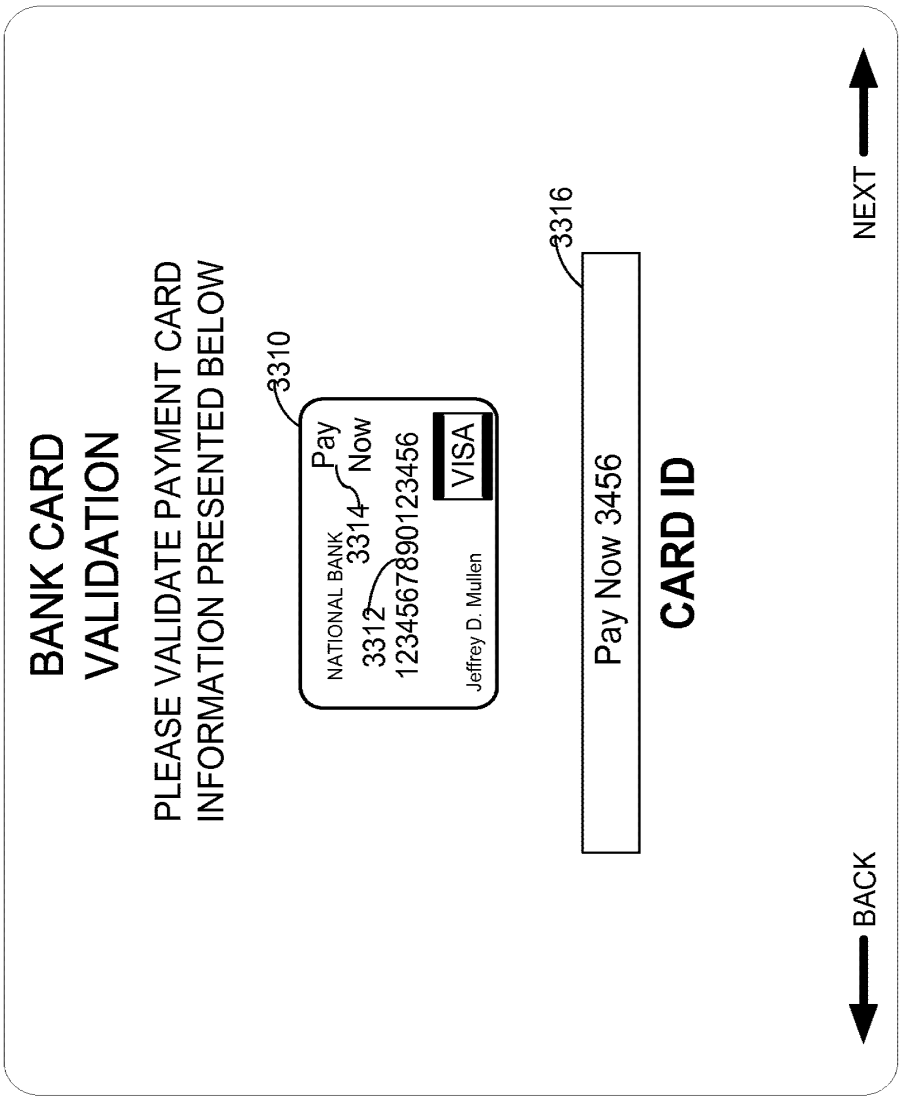

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
INFORMATION PRESENTED BELOW
3310
NATIONAL BANK
3314
Pay
Now
3312
1234567890123456
VISA
Jeffrey D. Mullen
3316
Pay Now 3456
CARD ID
NEXT
BACK

