AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas - Waco Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00288	March 17, 2022	Western District of Texas - Waco Division

PLAINTIFF	DEFENDANT
Fintiv, Inc.	PayPal Holdings, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,538,845	September 17, 2013	Fintiv, Inc.
2	9,892,386	February 13, 2018	Fintiv, Inc.
3	11,120,413	September 14, 2021	Fintiv, Inc.
4	9,208,488	December 8, 2015	Fintiv, Inc.
5	10,438,196	October 8, 2019	Fintiv, Inc.

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

PATENT

Docket No. 18756.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

	Michael A. Liberty et al.	
Serial No.:	13/484,199	
Filed:	May 30, 2012	Art Unit 3691
Confirmation No.:	5095	
For:	*MONETARY TRANSACTION SYSTEM*	
Examiner:	Edward Chang	
Patent No.:	8538845 B2	
Issue Date:	September 17, 2013	

REQUEST FOR A CERTIFICATE OF CORRECTION UNDER 37 C.F.R. § 1.323

Attention: Certificate of Corrections Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

In accordance with the provisions of 37 C.F.R. § 1.323, which implements 35 U.S.C. § 255, the Director is respectfully requested to issue a Certificate of Correction to correct mistakes in the above-identified patent. The enclosed Patent Office Form PTO/SB/44 reflects the desired corrections.

Payment in the amount of $160, as set forth in 37 C.F.R. § 1.20(a) is submitted herewith to cover the costs for issuance of the requested Certificate of Correction. The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to Deposit Account No. 23-3178: (1) any filing fees required under 37 CFR § 1.16; (2) any patent application and reexamination processing fees under

37 CFR § 1.17; and/or (3) any post issuance fees under 37 CFR § 1.20. In addition, if any additional extension of time is required, which has not otherwise been requested, please consider this a petition therefore and charge any additional fees that may be required to Deposit Account No. 23-3178.

Dated this 13th day of May 2021.

Respectfully submitted,

/John C. Stringham Reg. No. 40831/

JOHN C. STRINGHAM
Attorney for Applicant
Registration No.: 40831
Customer No.: 22913

WORKMAN NYDEGGER
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111
Phone: 801-533-9800
Fax: 801-328-1707

JCS:re
(41123166.1)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 3 of 1360

PTO/SB/44 (09-07)
Approved for use through 03/31/2023. OMB 0651-0033
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.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 8538845

APPLICATION NO.: 13/484199

ISSUE DATE : September 17, 2013

INVENTOR(S) : Michael A. Liberty

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

COVER SHEET

Item (75) , Inventors, change "Michael A. Liberty" to

--Michael A. Liberty, Windmere, (FL);
Felipe Fernandes, Austin (TX)--.

MAILING ADDRESS OF SENDER (Please do not use Customer Number below):

Workman Nydegger
60 East South Temple #1000
Salt Lake City, UT 84111

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. 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 1.0 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: Attention Certificate of Corrections Branch, 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.

Electronic Patent Application Fee Transmittal

Application Number:	13484199
Filing Date:	30 May 2012
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Filer:	John C. Stringham/Ralene Eller
Attorney Docket Number:	18756.8.1.1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
CERTIFICATE OF CORRECTION	1811	1	160	160

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	160

Electronic Acknowledgement Receipt	
EFS ID:	42717952
Application Number:	13484199
International Application Number:	
Confirmation Number:	5095
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Customer Number:	22913
Filer:	John C. Stringham/Ralene Eller
Filer Authorized By:	John C. Stringham
Attorney Docket Number:	18756.8.1.1
Receipt Date:	13-MAY-2021
Filing Date:	30 MAY 2012
Time Stamp:	16:18:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$160
RAM confirmation Number	E20215CG19323335
Deposit Account	233178
Authorized User	Ralene Eller
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 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	Request for Certificate of Correction	18756 8 1 1 2021 05 13 Request-for-Certificate-of-Correction.pdf	93380 220b6b9a576c775327cae:37a°055ca2521 [illegible]	no	2
Warnings:					
Information:					
2	Request for Certificate of Correction	18756 8 1 1 2021 05 13 Certificate-of-Correction-Fernandes.PDF	257595 [illegible]	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee info.pdf	30096 [illegible]	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	381071		