FIG. 33

34/73
3400

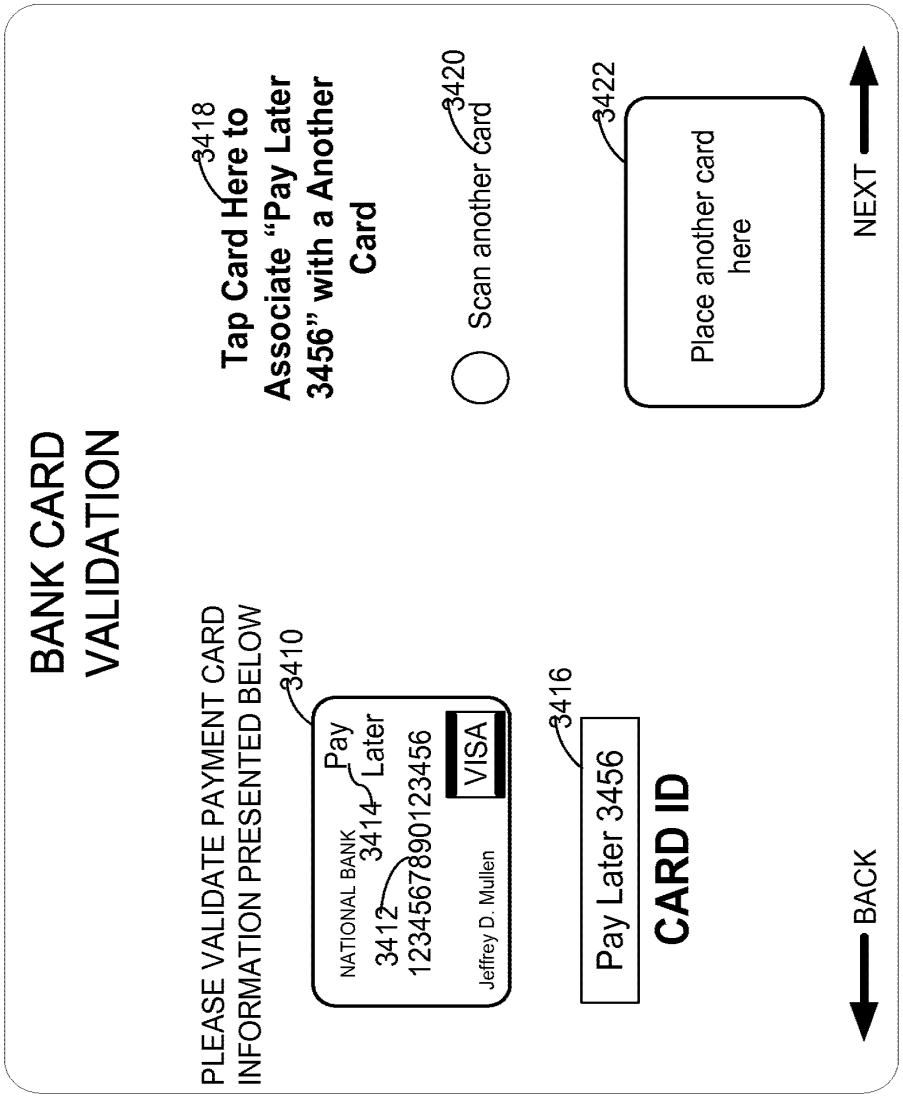



FIG. 34

35/73
3500

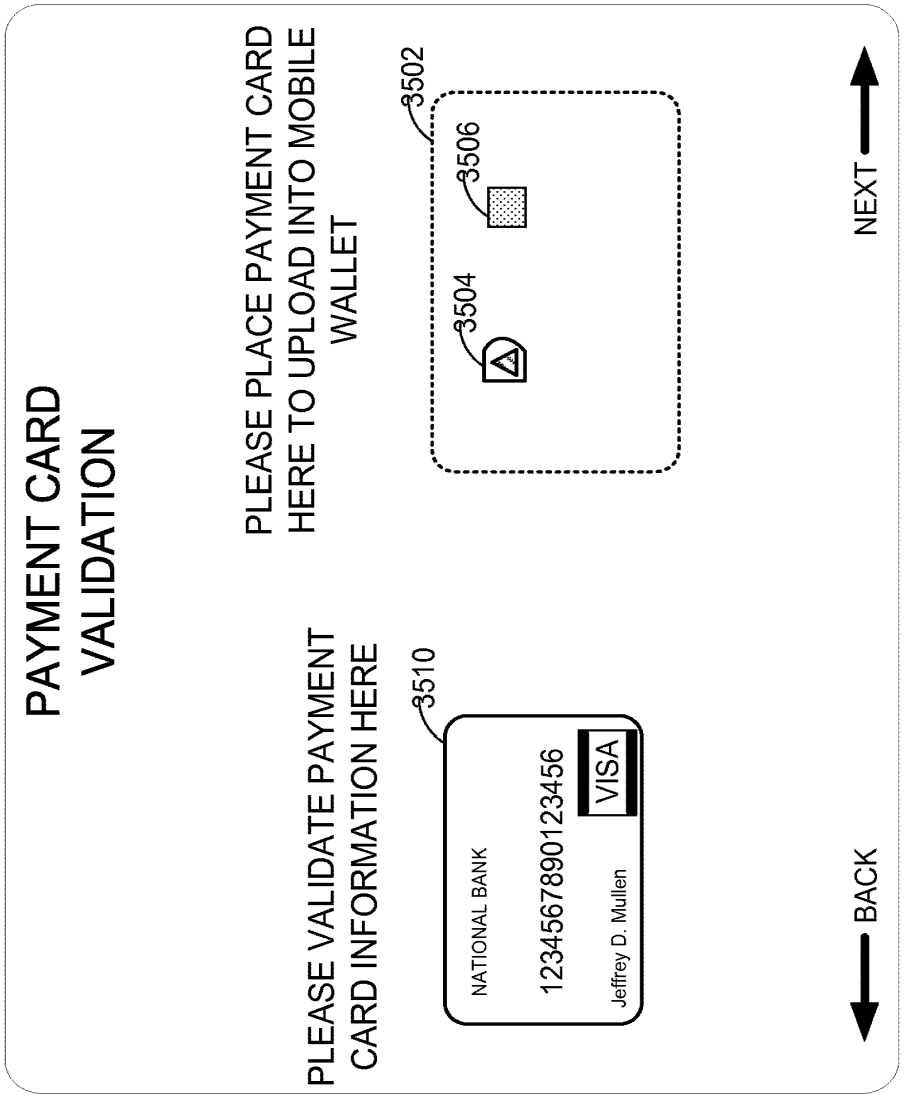



FIG. 35

36/73
3600

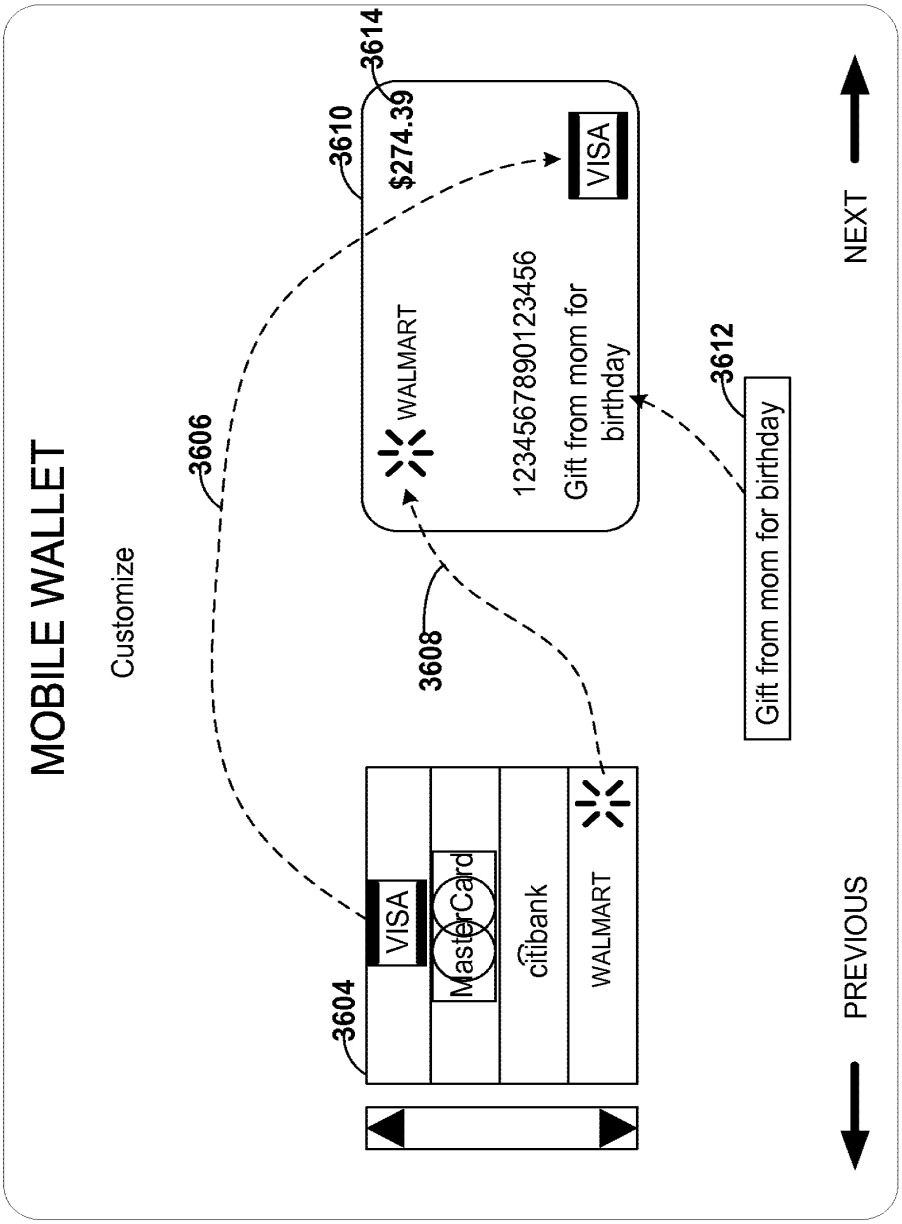



FIG. 36

37/73
3700

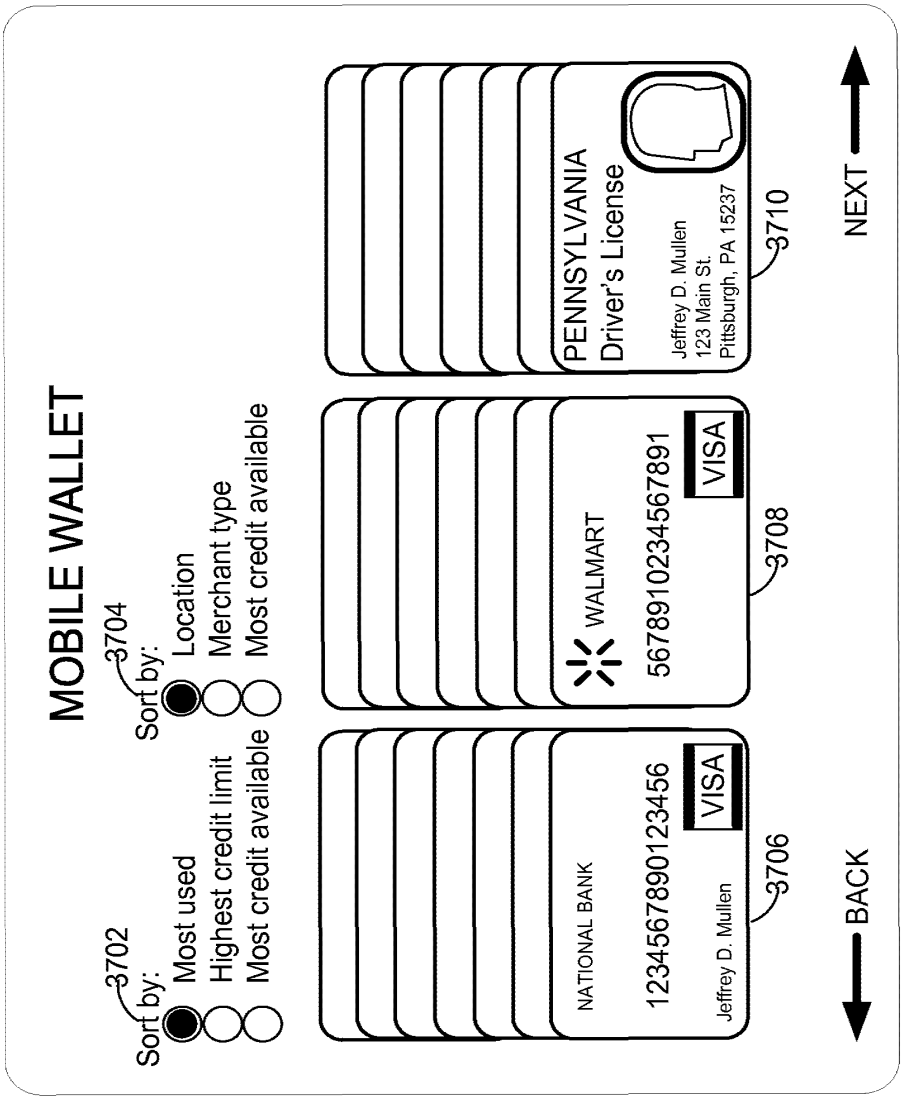



FIG. 37

38/73

3800

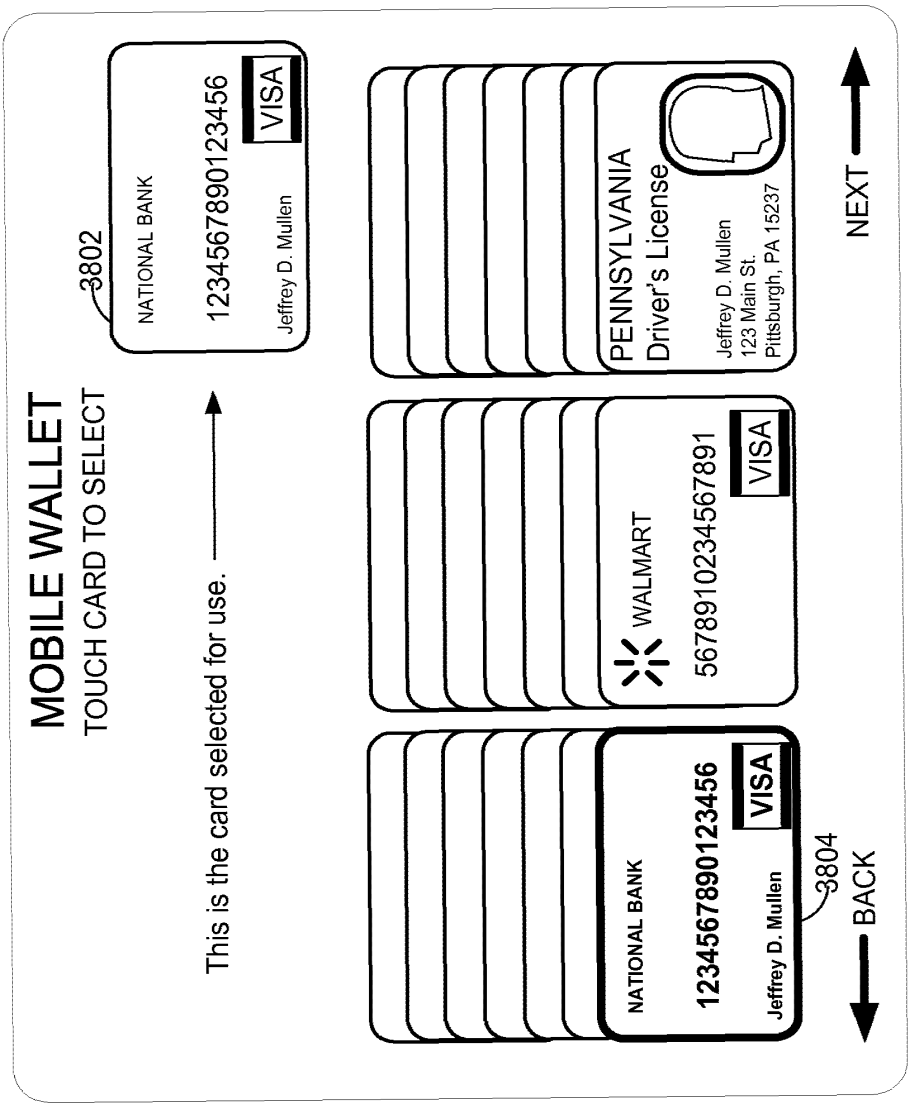



FIG. 38

39/73
3900

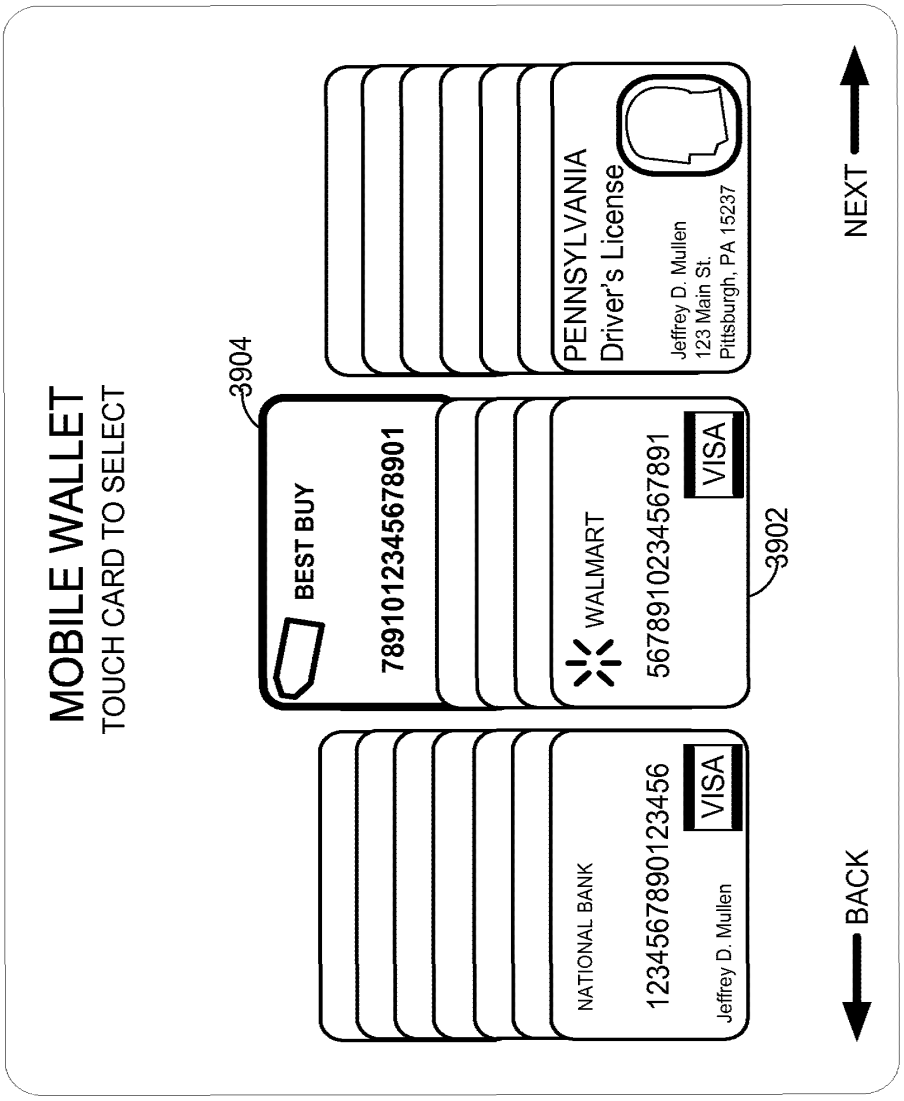



FIG. 39

40/73
4000

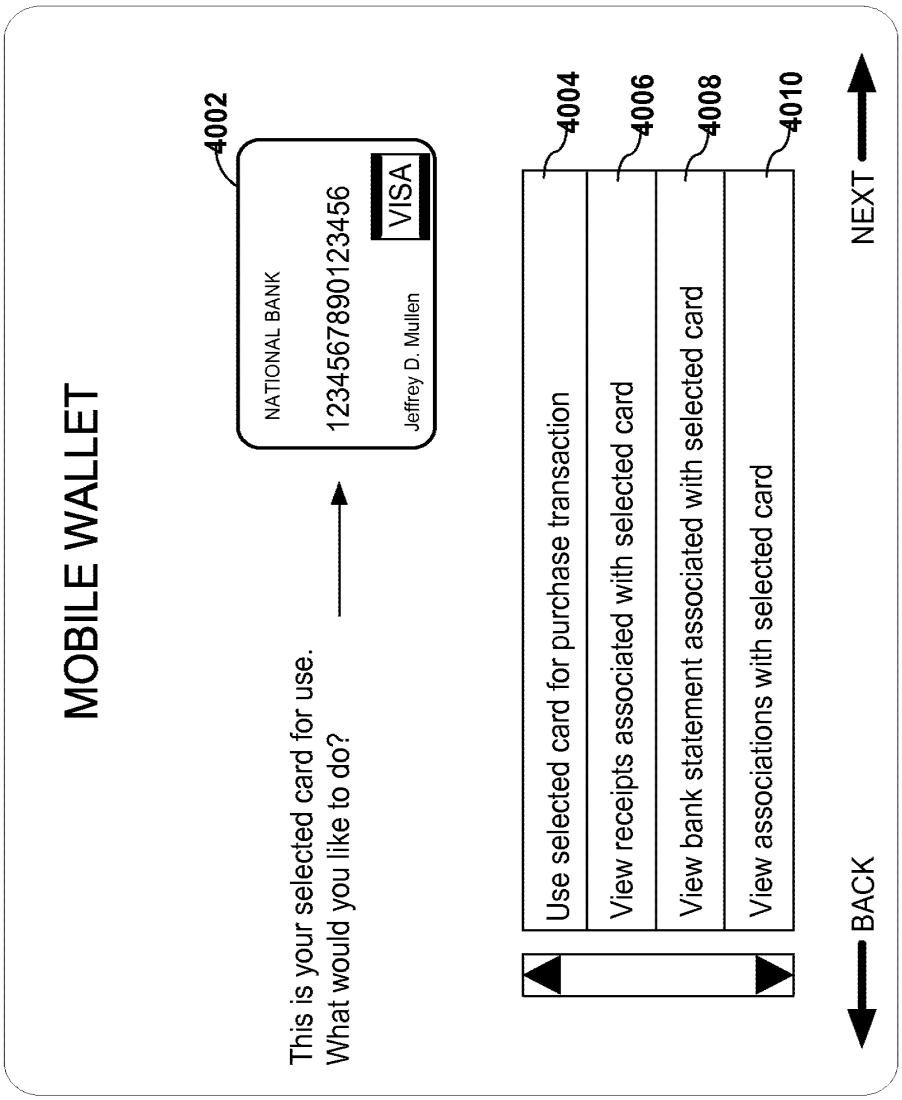



FIG. 40

41/73
4100

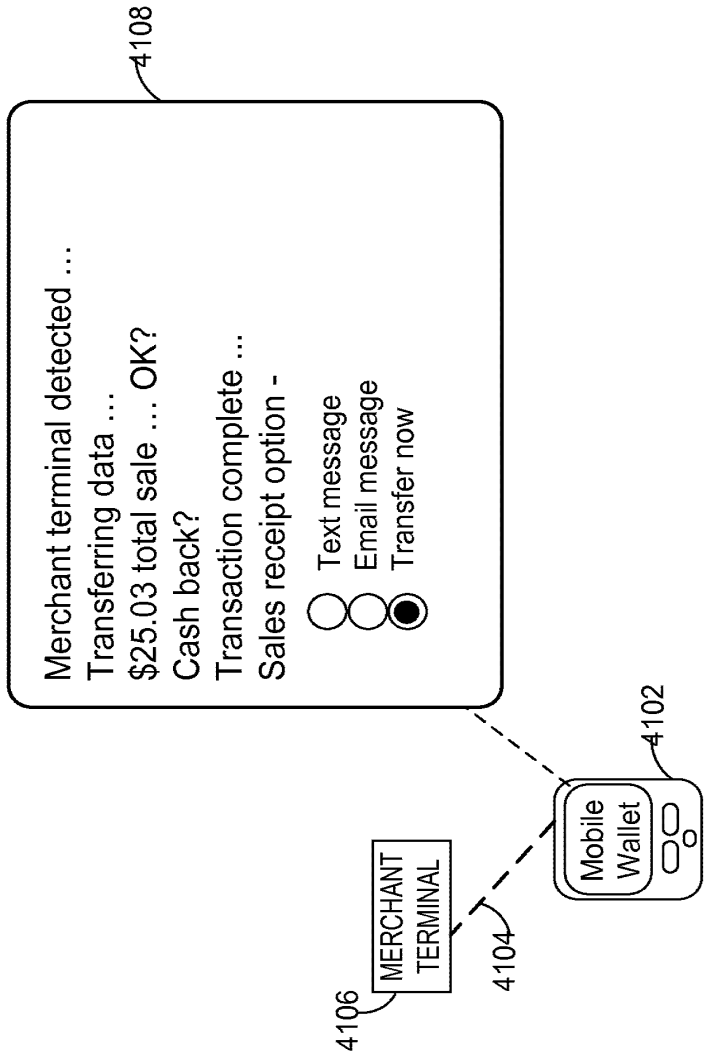



FIG. 41

42/73
4200

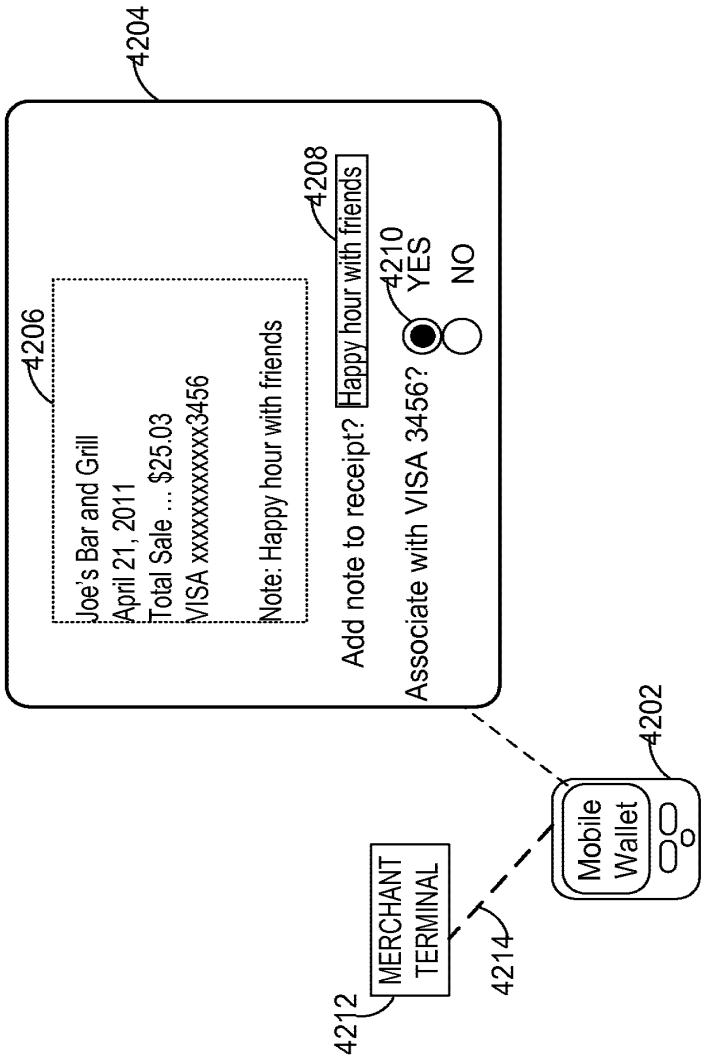



FIG. 42

43/73
4300

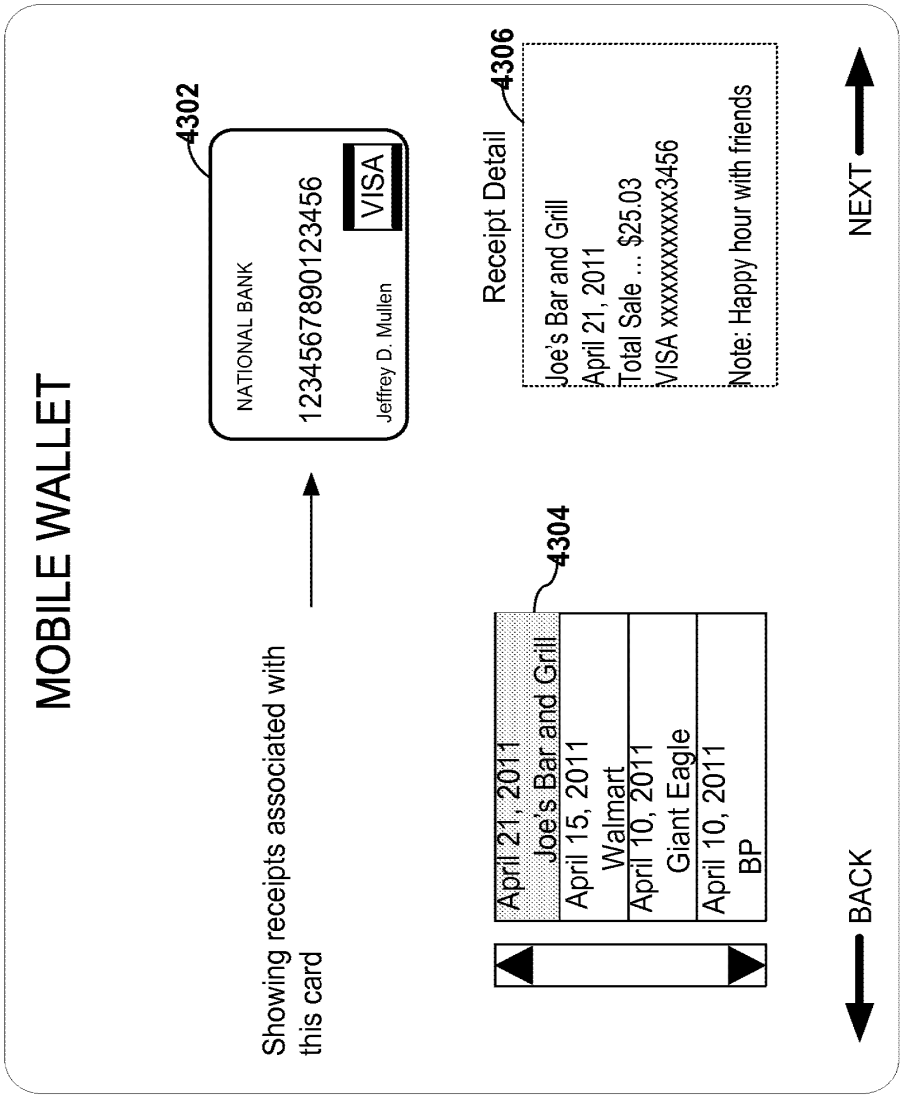



FIG. 43

4400

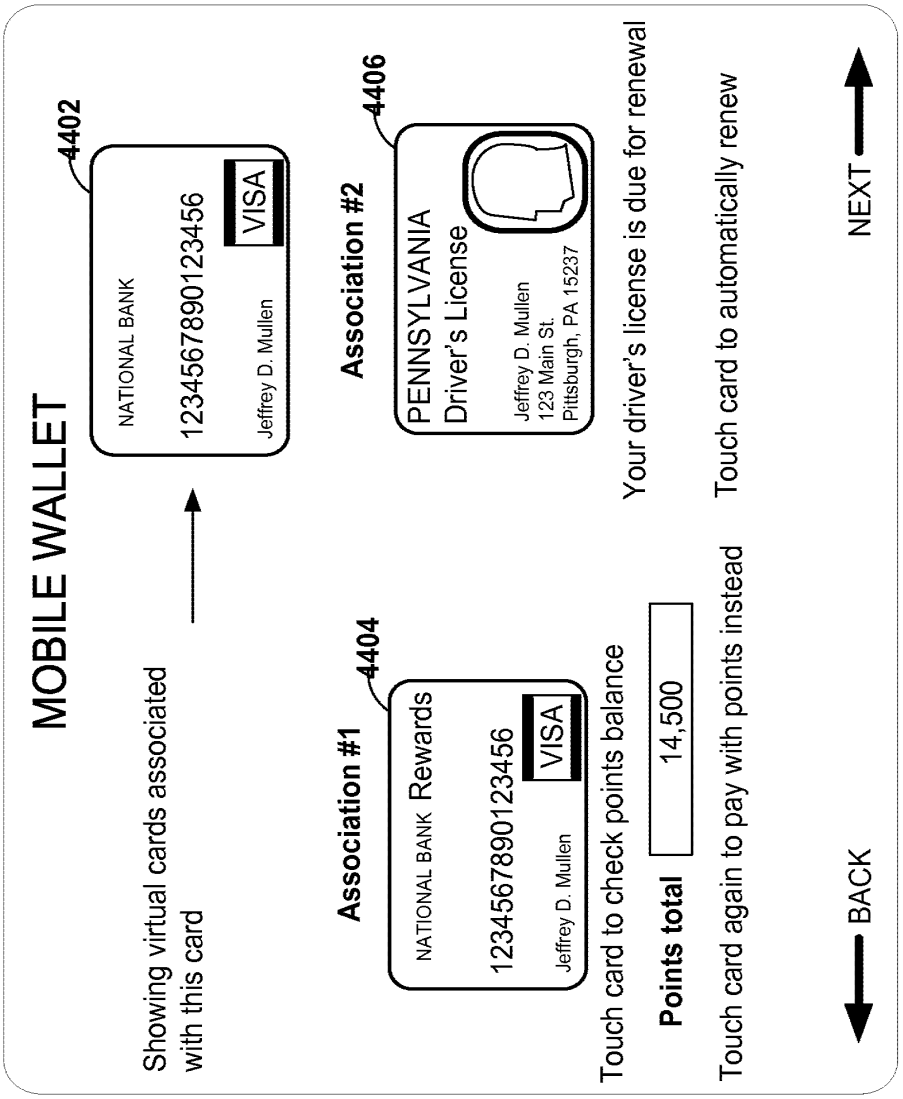

MOBILE WALLET
4402
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
Showing virtual cards associated with this card
Association #2
4406
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
Your driver's license is due for renewal
Association #1
4404
NATIONAL BANK Rewards
1234567890123456
Jeffrey D. Mullen
VISA
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

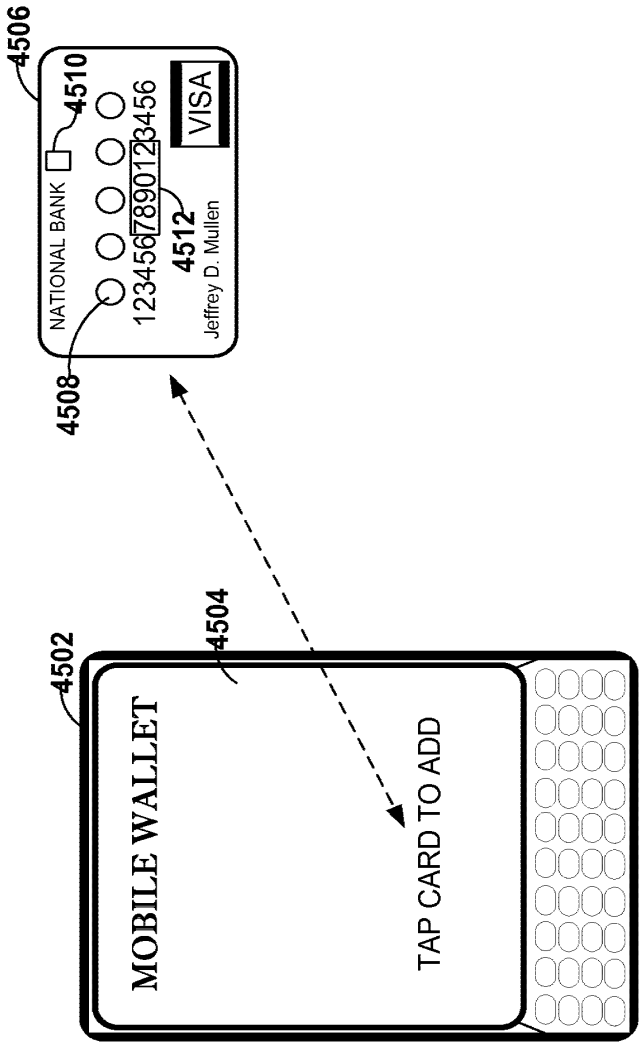

4506
4510
NATIONAL BANK
VISA
1234567890123456
4512
Jeffrey D. Mullen
4508
4502
4504
MOBILE WALLET
TAP CARD TO ADD

FIG. 45

46/73

4600

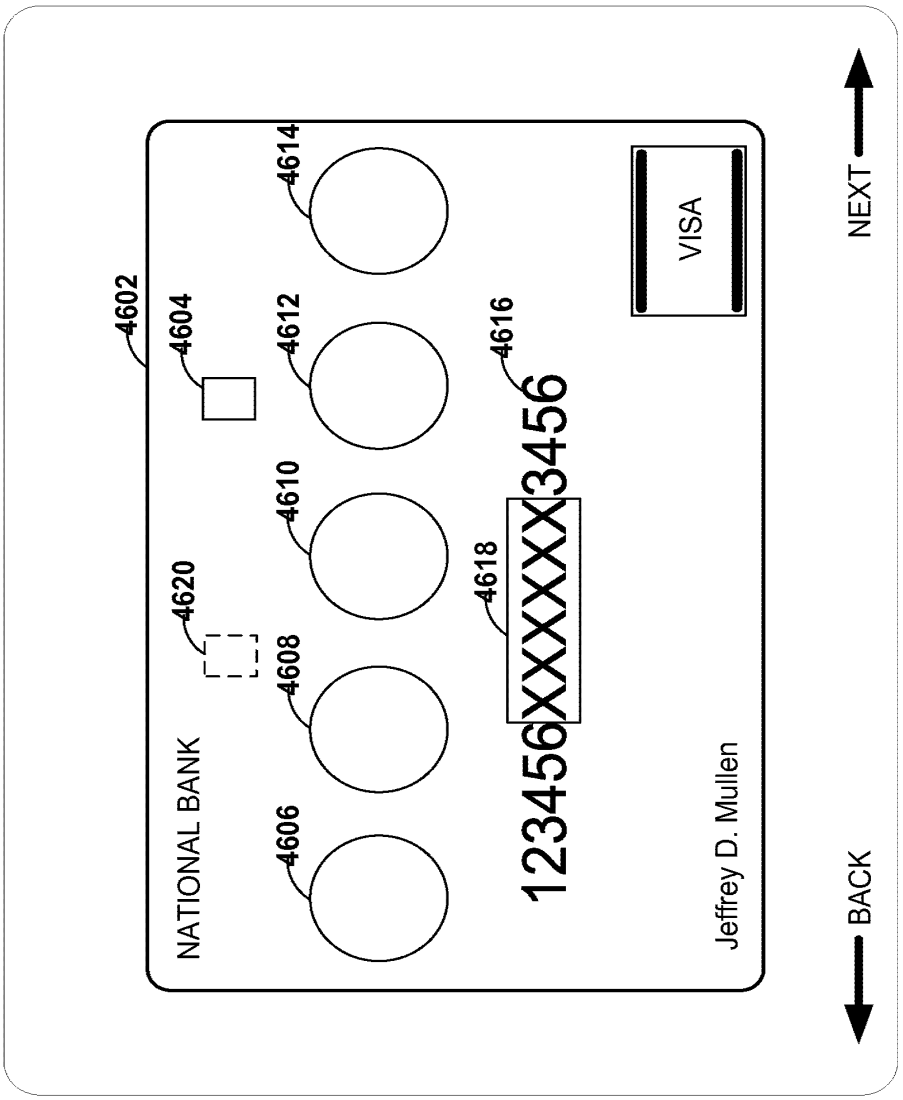



FIG. 46

47/73
4700

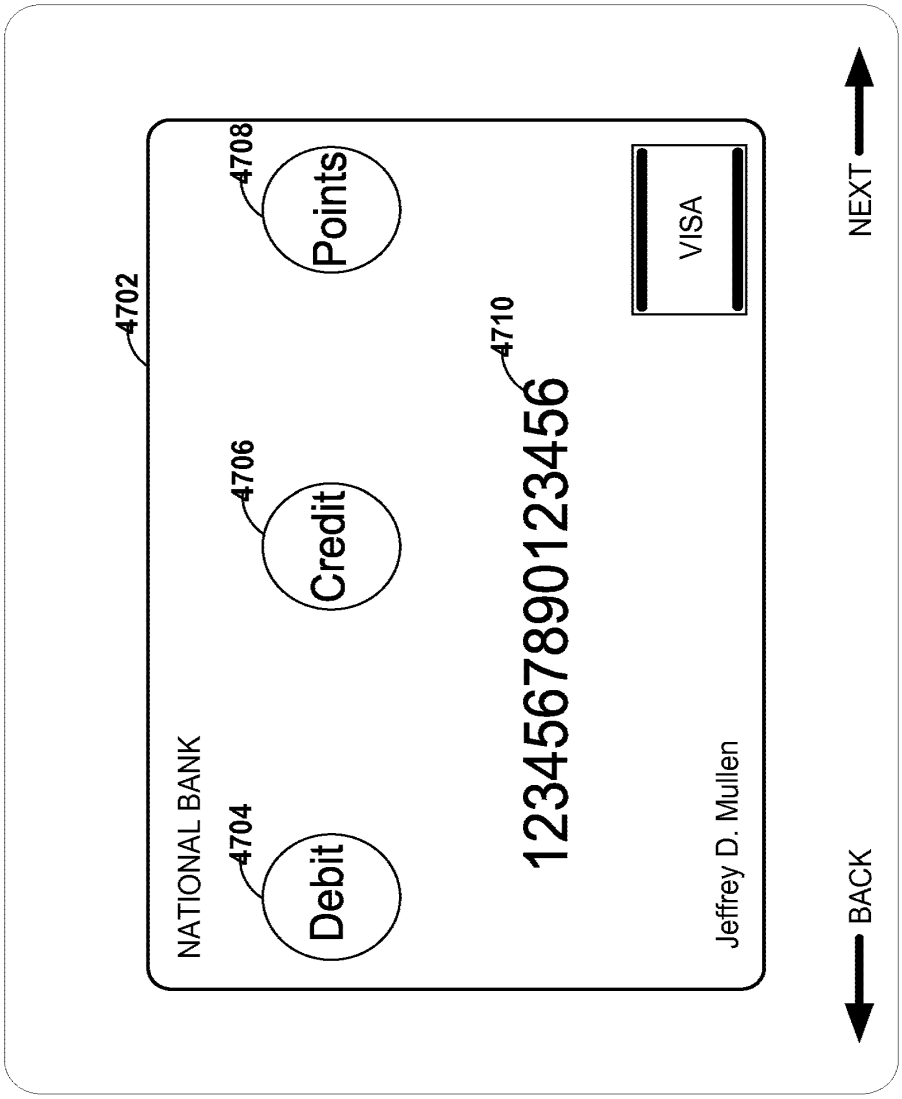



FIG. 47

4800

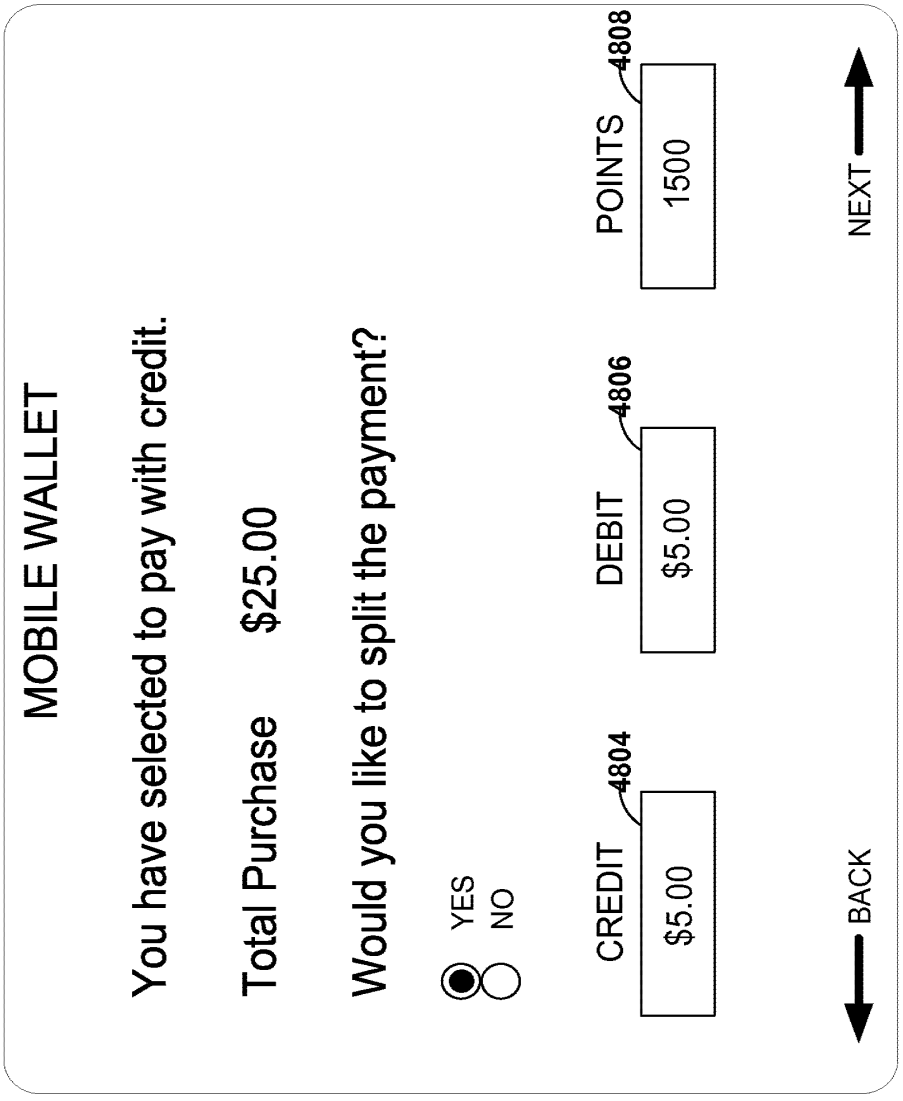

MOBILE WALLET
You have selected to pay with credit.
Total Purchase $25.00
Would you like to split the payment?
YES
NO
CREDIT
4804
$5.00
DEBIT
4806
$5.00
POINTS
4808
1500
BACK
NEXT

FIG. 48

4900

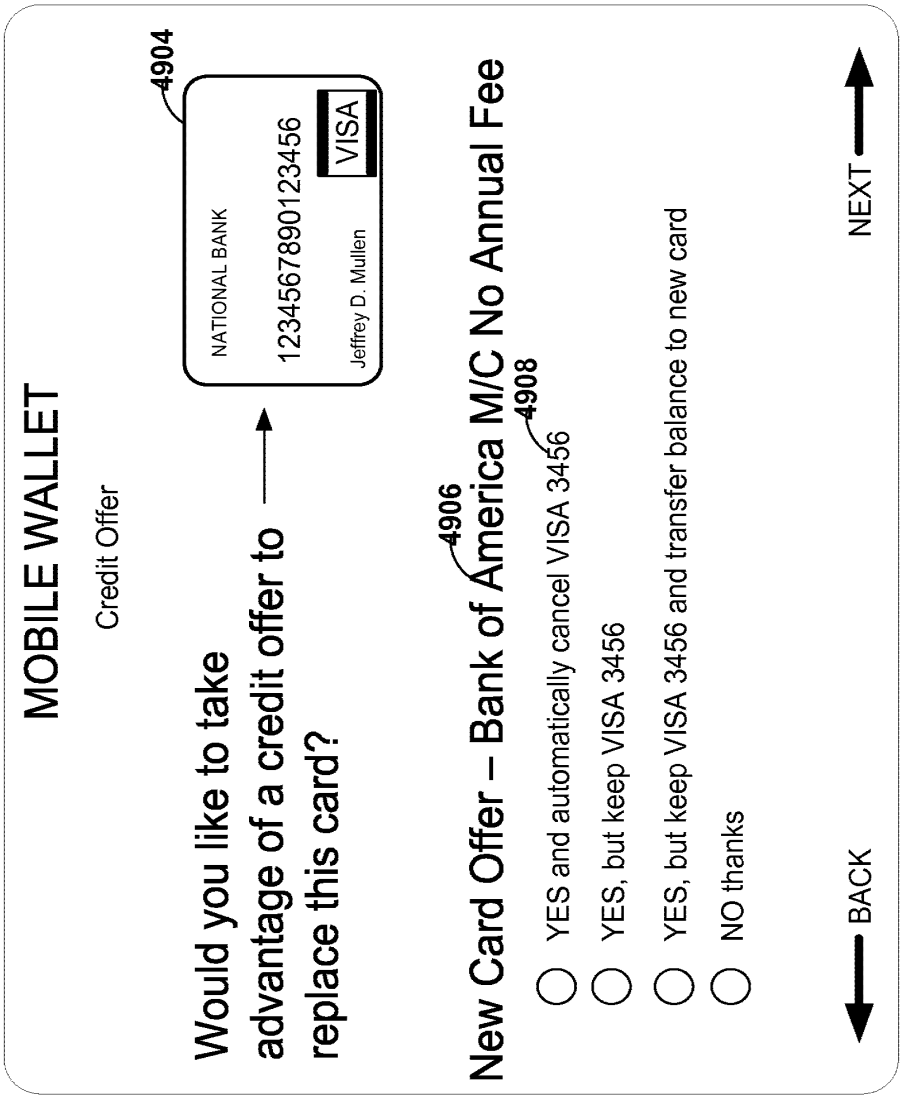

MOBILE WALLET
Credit Offer
Would you like to take advantage of a credit offer to replace this card?
4904
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
New Card Offer – Bank of America M/C No Annual Fee
4906
4908
YES and automatically cancel VISA 3456
YES, but keep VISA 3456
YES, but keep VISA 3456 and transfer balance to new card
NO thanks
BACK
NEXT

FIG. 49

50/73
5000

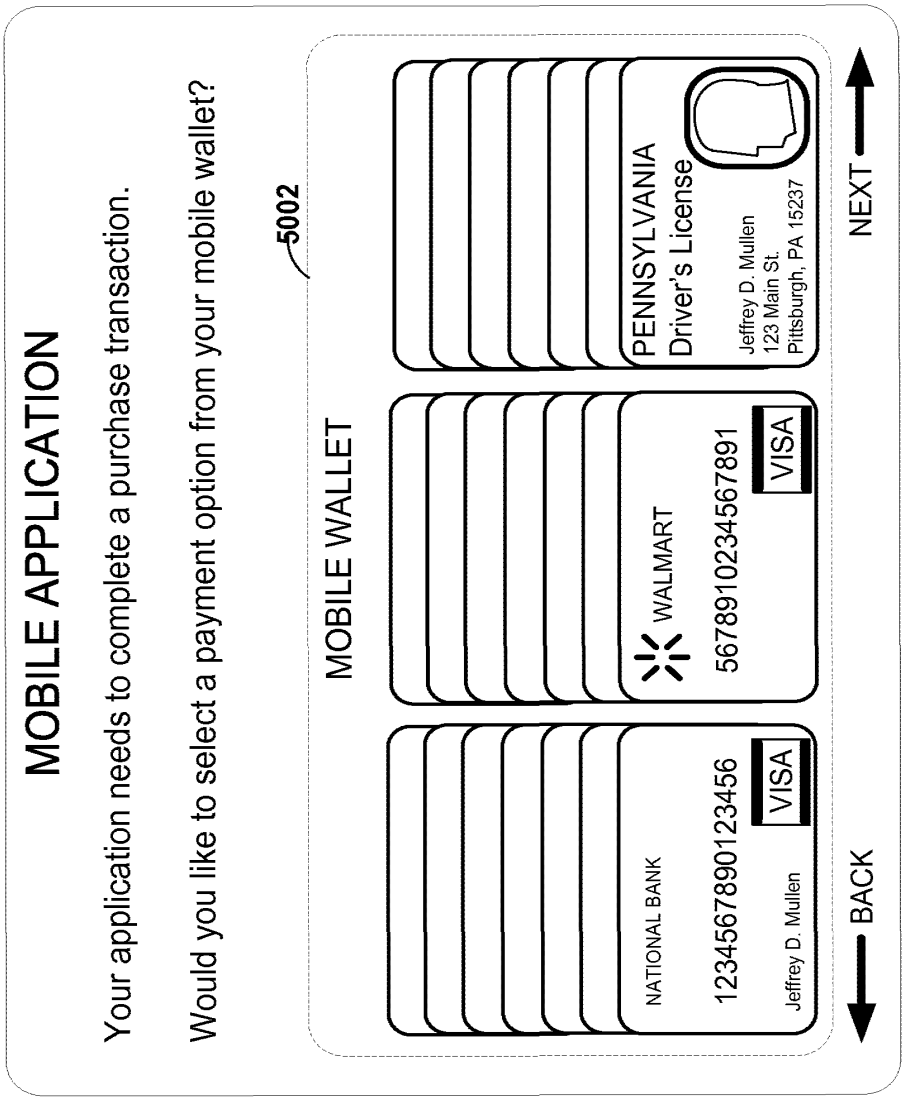



FIG. 50

51/73

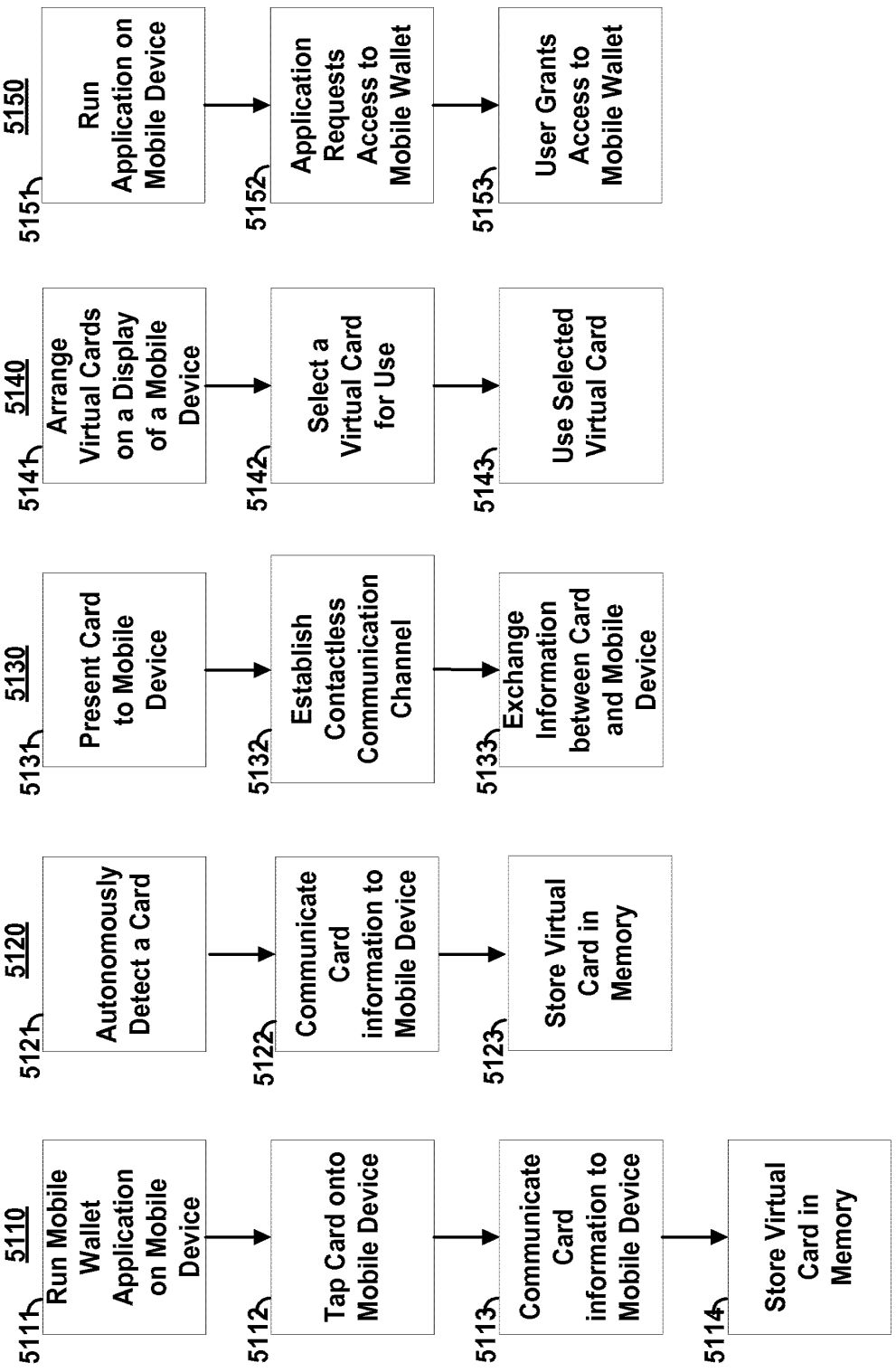

5110
5111
Run Mobile Wallet Application on Mobile Device
5112
Tap Card onto Mobile Device
5113
Communicate Card information to Mobile Device
5114
Store Virtual Card in Memory
5120
5121
Autonomously Detect a Card
5122
Communicate Card information to Mobile Device
5123
Store Virtual Card in Memory
5130
5131
Present Card to Mobile Device
5132
Establish Contactless Communication Channel
5133
Exchange Information between Card and Mobile Device
5140
5141
Arrange Virtual Cards on a Display of a Mobile Device
5142
Select a Virtual Card for Use
5143
Use Selected Virtual Card
5150
5151
Run Application on Mobile Device
5152
Application Requests Access to Mobile Wallet
5153
User Grants Access to Mobile Wallet