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
13/484,199	05/30/2012	Michael A. Liberty	18756.8.1.1

CONFIRMATION NO. 5095

22913
Workman Nydegger
60 East South Temple
Suite 1000
Salt Lake City, UT 84111

POA ACCEPTANCE LETTER

OC000000114936477

Date Mailed: 02/25/2020

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/20/2020.

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/

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 10 of 1360

VIA *e*FILE Docket No. 18756.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	Michael A. Liberty	)
		)
Serial No.:	13/484199	)
		)
Filed:	May 30, 2012	)
		)
Patent No.	8538845	)
		)
Issued:	September 17, 2013	)
		)
Confirmation No.:	5095	)
		)
FOR:	Monetary Transaction System	)
		)
Examiner:	n/a	)
		)
Customer No.:	22913	)

REQUEST TO CORRECT INVENTORSHIP UNDER 37 C.F.R. § 1.324

Via *e*File
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Assignee desires to correct inventorship of the above-identified United States patent under 37 C.F.R. §1.324.

As set forth in 37 C.F.R. § 1.324, Assignee requests to **add** the following named person as an inventor in the above-identified patent application:

Inventor: Felipe Fernandes
Residence: US
Citizenship: US

Enclosed:

X Statement from inventor Felipe Fernandes that the inventorship error occurred without any deceptive intention.

X Statement from inventor Michael A. Liberty that the inventorship error occurred without any deceptive intention.

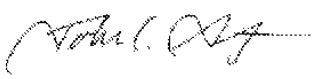
X Consent of Assignee to Correct Inventorship.

X The $150.00 fee for correction of inventorship of this patent under 37 C.F.R. § 1.20(b).

The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to Deposit Account No. 23-3178: any post issuance fees under 37 CFR § 1.20. In addition, please consider this a petition therefor and charge any additional fees that may be required to Deposit Account No. 23-3178.

Dated this 20th day of February, 2020

Respectfully submitted,



John C. Stringham
Registration No. 40831
Attorney for Applicant
Customer No. 022913

JCS:rc
43327341.1

VIA *e*FILE Docket No. 18756.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	Michael A. Liberty
Serial No.:	13/484199
Filed:	May 30, 2012
Patent No.	8538845
Issued:	September 17, 2013
Confirmation No.:	5095
FOR:	Monetary Transaction System
Examiner:	n/a
Customer No.:	22913

STATEMENT AND WRITTEN CONSENT OF
ASSIGNEE PURSUANT TO 37 C.F.R. § 1.324 and § 3.73(b)

VIA *e*FILE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The undersigned, Mike Love, declares that he is the President of FINTIV, INC. and that he is authorized to execute this statement on behalf of FINTIV, INC. organized and existing under laws of Delaware and that FINTIV, INC. is the Assignee of the right, title and interest of the above-identified application, as shown in the chain of title from the original named inventors of the patent application identified above, to FINTIV, INC.. From the original named inventors to MOZIDO, LLC as recorded in the United States Patent and Trademark Office at Reel 028295, Frame 0750; from MOZIDO, LLC to MOZIDO, INC. recorded at Reel 031769, Frame 0677, and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 13 of 1360

from MOZIDO, INC. to FINTIV, INC recorded by virtue of a name change at Reel 051276, frame 0649.

FINTIV, INC. consents to the change of inventorship set forth in the accompanying request that adds Felipe Fernandes as a joint inventor of the above-identified patent application.

Signed this 1 day of February, 2020.

FINTIV, INC.