FIG. 51

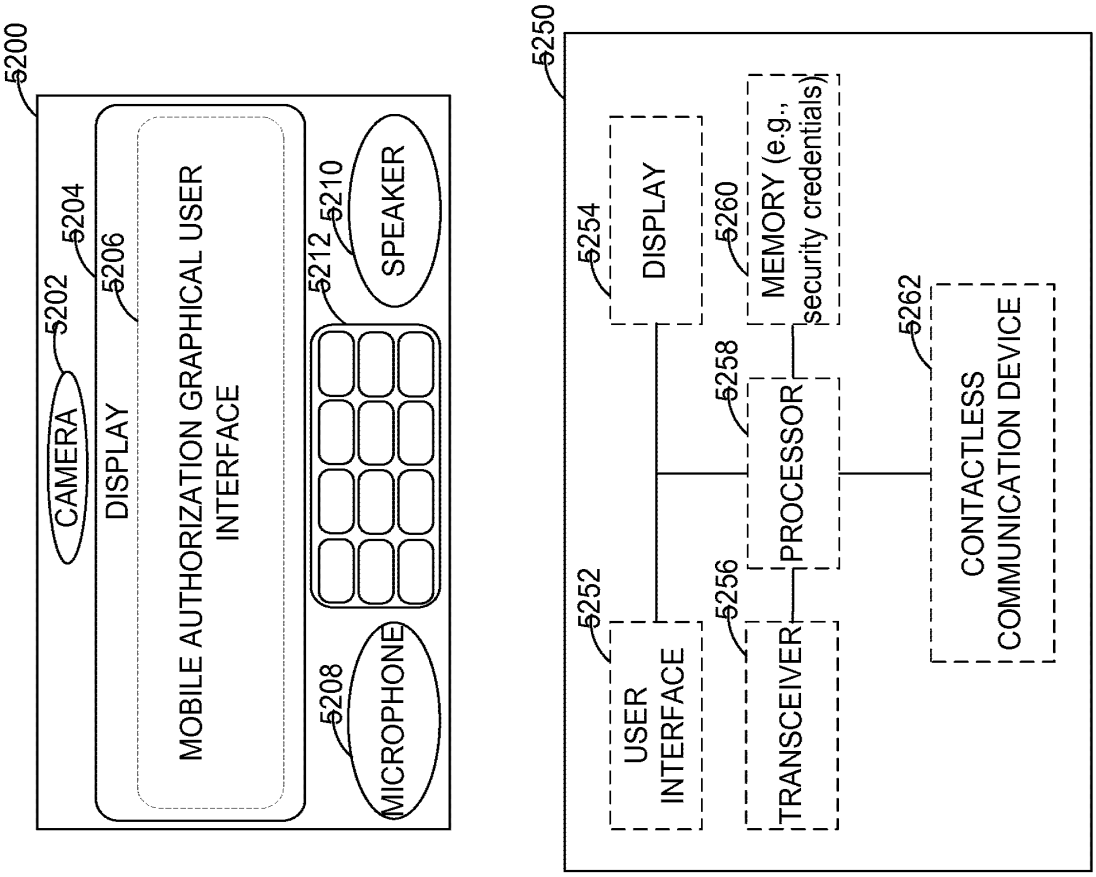

5200
CAMERA
5202
DISPLAY
5204
MOBILE AUTHORIZATION GRAPHICAL USER INTERFACE
5206
5212
SPEAKER
5210
MICROPHONE
5208
5250
USER INTERFACE
5252
DISPLAY
5254
TRANSCEIVER
5256
PROCESSOR
5258
MEMORY (e.g., security credentials)
5260
CONTACTLESS COMMUNICATION DEVICE
5262

FIG. 52

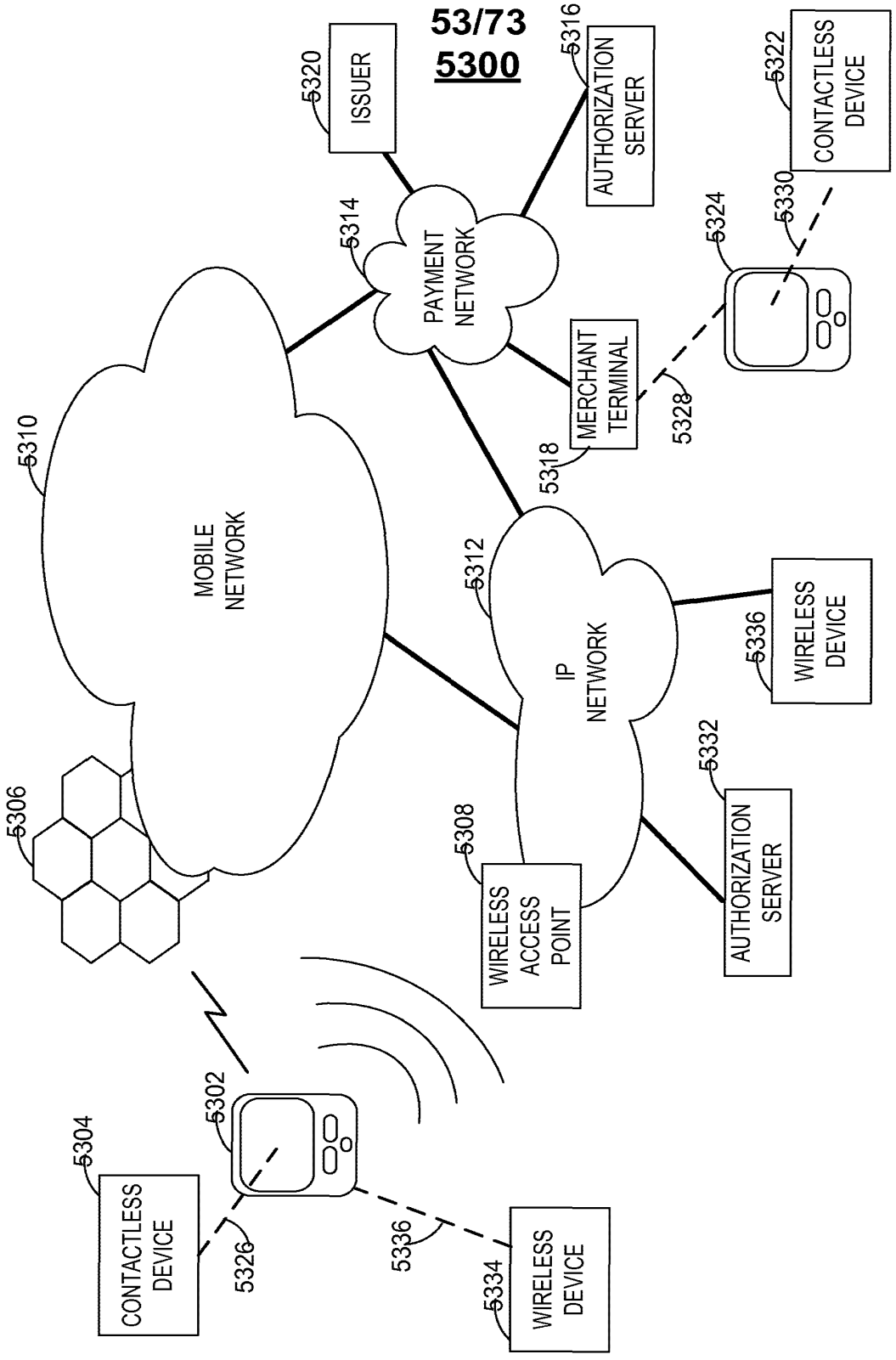

53/73
5300
5320
ISSUER
5316
AUTHORIZATION SERVER
5322
CONTACTLESS DEVICE
5314
PAYMENT NETWORK
5324
5330
5310
MOBILE NETWORK
MERCHANT TERMINAL
5328
5318
5312
IP NETWORK
5336
WIRELESS DEVICE
5306
5332
AUTHORIZATION SERVER
5308
WIRELESS ACCESS POINT
5302
5304
CONTACTLESS DEVICE
5326
5336
5334
WIRELESS DEVICE

FIG. 53

5400

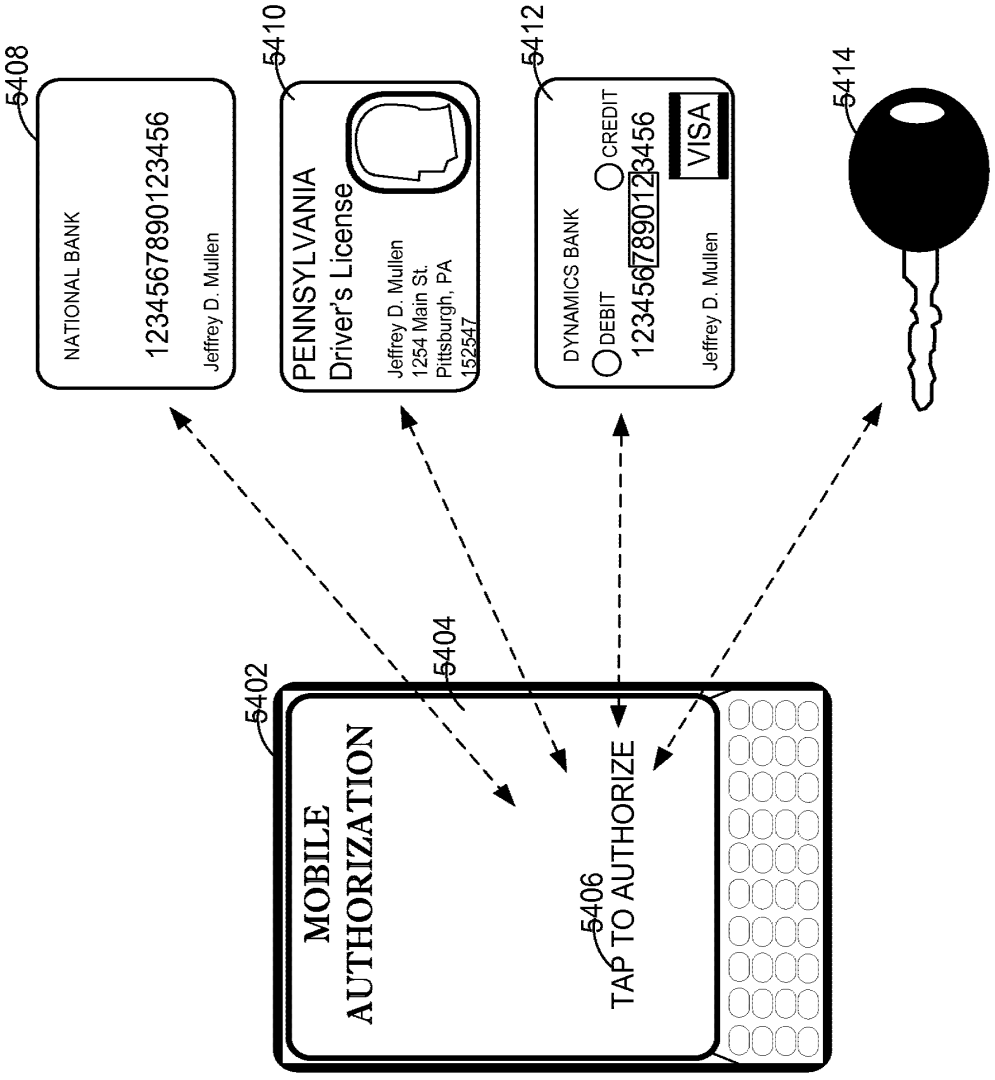

5408
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
5410
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
1254 Main St.
Pittsburgh, PA
152547
5412
DYNAMICS BANK
DEBIT
CREDIT
1234567890123456
VISA
Jeffrey D. Mullen
5414
5402
MOBILE AUTHORIZATION
5404
5406
TAP TO AUTHORIZE

FIG. 54

5500

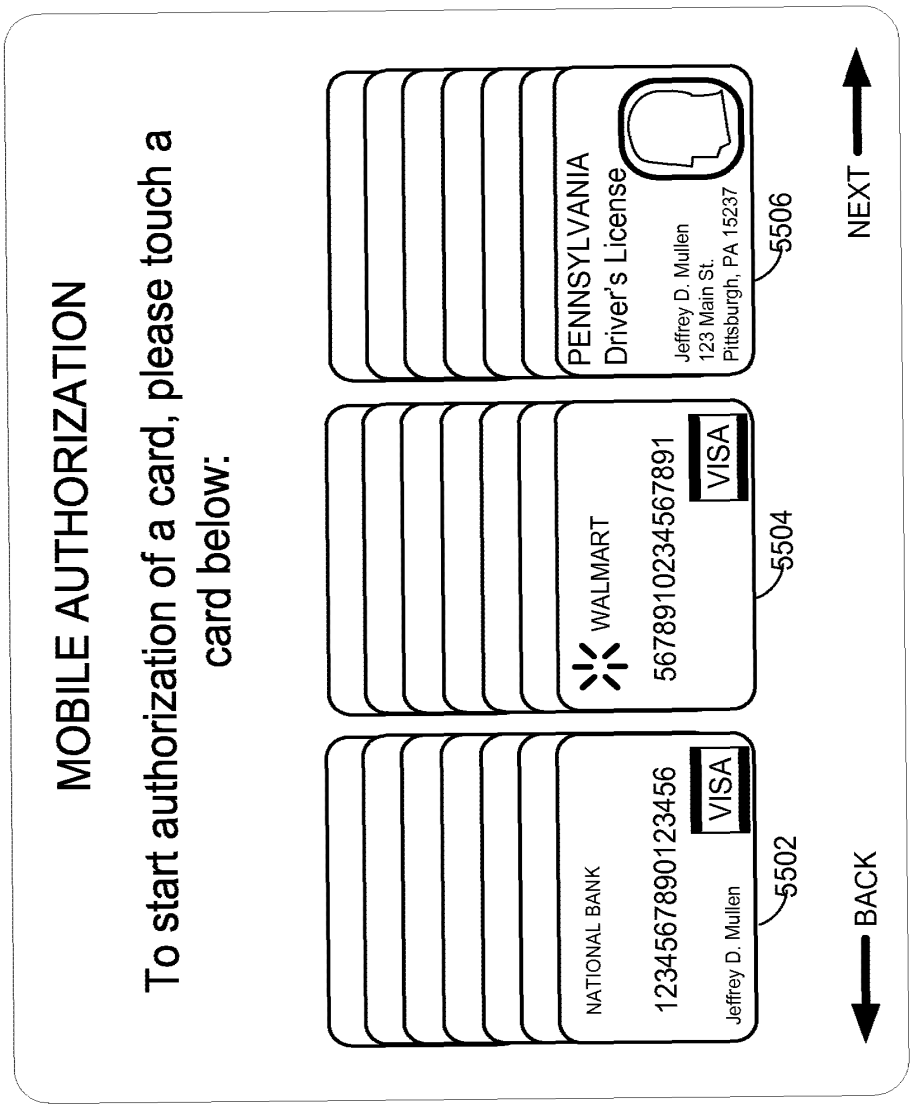

MOBILE AUTHORIZATION
To start authorization of a card, please touch a card below:
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
5502
WALMART
5678910234567891
VISA
5504
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
5506
BACK
NEXT

FIG. 55

5600

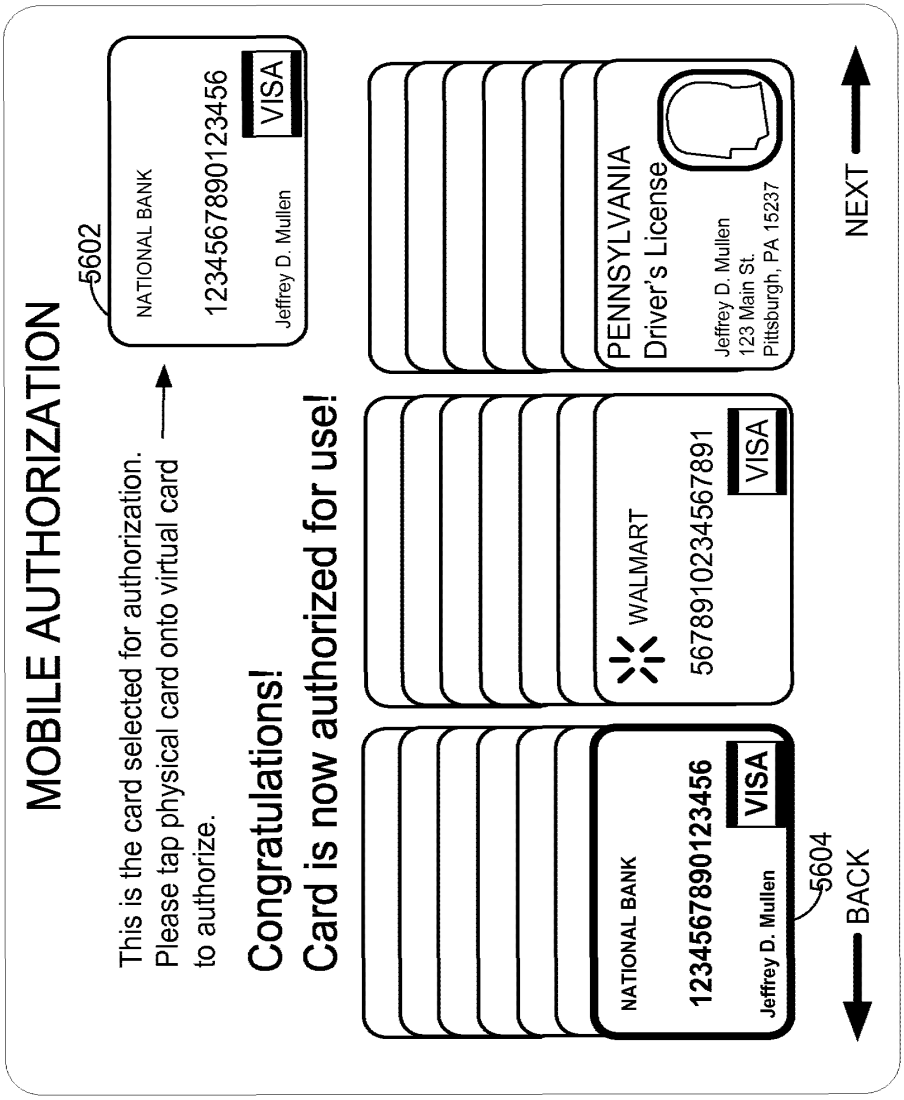

MOBILE AUTHORIZATION
This is the card selected for authorization.
Please tap physical card onto virtual card
to authorize.
Congratulations!
Card is now authorized for use!
5602
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
WALMART
5678910234567891
VISA
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
5604
BACK
NEXT