Mike Love
Title: President

JCJ:re
43327336.1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 14 of 1360

VIA *e*FILE Docket No. 18756.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	Michael A. Liberty
Serial No.:	13/484199
Filed:	May 30, 2012
Patent No.	8538845
Issued:	September 17, 2013
Confirmation No.:	5095
FOR:	Monetary Transaction System
Examiner:	n/a
Customer No.:	22913

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

STATEMENT OF CURRENT INVENTOR– Michael A. Liberty
Under 37 CFR 1.324(b)(2)

Sir:

I, Michael A. Liberty, current inventor for the above-identified application, hereby agree to the addition of Felipe Fernandes as an inventor, and have no disagreement with regard to the requested change.

Dated this 28 day of Jan, 2020.

Michael A. Liberty

43327344.1

VIA *e*FILE

Docket No. 18756.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	Michael A. Liberty	)
		)
Serial No.:	13/484199	)
		)
Filed:	May 30, 2012	)
		)
Patent No.	8538845	)
		)
Issued:	September 17, 2013	)
		)
Confirmation No.:	5095	)
		)
FOR:	Monetary Transaction System	)
		)
Examiner:	n/a	)
		)
Customer No.:	22913	)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

STATEMENT OF ADDED INVENTOR under 37 CFR 1.324(b)(1)

Sir:

I, Felipe Fernandes, joint inventor for the above-identified application, hereby state that the error in inventorship occurred without deceptive intent on my part, and respectfully request that I be added as a joint inventor on the above-referenced application.

Dated this 3 day of FEBRUARY, 2020.

Felipe Fernandes

PTO/SB/81 (01-09)
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 OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	13/484199
Filing Date	May 13, 2012
First Named Inventor	Michael A. Liberty
Title	Monetary Transaction System
Art Unit	
Examiner Name	
Attorney Docket Number	18756.8.1.1

I hereby revoke all previous powers of attorney given in the above-identified application.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

022913

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application 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/Inventor.

OR

☒ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Applicant or Assignee of Record

Signature		Date	4/1/2020
Name	Mike Love	Telephone	512 904 5789
Title and Company	President, FINTIV, INC.		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. 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 1.31, 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.

PTO/SB/96 (07-09)
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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Michael A. Liberty

Application No./Patent No.: 13/484199 Filed/Issue Date: May 13, 2012

Titled: Monetary Transaction System

FINTIV, INC. , a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. [X] the assignee of the entire right, title, and interest in;

2. [ ] an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is _____ %); or

3. [ ] the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

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 therefore is attached.

OR

B. [X] A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Michael A. Liberty To: Mozido, LLC

The document was recorded in the United States Patent and Trademark Office at Reel 028698, Frame 0135, or for which a copy thereof is attached.

2. From: Mozido, LLC To: Mozido, Inc.

The document was recorded in the United States Patent and Trademark Office at Reel 031769, Frame 0677, or for which a copy thereof is attached.

3. From: Mozido, Inc. To: Fintiv, Inc.

The document was recorded in the United States Patent and Trademark Office at Reel 051276, Frame 0649, or for which a copy thereof is attached.

[ ] Additional documents in the chain of title are listed on a supplemental sheet(s).

[X] As required by 37 CFR 3.73(b)(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.

/John C. Stringham/ — Signature

February 20, 2020 — Date

John C. Stringham — Printed or Typed Name

Attorney for applicant — Title

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.

Electronic Patent Application Fee Transmittal

Application Number:	13484199
Filing Date:	30 May 2012
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Filer:	John C. Stringham/Ralene Eller
Attorney Docket Number:	18756.8.1.1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
PROCESSING FEE CORRECTING INVENTORSHIP	1816	1	150	150