FIG. 56

57/73
5700

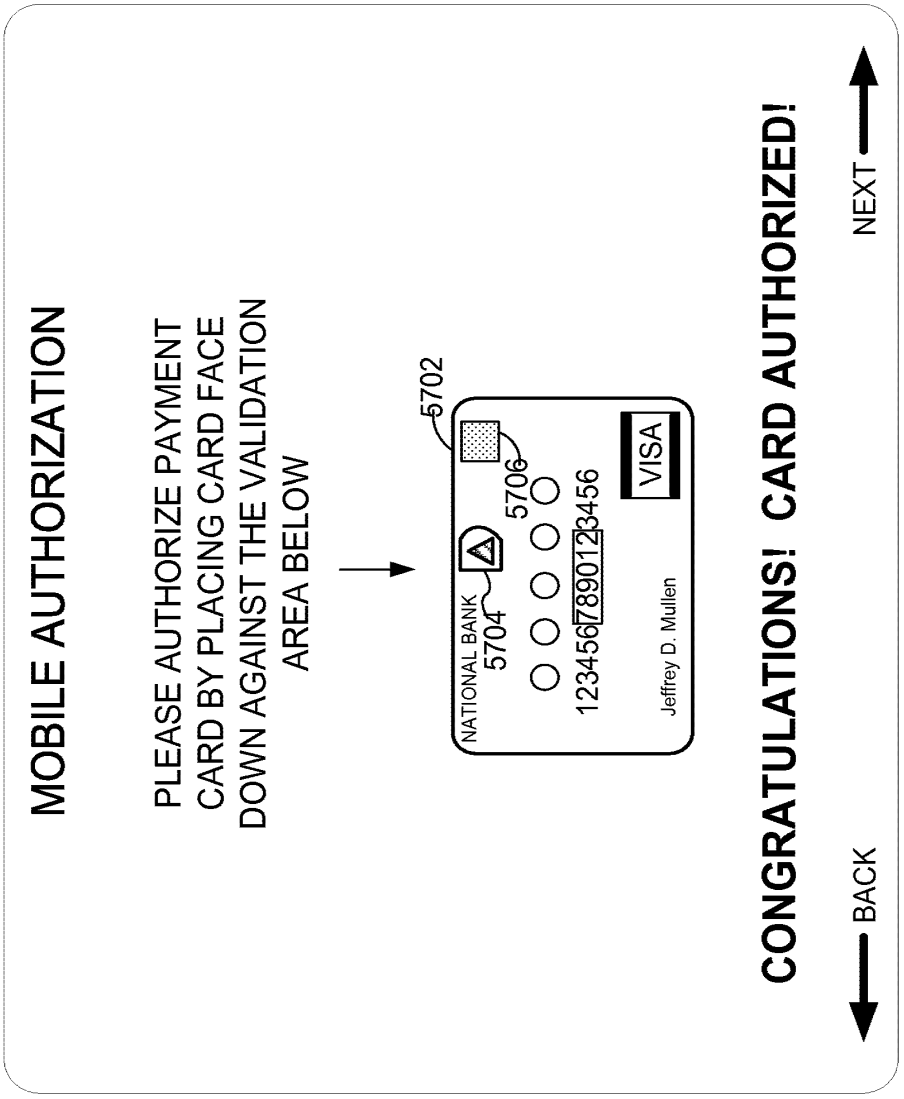



FIG. 57

58/73
5800

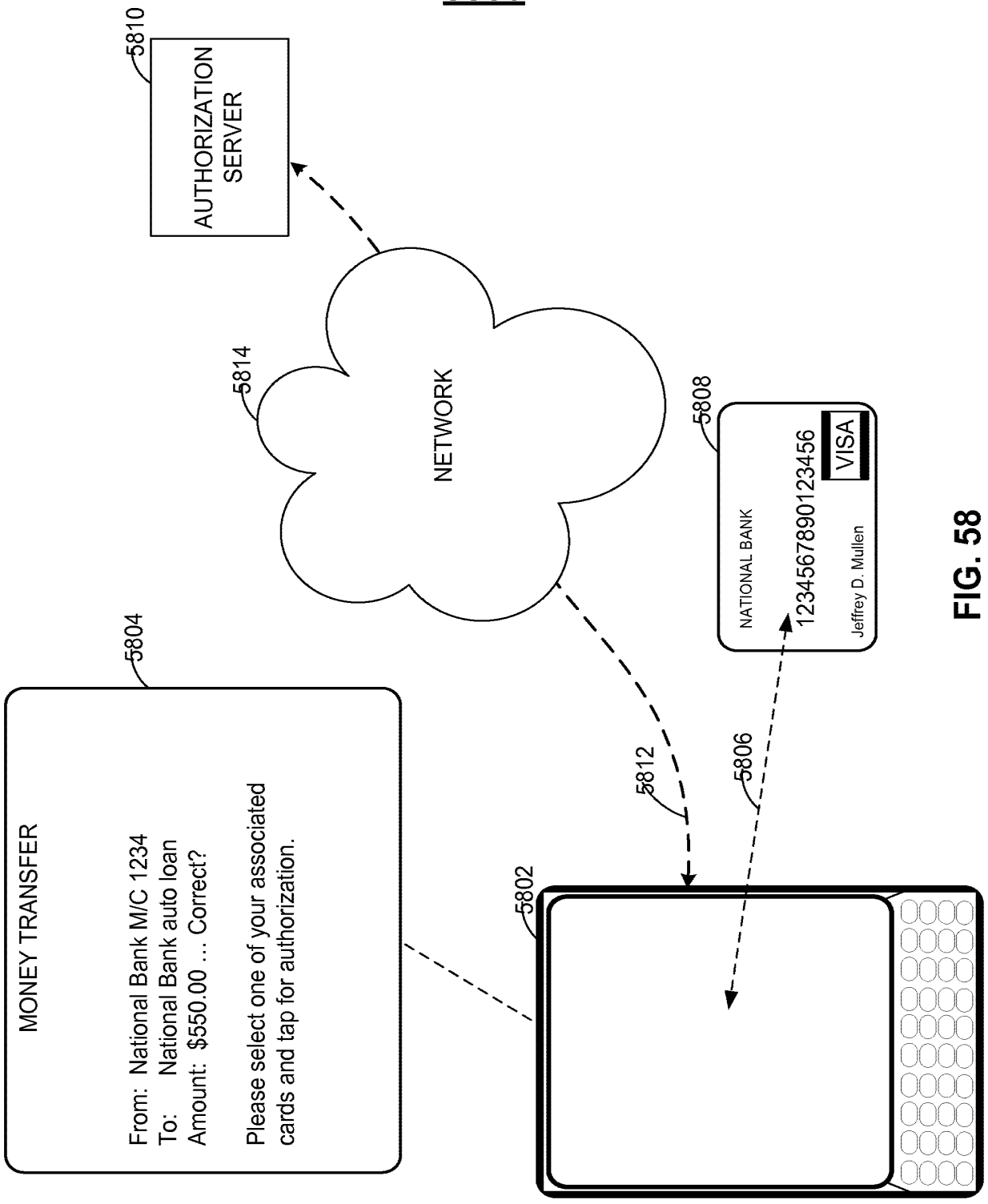



FIG. 58

59/73

5900

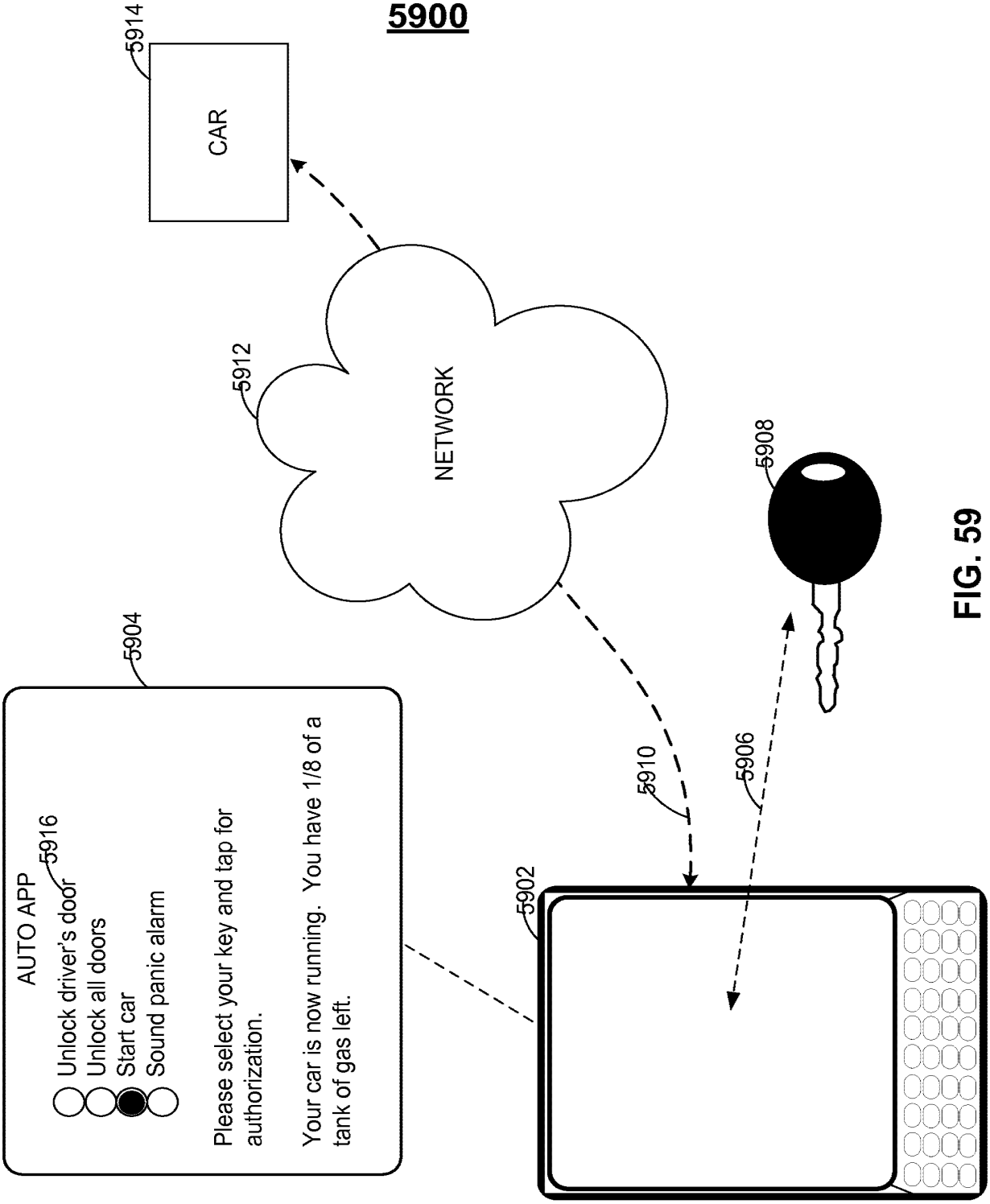



FIG. 59

6000

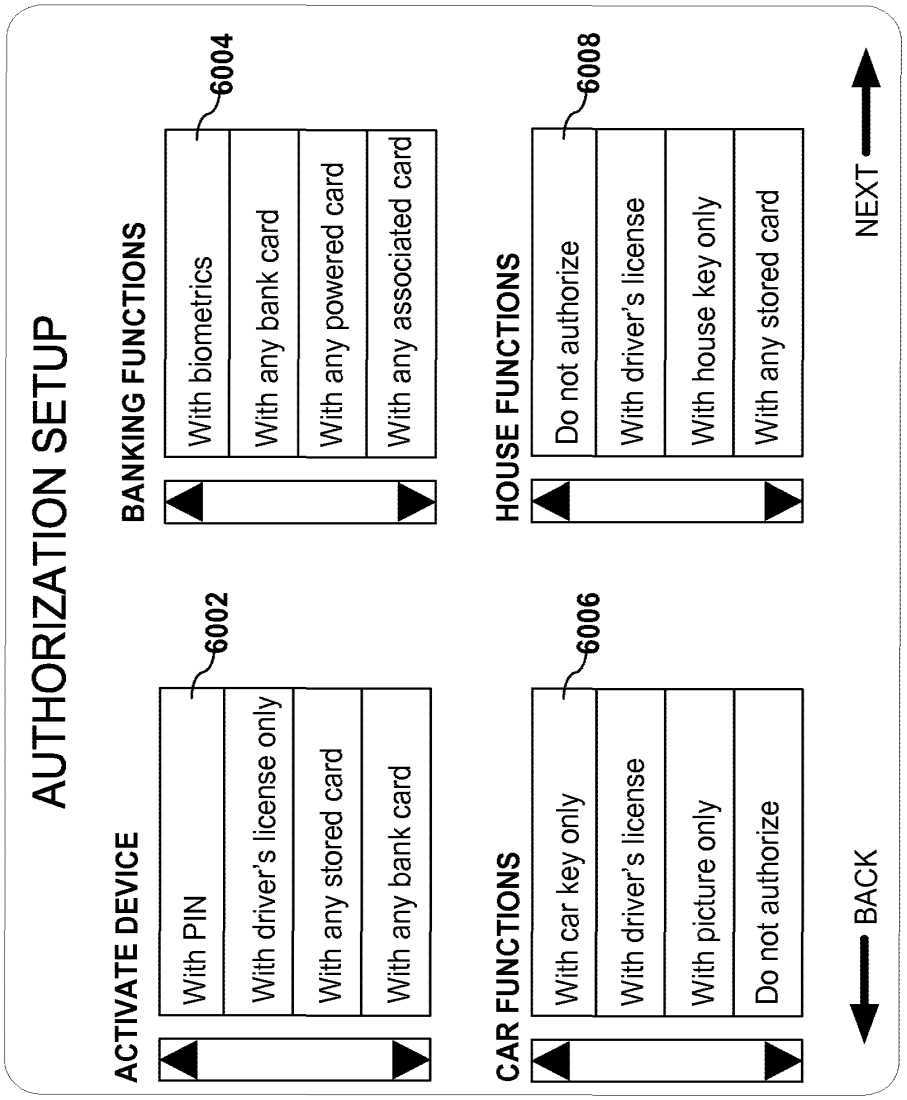

AUTHORIZATION SETUP
ACTIVATE DEVICE
6002
With PIN
With driver's license only
With any stored card
With any bank card
BANKING FUNCTIONS
6004
With biometrics
With any bank card
With any powered card
With any associated card
CAR FUNCTIONS
6006
With car key only
With driver's license
With picture only
Do not authorize
HOUSE FUNCTIONS
6008
Do not authorize
With driver's license
With house key only
With any stored card
BACK
NEXT

FIG. 60

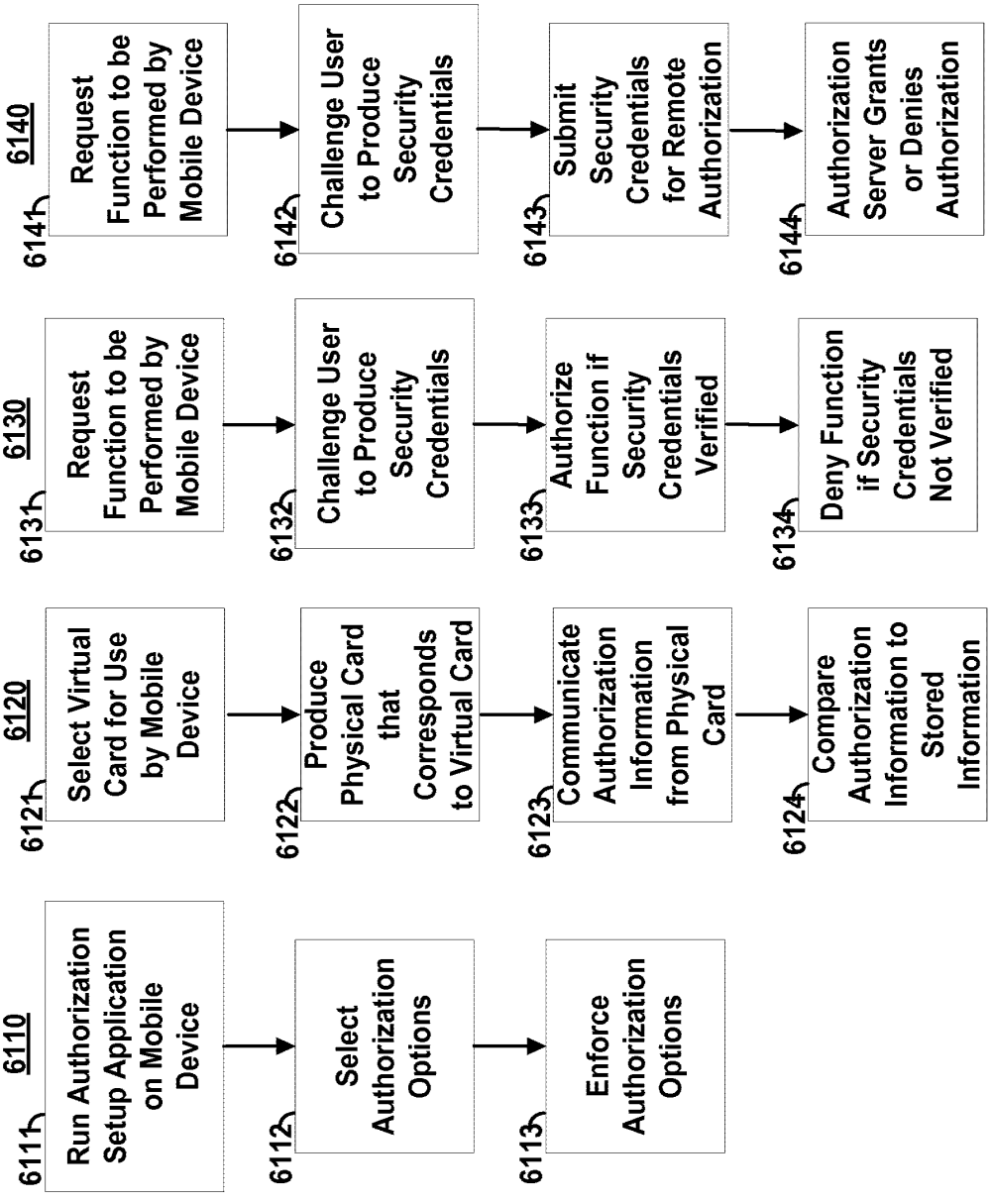

6110
6111
Run Authorization Setup Application on Mobile Device
6112
Select Authorization Options
6113
Enforce Authorization Options
6120
6121
Select Virtual Card for Use by Mobile Device
6122
Produce Physical Card that Corresponds to Virtual Card
6123
Communicate Authorization Information from Physical 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

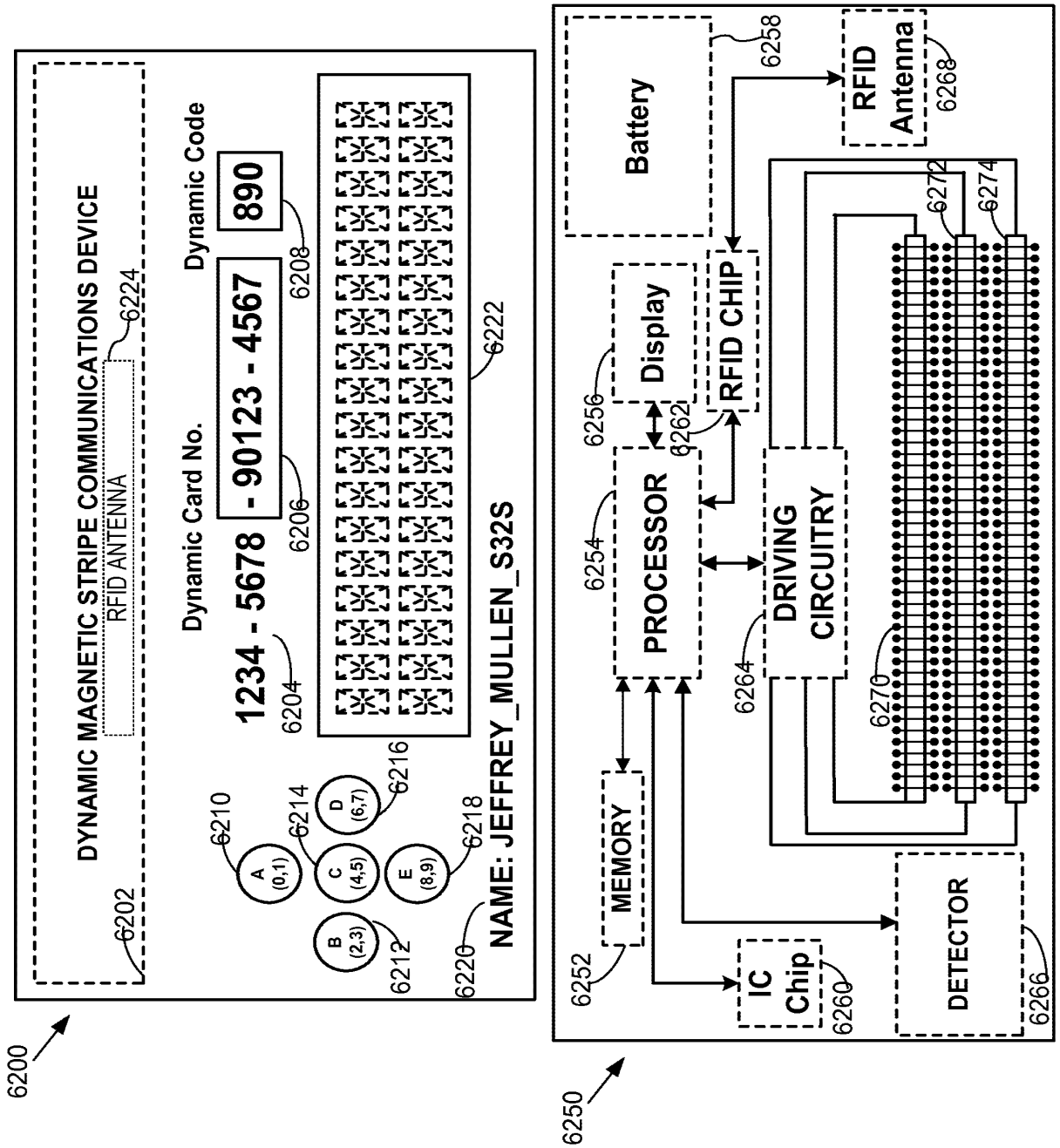

6200
DYNAMIC MAGNETIC STRIPE COMMUNICATIONS DEVICE
RFID ANTENNA
6224
6202
Dynamic Card No.
1234 - 5678 - 90123 - 4567
6204
6206
Dynamic Code
890
6208
6222
A (0,1)
B (2,3)
C (4,5)
D (6,7)
E (8,9)
6210
6212
6214
6216
6218
6220
NAME: JEFFREY_MULLEN_S32S
6250
Battery
6258
RFID Antenna
6268
Display
6256
RFID CHIP
6262
PROCESSOR
6254
DRIVING CIRCUITRY
6264
6270
6272
6274
MEMORY
6252
IC Chip
6260
DETECTOR
6266