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	150

Electronic Acknowledgement Receipt	
EFS ID:	38645809
Application Number:	13484199
International Application Number:	
Confirmation Number:	5095
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Customer Number:	22913
Filer:	John C. Stringham/Ralene Eller
Filer Authorized By:	John C. Stringham
Attorney Docket Number:	18756.8.1.1
Receipt Date:	20-FEB-2020
Filing Date:	30 MAY 2012
Time Stamp:	15:59:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$150
RAM confirmation Number	E20202JG01039273
Deposit Account	233178
Authorized User	Ralene Eller
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.20 (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	Request under Rule 48 correcting inventorship	18756-8-1-1_2020-02-20_Request to Correct Inventorship.pdf	122391 05b56a7c6170962 5cc1c158a4a73623f6c6 5afe	no	2
Warnings:					
Information:					
2	Consent of Assignee accompanying the declaration	18756-8-1-1_2020-02-20_Written Consent Assignee.pdf	104940 df1938 1a2e4e1e1d8b5506d1f459d0c8aee c9b1	no	2
Warnings:					
Information:					
3	Request under Rule 48 correcting inventorship	18756-8-1-1_2020-02-20_Liberty Stmt.pdf	84450 b5212cc1c1c1945f7079 4fc2 2a5cc1ebc8f 2ac0	no	1
Warnings:					
Information:					
4	Request under Rule 48 correcting inventorship	18756-8-1-1_2020-02-20_Felipe Stmt.pdf	82119 7a714df1e594c6015 2e1 1f829 0ae0a5694 076d	no	1
Warnings:					
Information:					
5	Power of Attorney	18756 8 1 1 2020 02 20 POA.pdf	140673 04174 1a1 a0 4 e8 95c185 d1 8fd3 d6 d85 06 5dd	no	1
Warnings:					
Information:					
6	Assignee showing of ownership per 37 CFR 3.73	18756 8 1 1 2020 02 20 373b Stmt.pdf	109082 8cfc41a1c3e002607dd5c0c6ca6c339b7a9 5a72a	no	1
Warnings:					
Information:					

1	Fee Worksheet (SB06)	fee-info.pdf	30267 [illegible]	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	673922		

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 NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/484,199	09/17/2013	8538845	18756.8.1.1	5095

22913 7590 08/28/2013

Workman Nydegger
60 East South Temple
Suite 1000
Salt Lake City, UT 84111

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Michael A. Liberty, Windermere, FL;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	111	20130018793	17-Jan-2013	Wong	
	112	20130018742	17-Jan-2013	Fisher	
	113	20130018740	17-Jan-2013	Fisher	
	114	20130018738	17-Jan-2013	Faires	
	115	20130017784	17-Jan-2013	Fisher	
	116	20130013501	10-Jan-2013	Rackley	
Change(s) applied to document, /N.W.S./ 8/1/2013	117	20130013499	~~10-Oct-2013~~	Kalgi	January 10, 2013
	118	20130013498	10-Jan-2013	Fisher	
	119	20130013490	10-Jan-2013	Keller	
	120	20130013434	10-Jan-2013	Fisher	
	121	20130013432	10-Jan-2013	Fisher	
	122	20130013355	10-Jan-2013	Fisher	
	123	20130013353	10-Jan-2013	Fisher	
	124	20130013352	10-Jan-2013	Fisher	
	125	20130012131	10-Jan-2013	Fisher	
	126	20130012126	10-Jan-2013	Fisher	
	127	20130012125	10-Jan-2013	Fisher	
	128	20120330792	27-Dec-2012	Kashanian	
	129	20120330737	27-Dec-2012	Liberty	
	130	20120329394	27-Dec-2012	Fisher	
	131	20120323777	20-Dec-2012	Liberty	
	132	20120323670	20-Dec-2012	Fisher	
	133	20120323664	20-Dec-2012	Klems	
	134	20120323653	20-Dec-2012	Fisher	
	135	20120317019	13-Dec-2012	Carnes	
	136	20120316992	13-Dec-2012	Oborne	
	137	20120316951	13-Dec-2012	Fisher	
	138	20120316950	13-Dec-2012	LaPorte	
	139	20120310826	6-Dec-2012	Chatterjee	
	140	20120310824	6-Dec-2012	Liberty	

~~ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./~~

Receipt date: 06/05/2013

13484199 - GAU: 3691

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	81	20130041700	14-Feb-2013	Fisher	
	82	20130041699	14-Feb-2013	Fisher	
	83	20130040569	14-Feb-2013	Fisher	
	84	20130040568	14-Feb-2013	Fisher	
	85	20130035970	7-Feb-2013	Fisher	
	86	20130035969	7-Feb-2013	Fisher	
	87	20130035968	7-Feb-2013	Fisher	
	88	20130035967	7-Feb-2013	Fisher	
	89	20130035087	7-Feb-2013	Fisher	
	90	20130035072	7-Feb-2013	Fisher	
	91	20130035071	7-Feb-2013	Fisher	
	92	20130035070	7-Feb-2013	Fisher	
	93	20130035069	7-Feb-2013	Fisher	
	94	20130035068	7-Feb-2013	Fisher	
	95	20130035037	7-Feb-2013	Fisher	
	96	20130035036	7-Feb-2013	Fisher	
	97	20130035035	7-Feb-2013	Fisher	
	98	20130030997	31-Jan-2013	Spodak	
	99	20130030960	31-Jan-2013	Kashanian	
	100	20130030828	31-Jan-2013	Pourfallah	
	101	20130029646	31-Jan-2013	Chowdhury	
	102	20130024372	1/214/13	Spodak	
	103	20130024371	24-Jan-2013	Hariramani	
	104	20130024364	24-Jan-2013	~~Fisher~~	Shrivastava et al.
	105	20130024280	24-Jan-2013	Fisher	
	106	20130024223	24-Jan-2013	Thomas	
	107	20130024221	24-Jan-2013	Fisher	
	108	20130024220	24-Jan-2013	Fisher	
	109	20130023294	24-Jan-2013	Singh	
	110	20130023290	24-Jan-2013	Fisher	

Change(s) applied to document.
/N.W.S./
8/1/2013

~~ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./~~

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (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)

22913 7590 06/07/2013
Workman Nydegger
60 East South Temple
Suite 1000
Salt Lake City, UT 84111

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO
13/481,199	05/30/2012	Michael A. Liberty	18756.8.1.1	5095

TITLE OF INVENTION: MONETARY TRANSACTION SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1780	$300	$0	$2080	09/09/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHANG, EDWARD	3691	705-035000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 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 Workman Nydegger
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 has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: MOZIDO, LLC
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Dallas, Texas

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☒ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 23-3178 (enclose an extra copy of this form).

PTOL-85 (Rev. 02/11)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 27 of 1360

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

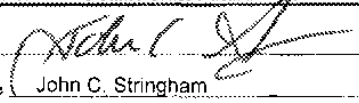
☒ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee 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: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature  Date August 16, 2013

Typed or printed name John C. Stringham Registration No. 40,831

This collection of information 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 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, 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.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 28 of 1360

Electronic Patent Application Fee Transmittal	
Application Number:	13484199
Filing Date:	30-May-2012
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Filer:	John C. Stringham/Sue Held
Attorney Docket Number:	18756.8.1.1
Filed as Small Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	890	890
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	1190

Electronic Acknowledgement Receipt	
EFS ID:	16610482
Application Number:	13484199
International Application Number:	
Confirmation Number:	5095
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Customer Number:	22913
Filer:	John C. Stringham/Sue Held
Filer Authorized By:	John C. Stringham
Attorney Docket Number:	18756.8.1.1
Receipt Date:	16-AUG-2013
Filing Date:	30-MAY-2012
Time Stamp:	13:18:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1190
RAM confirmation Number	10331
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Transmittal Letter	18756_8_1_1_Transmittal_For_Issue_Fee_Payment.pdf	110017	no	2
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	18756_8_1_1_Fees_Transmittal.pdf	162011	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31740	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	303768		

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.