FIG. 62

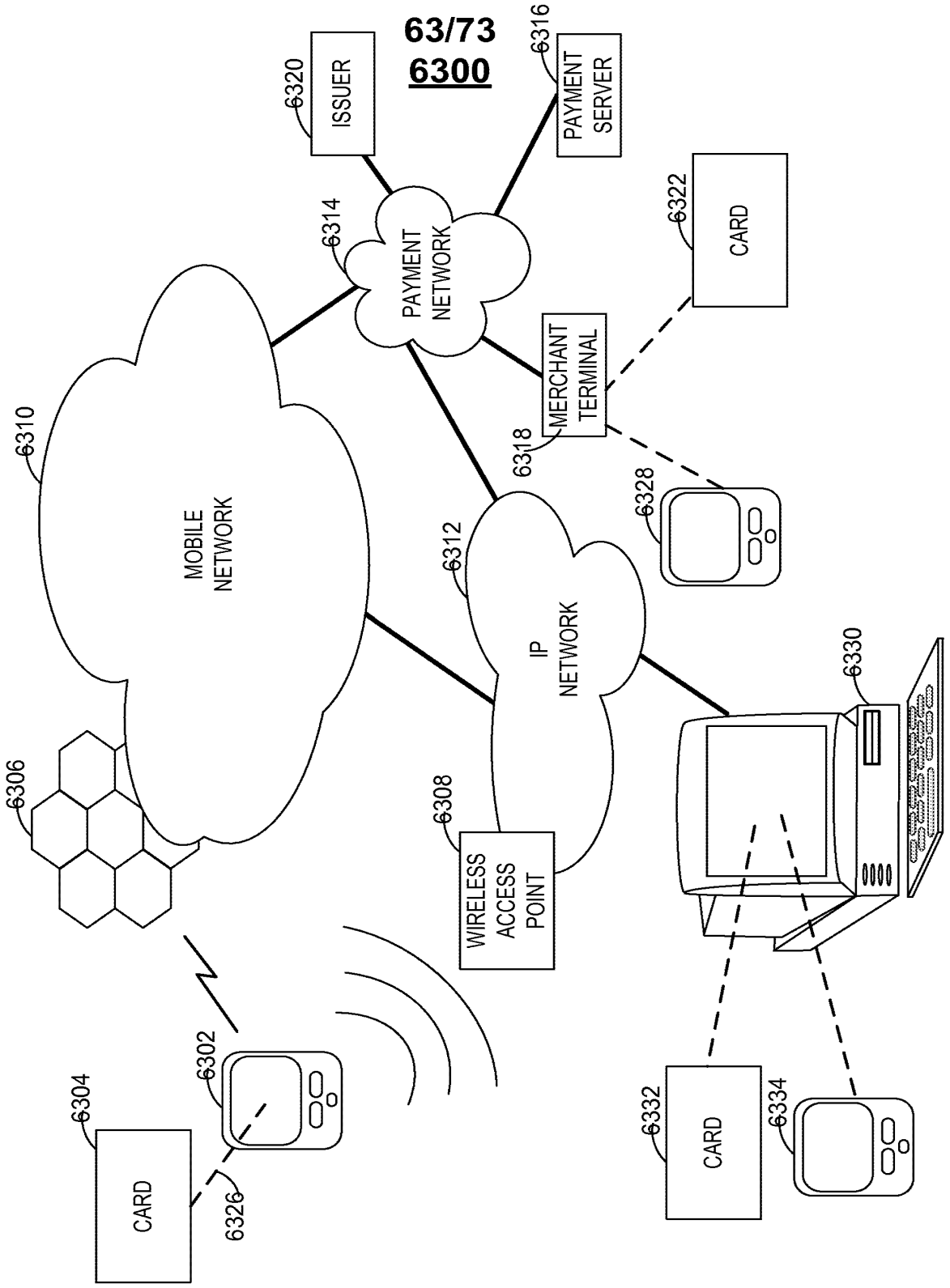

63/73
6300
6320
ISSUER
6316
PAYMENT SERVER
6314
PAYMENT NETWORK
6322
CARD
MERCHANT TERMINAL
6318
6310
MOBILE NETWORK
6328
6312
IP NETWORK
6330
6306
6308
WIRELESS ACCESS POINT
6302
6304
CARD
6326
6332
CARD
6334

FIG. 63

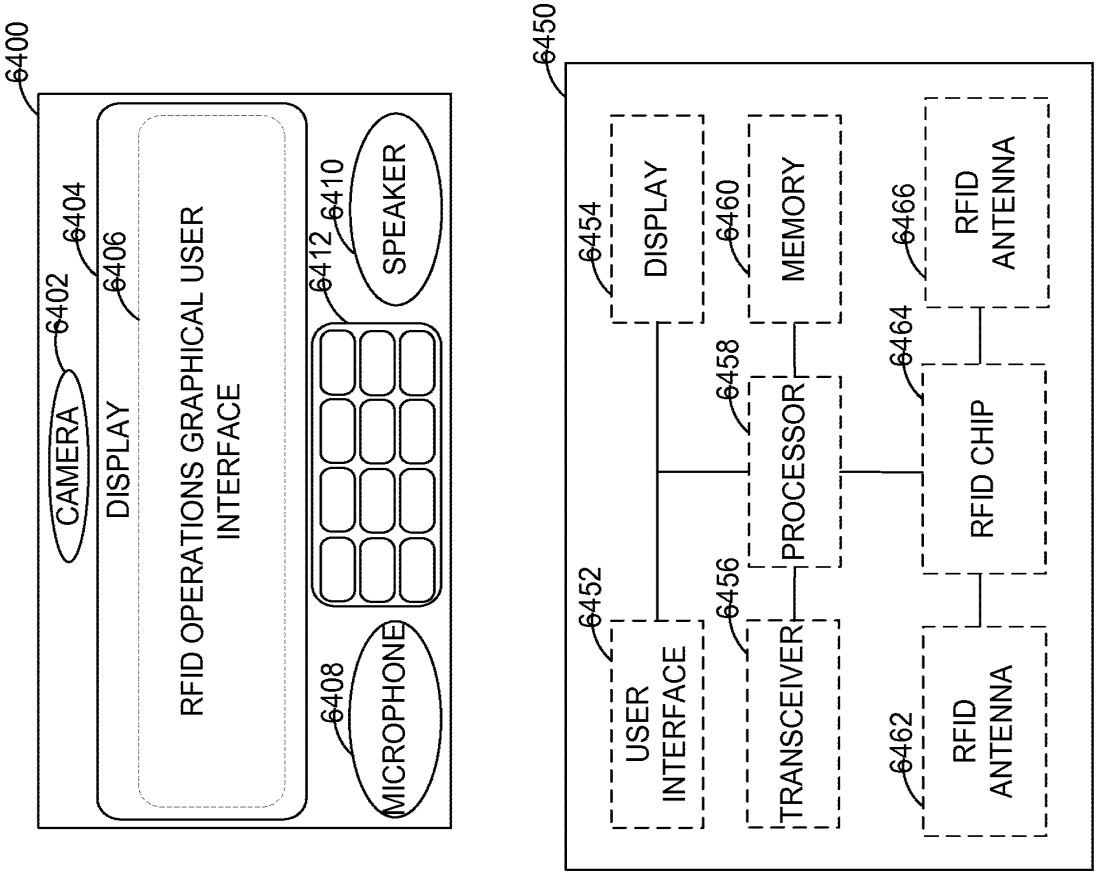

6400
CAMERA
6402
DISPLAY
6404
RFID OPERATIONS GRAPHICAL USER INTERFACE
6406
6408
MICROPHONE
6410
SPEAKER
6412
6450
USER INTERFACE
6452
TRANSCEIVER
6456
PROCESSOR
6458
DISPLAY
6454
MEMORY
6460
RFID CHIP
6464
RFID ANTENNA
6462
RFID ANTENNA
6466

FIG. 64

65/73
6500

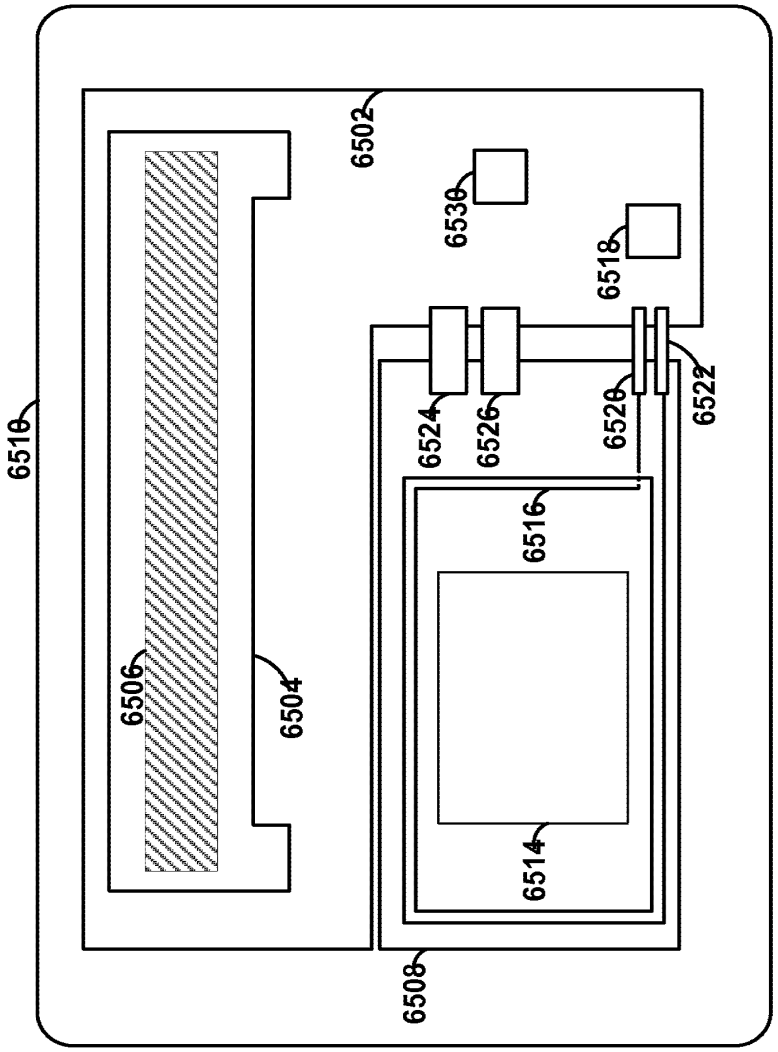



FIG. 65

66/73
6600

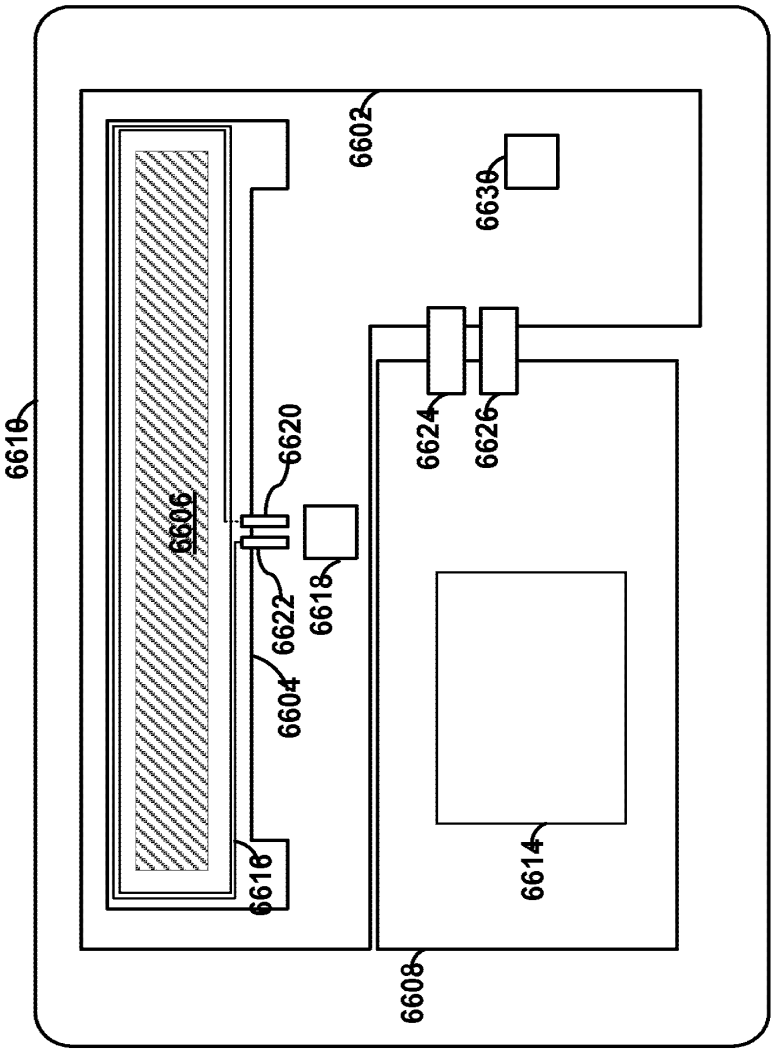



FIG. 66

67/73

6700

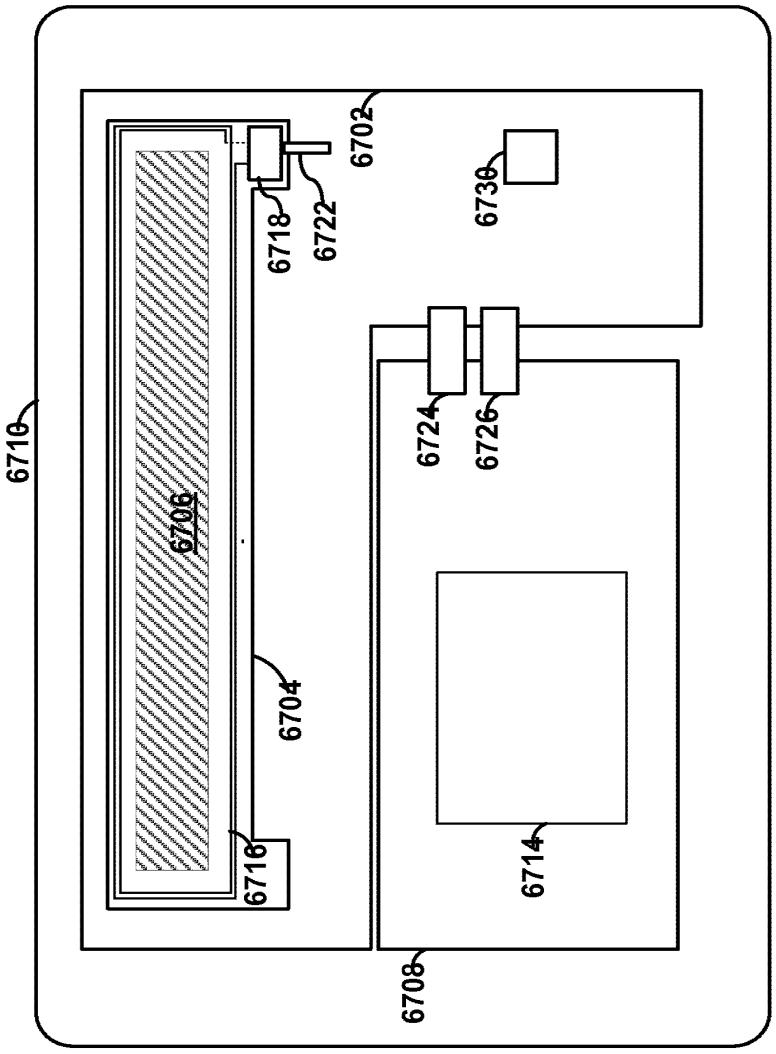



FIG. 67

68/73
6800

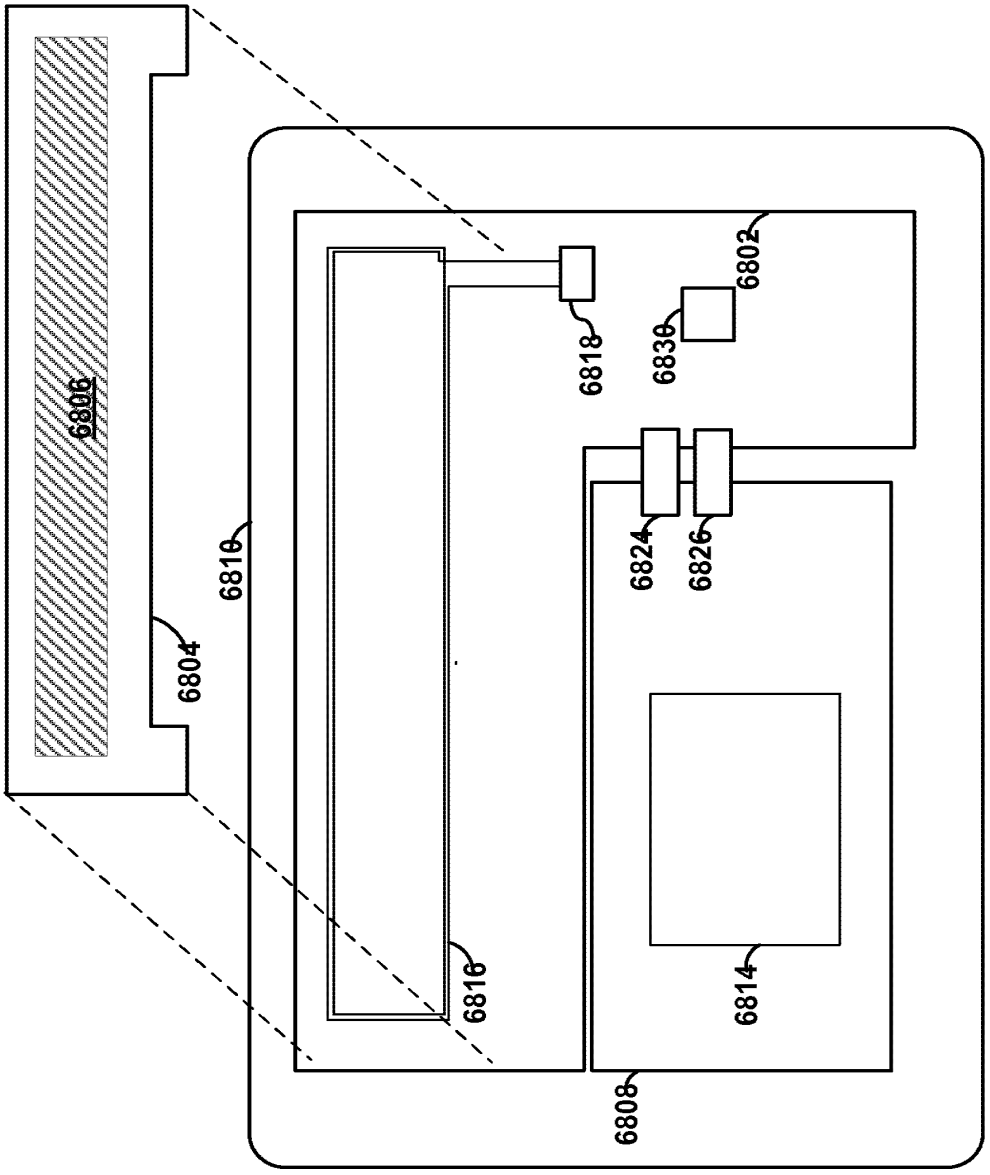



FIG. 68

69/73
6900

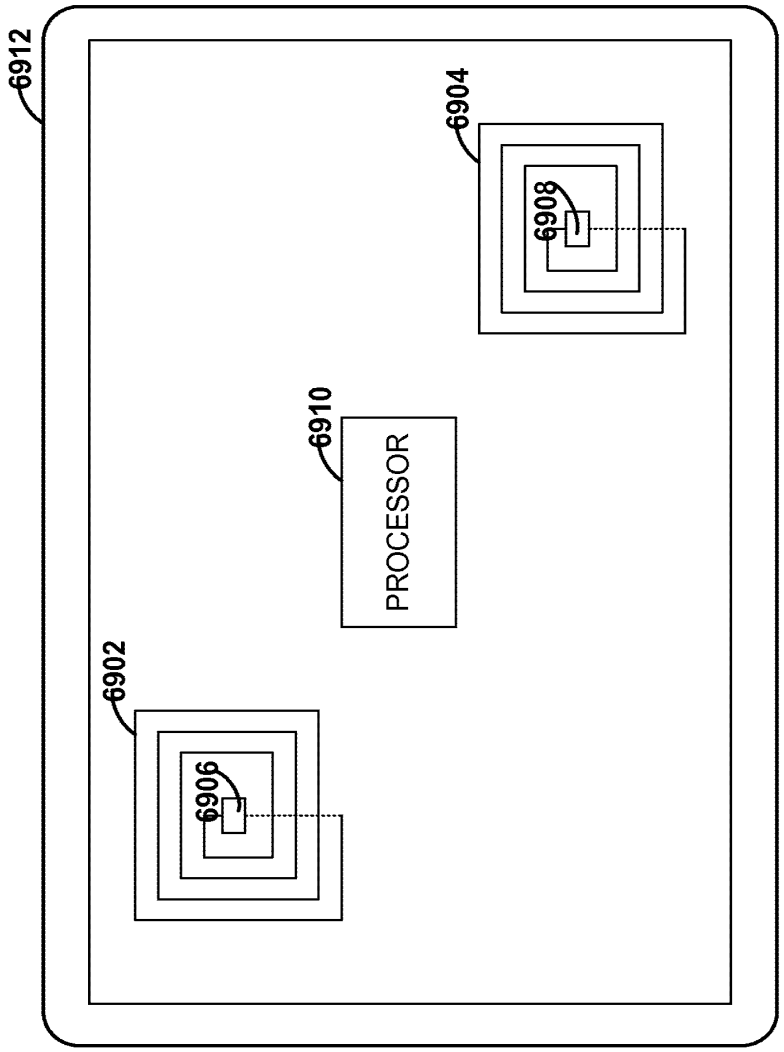



FIG. 69

70/73
7000

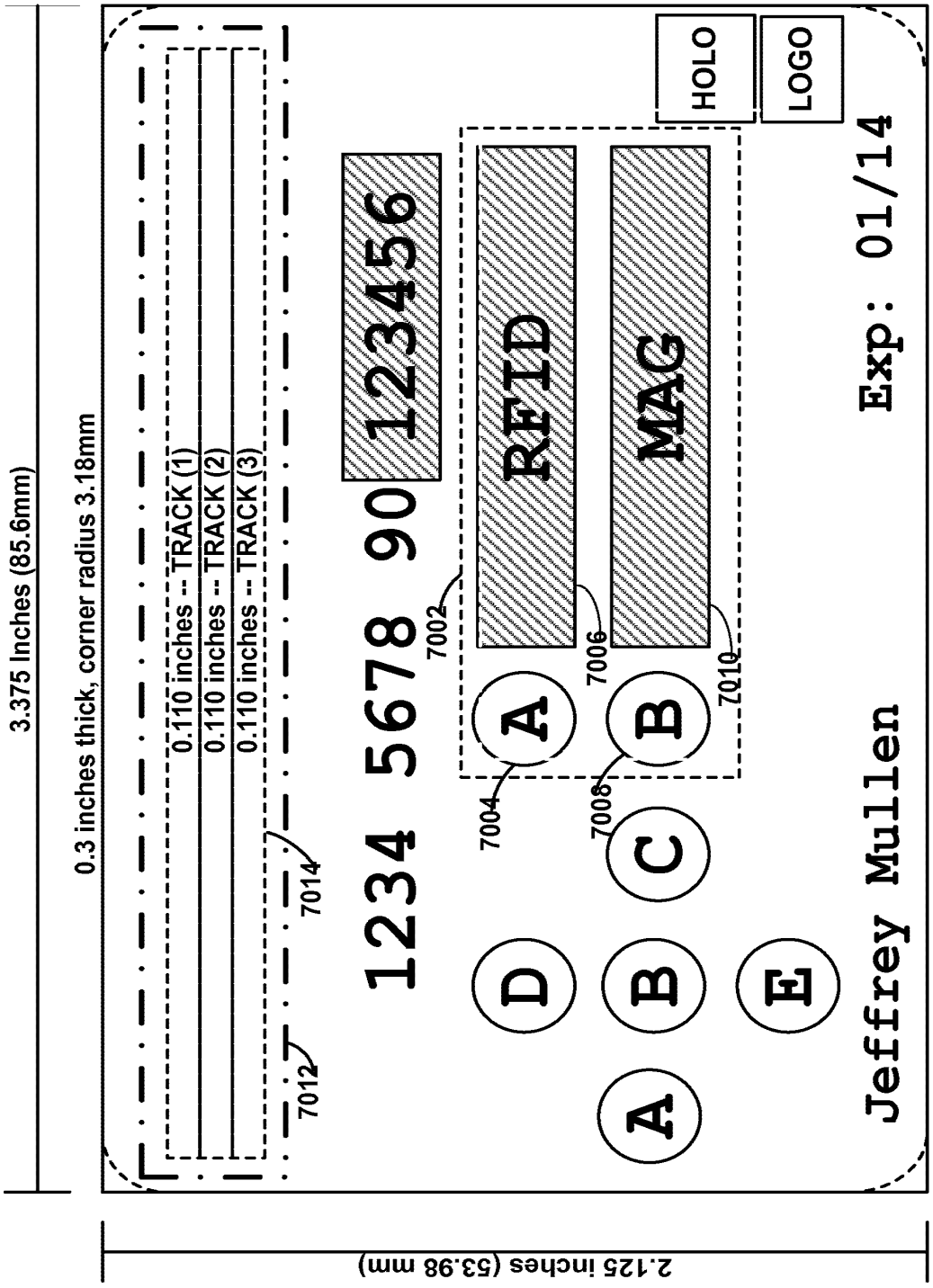



FIG. 70

71/73
7100

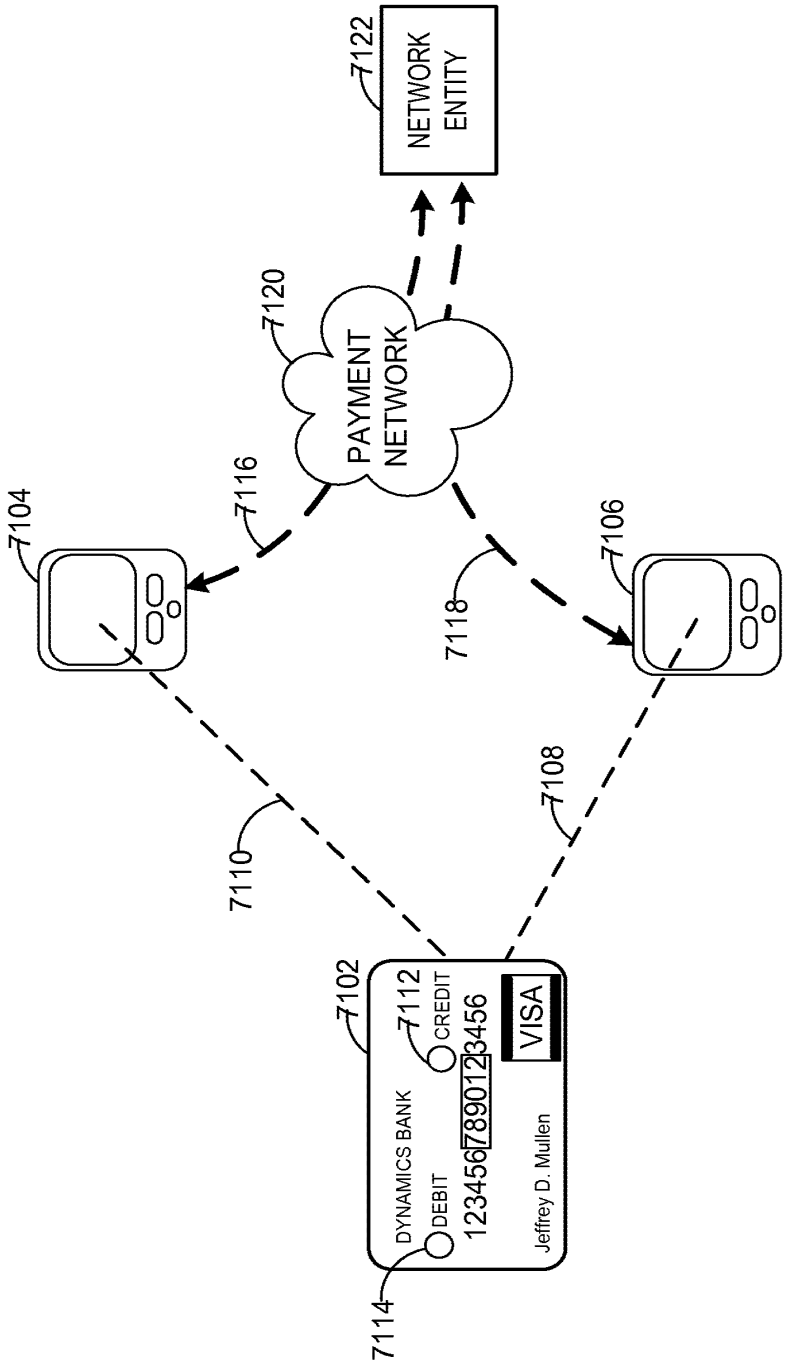



FIG. 71

72/73
7200

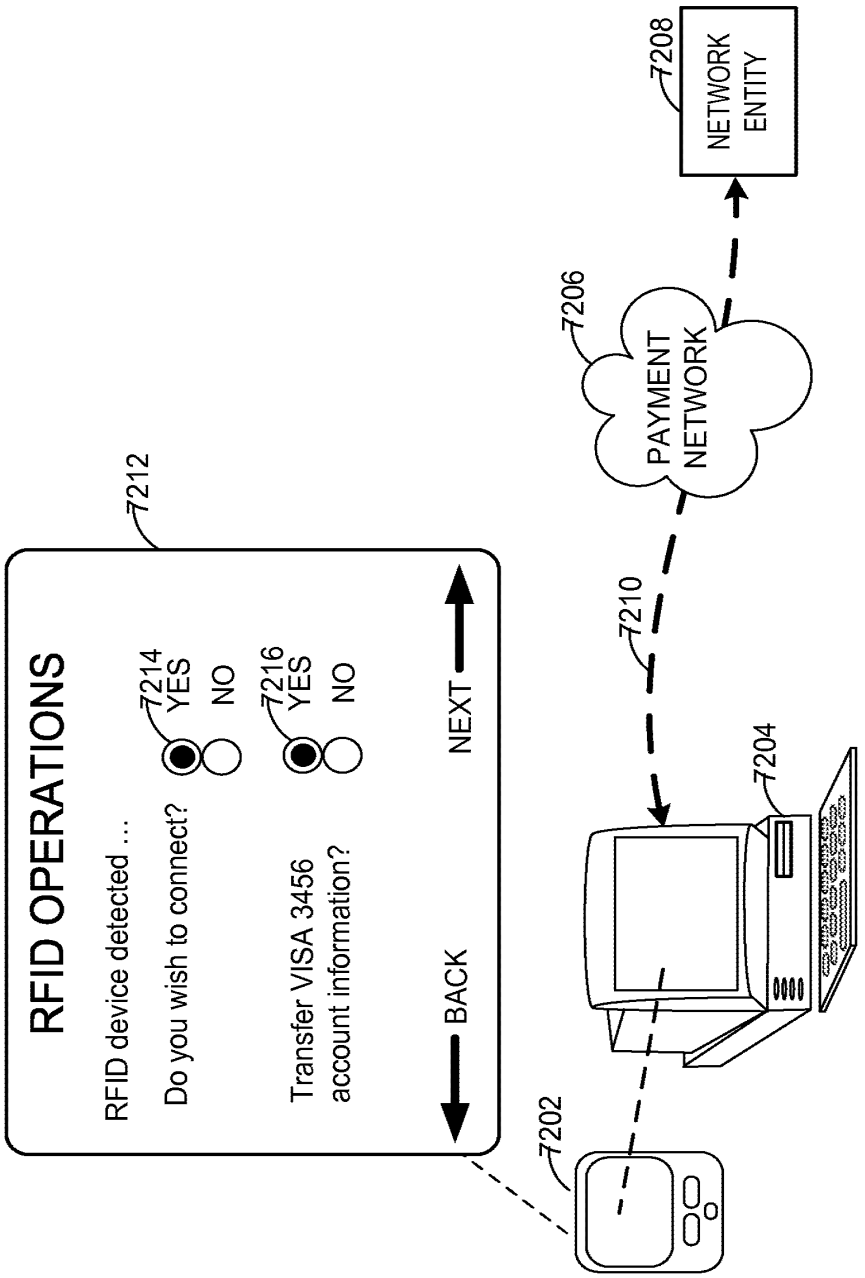



FIG. 72

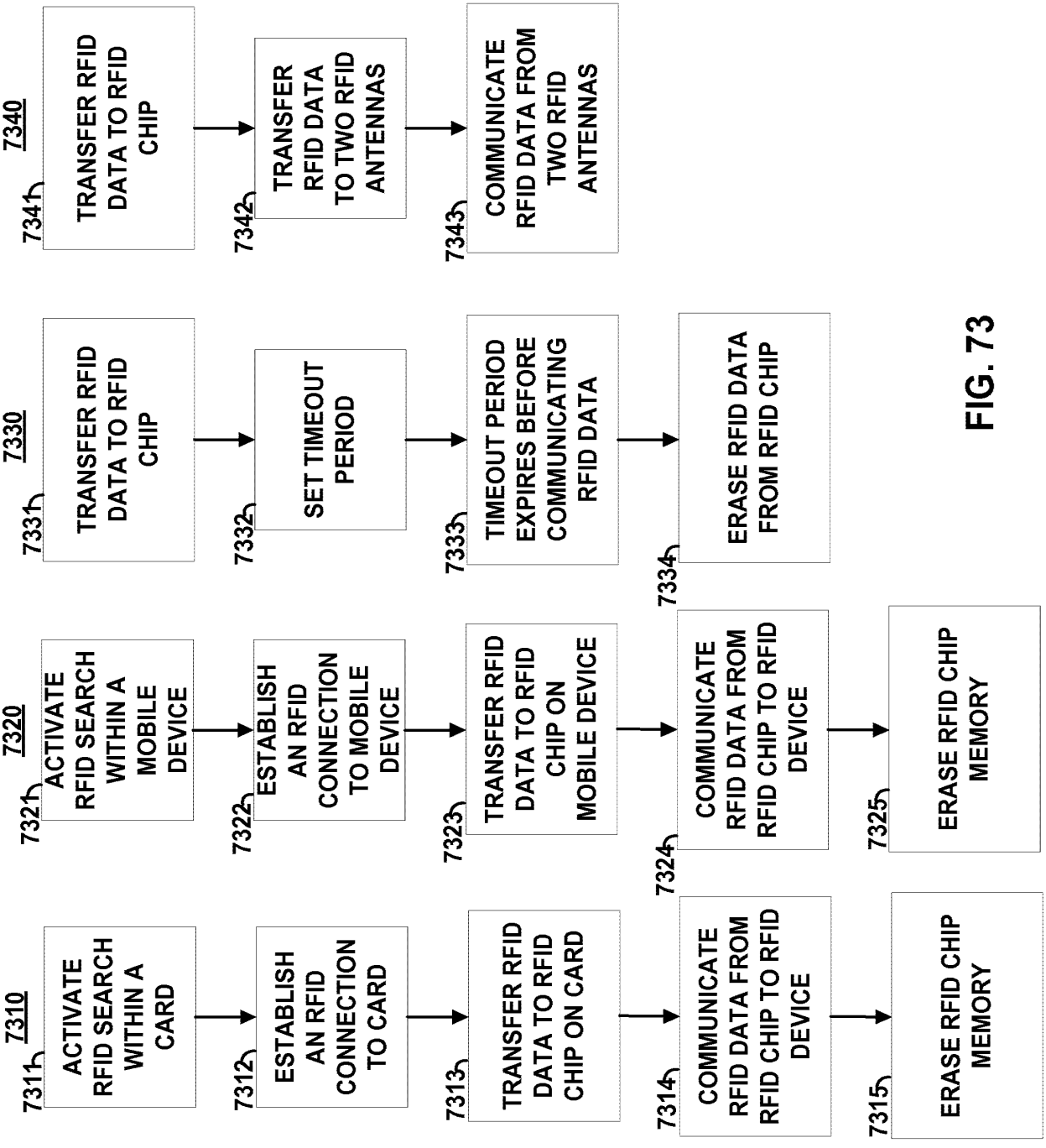

7310
7311
ACTIVATE RFID SEARCH WITHIN A CARD
7312
ESTABLISH AN RFID CONNECTION TO CARD
7313
TRANSFER RFID DATA TO RFID CHIP ON CARD
7314
COMMUNICATE RFID DATA FROM RFID CHIP TO RFID DEVICE
7315
ERASE RFID CHIP MEMORY
7320
7321
ACTIVATE RFID SEARCH WITHIN A MOBILE DEVICE
7322
ESTABLISH AN RFID CONNECTION 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, 8 1** |
| 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<br>**Mail Stop PCT, Attn: ISA/US, Commissioner for Patents**<br>**P.O. Box 1450, Alexandria, Virginia 22313-1450**<br>Facsimile No. **571-273-3201** | Authorized officer:<br>**Blaine R. Copenheaver**<br>**PCT Helpdesk: 571-272-4300**<br>**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.

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.

# 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<br>427eed86832963839eaf594865df5c2d49f6ac57 | no | 5 |

**Warnings:**

| Information: | | | | | |
|---|---|---|---|---|---|
| 2 | Foreign Reference | WO2012154915A1.pdf | 2516187<br>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.**

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/

# 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:<br>37 CFR 1.17 (Patent application and reexamination processing fees)<br>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<br>d75fd13af1fcf453d256bbf8830d5497825ed4fc | no | 2 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 2 | Fee Worksheet (SB06) | fee-info.pdf | 49236<br>6086a42e2680174242ef1816e5270c4d084152c9 | 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.**

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 | 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

**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.

## 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 | RATE($) | ADDITIONAL FEE($) | | RATE($) | ADDITIONAL FEE($) |
|---|---|---|---|---|---|---|---|---|---|---|
| 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.

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 |

| **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

EFS Web 2.2.12

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.

## 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

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.

## 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.

## 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.

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.

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).

**[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.

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.

**[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.

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.

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.

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.

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.

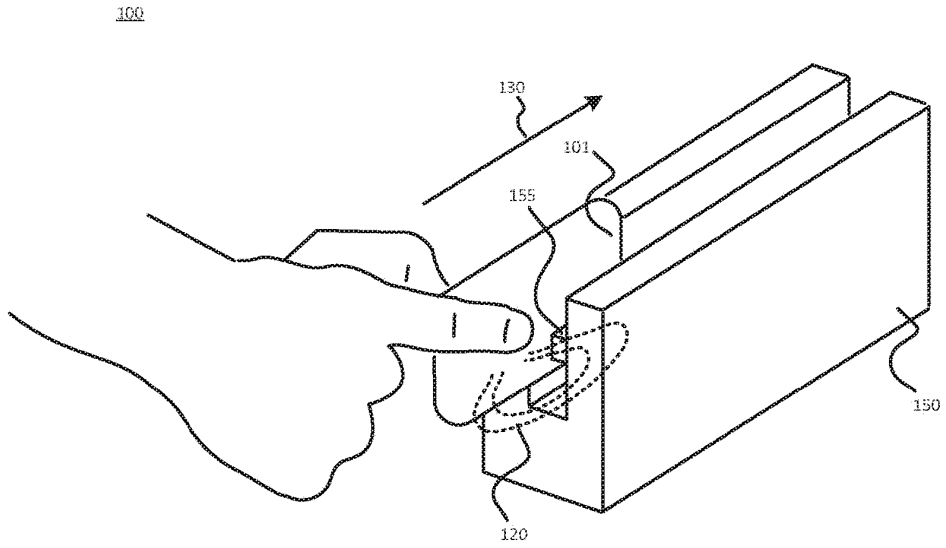



FIG. 1

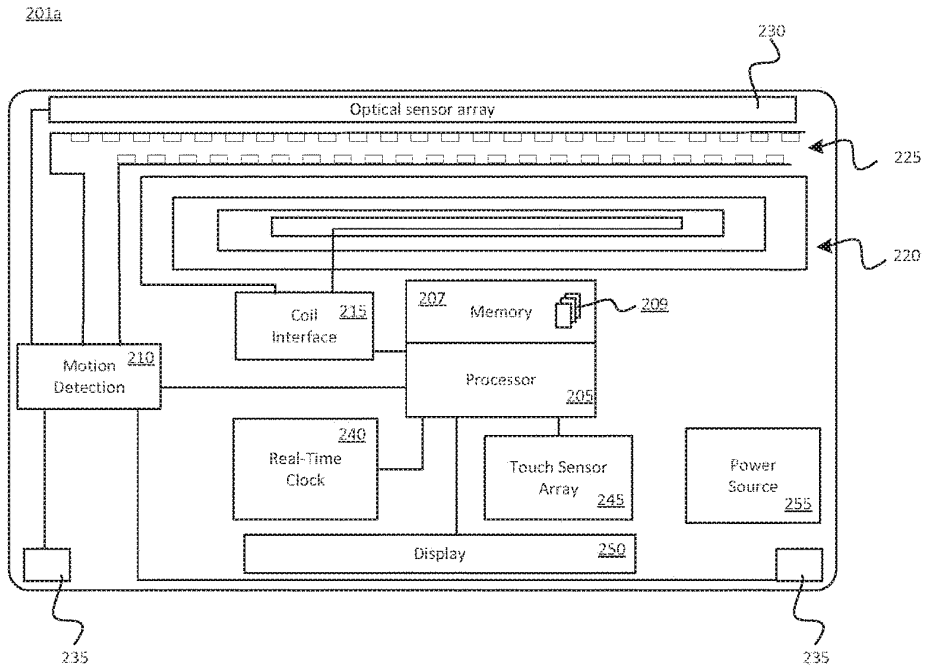

201a
230
Optical sensor array
225
220
Coil Interface 215
207 Memory
209
Motion Detection 210
Processor 205
240 Real-Time Clock
Touch Sensor Array 245
Power Source 255
Display 250
235
235

FIG. 2A

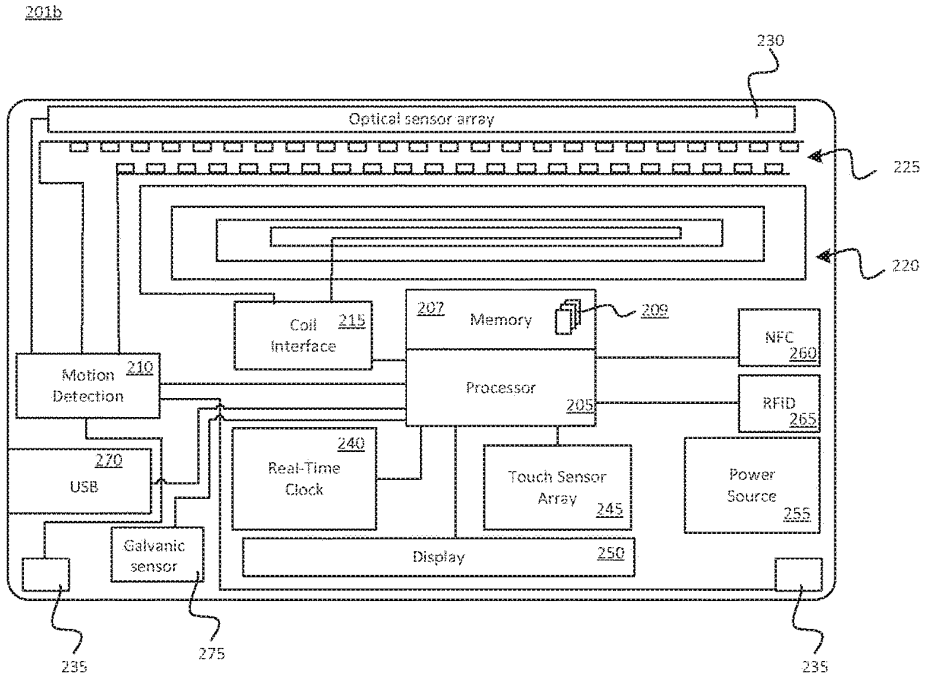

201b
230
Optical sensor array
225
220
Coil Interface 215
207 Memory
209
NFC 260
Motion Detection 210
Processor 205
RFID 265
240 Real-Time Clock
270 USB
Touch Sensor Array 245
Power Source 255
Galvanic sensor
Display 250
235
275
235

FIG. 2B

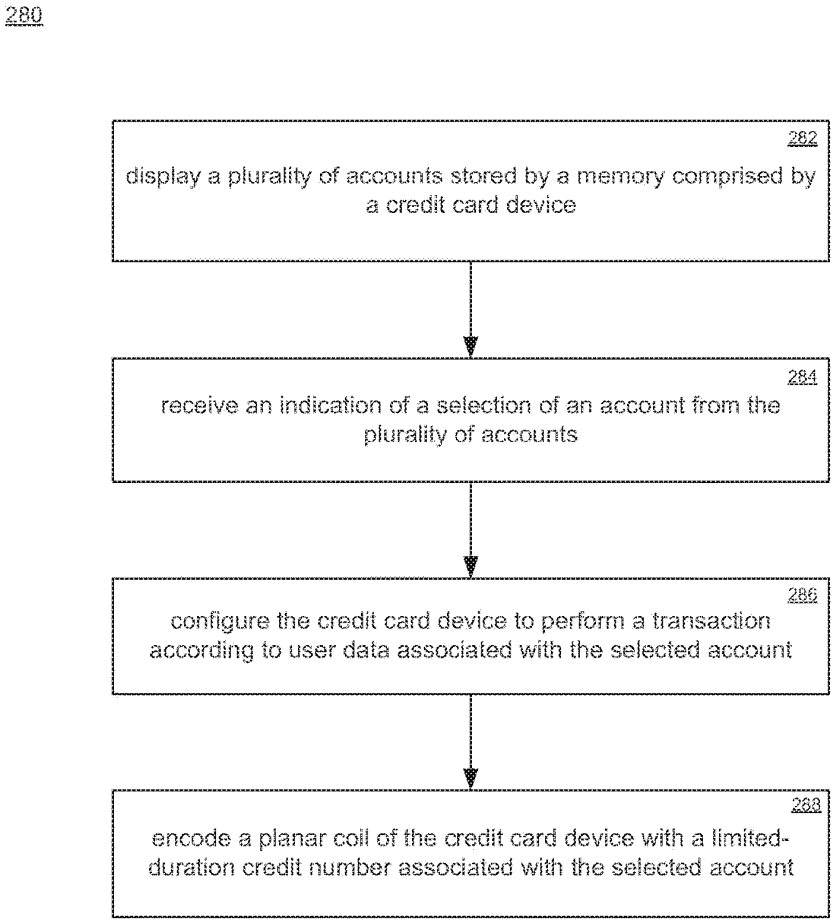

280
282
display a plurality of accounts stored by a memory comprised by a credit card device
284
receive an indication of a selection of an account from the plurality of accounts
286
configure the credit card device to perform a transaction according to user data associated with the selected account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

FIG. 2C

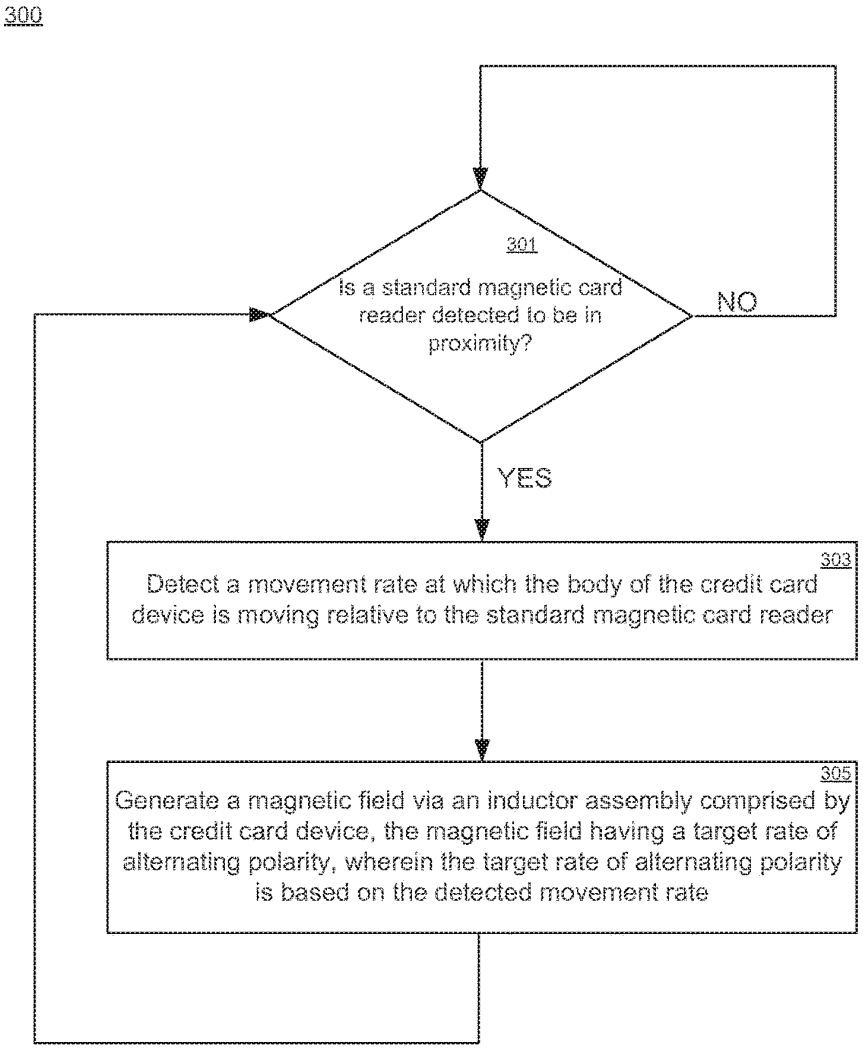

300
301
Is a standard magnetic card reader detected to be in proximity?
NO
YES
303
Detect a movement rate at which the body of the credit card device is moving relative to the standard magnetic card reader
305
Generate a magnetic field via an inductor assembly comprised by the credit card device, the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

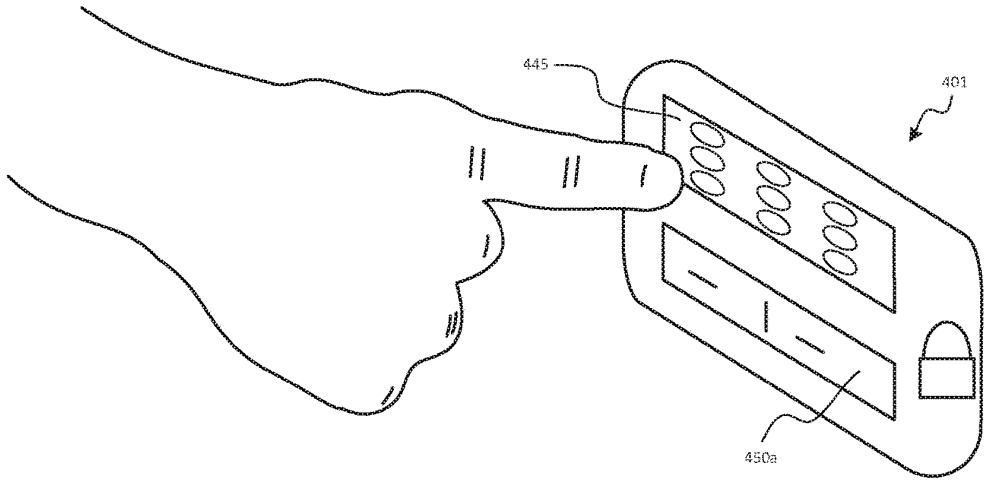



FIG. 4A

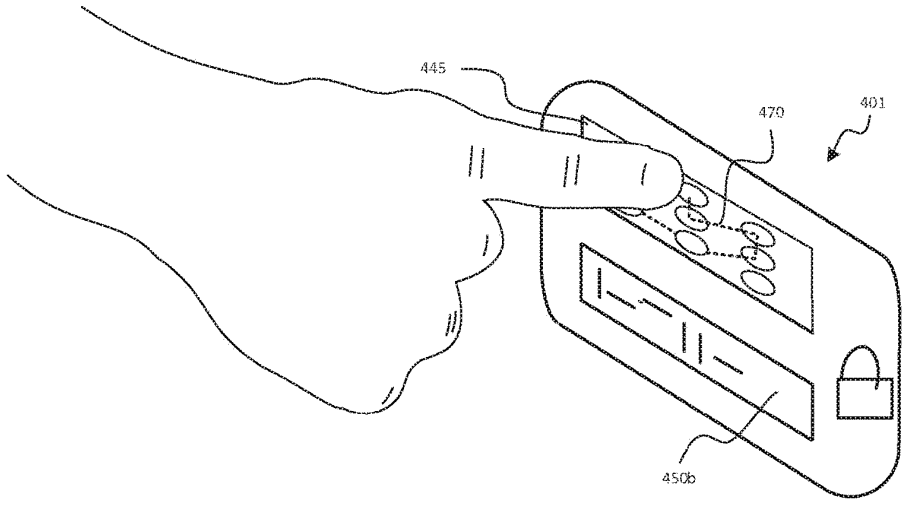



FIG. 4B

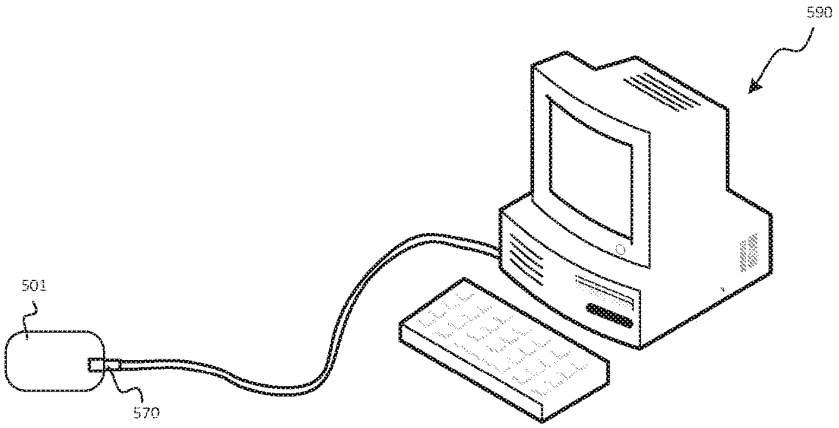



FIG. 5

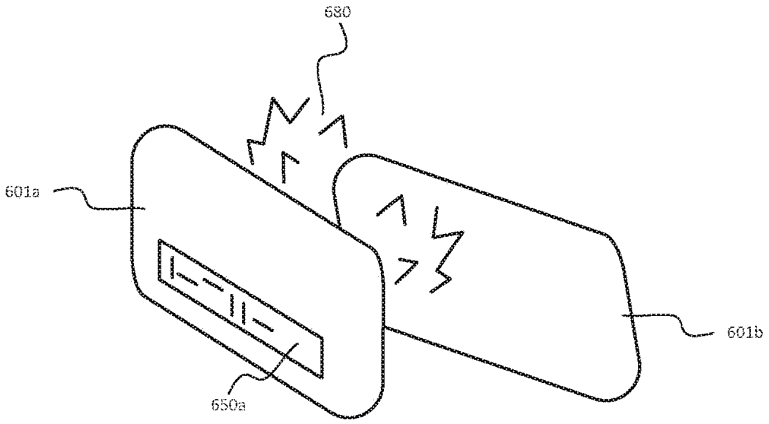



FIG. 6

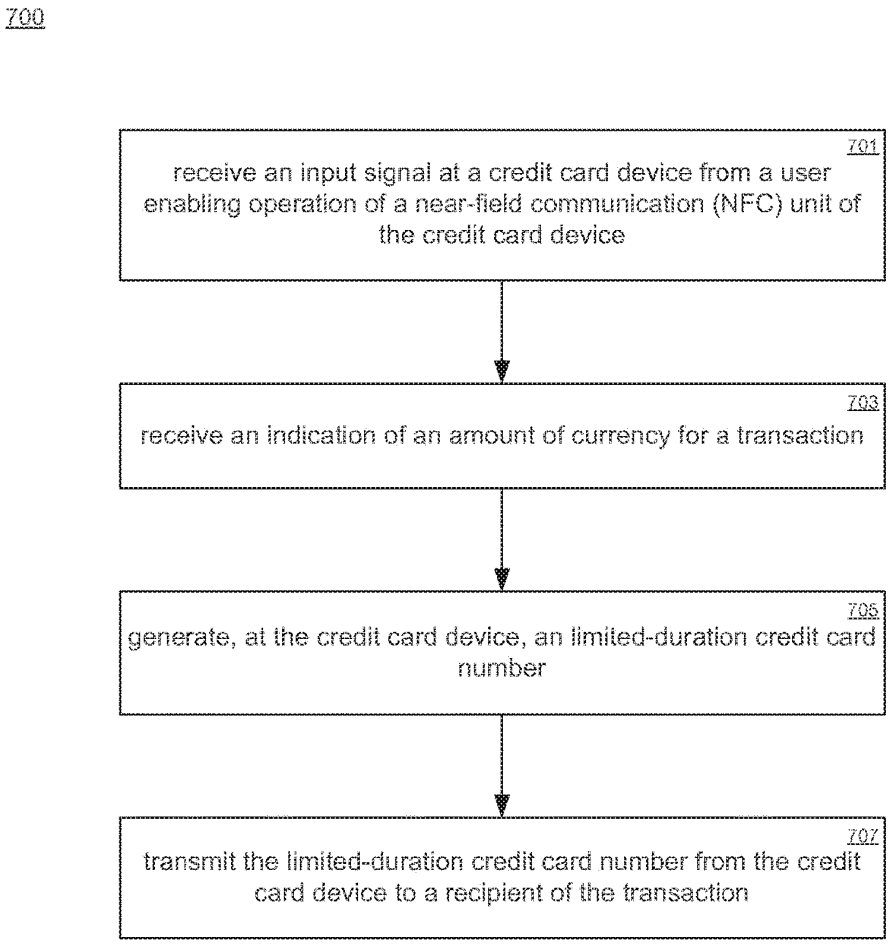

700
701
receive an input signal at a credit card device from a user enabling operation of a near-field communication (NFC) unit of the credit card device
703
receive an indication of an amount of currency for a transaction
705
generate, at the credit card device, an limited-duration credit card number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

- [■] 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<br>62b4a63f295cdc1f5a0f24a9ecfb06d0ff3629a5 | no | 9 |

**Warnings:**

| | | | | | |
|---|---|---|---|---|---|
| **Information:** | | | | | |
| 2 | | WYAT-0002USD1C1C1C1C1C_CON_APP_11-16-2021.pdf | 250438<br>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<br>c221514b3dda9b2eb45b3f19858633199bee3641 | no | 7 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 4 | Oath or Declaration filed | WYAT-0002USD1C1C1C_DEC_FROM_PARENT_10-20-2020.pdf | 69977<br>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.**