Via E-File

PATENT APPLICATON
Docket No: 18756.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:		)
	Michael A. Liberty	)
Serial No:	13/484,199	) Art Unit
		) 3691
Filed:	May 30, 2012	)
Confirmation No.:	5095	)
For:	MONETARY TRANSACTION SYSTEM	)
Examiner:	Edward Chang	)
Customer No.:	22913	)

TRANSMITTAL OF ISSUE FEE PAYMENT

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Notice of Allowance and Fee(s) Due dated June 7, 2013, please find enclosed herewith the following items for filing in the United States Patent and Trademark Office in connection with the above identified patent application:

X Fee(s) Transmittal (PTOL-85) submitted pursuant to 37 C.F.R. § 1.311.

___ A Supplemental Declaration executed by the inventor(s) is submitted pursuant to 37 C.F.R. § 1.67.

___ Pursuant to the request for submission of formal drawings, enclosed are the following:

___ A Letter to the Official Draftsperson;

___ A set of _____ (__) sheets of formal drawings to replace the corresponding drawings originally filed with the subject application.

___ A duplicate set of the _____ (___) sheets of formal drawings with the changes therein highlighted in red.

___ Petition to Excuse Error in Small Entity Status is enclosed.

___ Form PTO-2038 submitting Credit Card Payment in the amount of $_____ is enclosed to cover the fee deficiency for the Petition to Excuse Error.

X Payment by credit card using the payment option in E-Filer with RAM will be used to cover the payment of the fees as follows:

X The $890.00 government issue fee pursuant to 37 C.F.R. § 1.18.

X The $300.00 government publication fee pursuant to 37 C.F.R. § 1.18.(d)

X The Commission is hereby authorized to charge payment of any additional fees or credit any overpayment to Deposit Account No. 23-3178.

Please address all future correspondence in connection with the above-identified patent application to the attention of the undersigned.

Dated this 16th day of August, 2013.

Respectfully submitted,

JOHN C. STRINGHAM
Registration No. 40,831
WORKMAN NYDEGGER
Attorneys for Applicant
Customer No. 022913
Telephone No. 801.533.9800

JCS/sch

4224135_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

U.S. PATENT APPLICATIONS

Examiner Initials*	Cite No.	Document Number	Filing Date	Name of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENTS

Examiner Initials*	Cite No.	Patent Number	Issue Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	8396793	12-Mar-2013	Hill	
	2	8374916	12-Feb-2013	White	
	3	8360329	29-Jan-2013	Grigg	
	4	8359265	22-Jan-2013	Van Rensburg	
	5	8355670	15-Jan-2013	White	
	6	8352323	1/8/2013	Fisher	
	7	8332272	12/11/2012	Fisher	
	8	8290433	16-Oct-2012	Fisher	
	9	8275312	25-Sep-2012	Fisher	
	10	8239325	7-Aug-2012	Schwarz	
	11	8213470	3-Jul-2012	Gu	
	12	8229354	24-Jul-2012	Sklovsky	
	13	8196131	5-Jun-2012	von Behren	
	14	8195576	5-Jun-2012	Grigg	
	15	8190087	29-May-2012	Fisher	
	16	8170485	1-May-2012	Hulvey	
	17	8160959	17-Apr-2012	Rackley	
	18	8145568	27-Mar-2012	Rackley	
	19	8121945	21-Feb-2012	Rackley	
	20	8116773	14-Feb-2012	Chitrapu	
	21	8116734	14-Feb-2012	Vawter	
	22	8095113	10-Jan-2012	Kean	
	23	8077042	13-Dec-2011	Peeters	
	24	8060012	15-Nov-2011	Sklovsky	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

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

Application Number	13/484199
Filing Date	05/30/2012
First Named Inventor	Liberty, Michael A.
Art Unit	3691
Confirmation Number	4095
Examiner Name	Chang, Edward
Attorney Docket Number	18756.8.1.1

25	8019365	13-Sep-2011	Fisher	
26	7979026	12-Jul-2011	Hulvey	
27	7967196	28-Jun-2011	Bierbaum	
28	7886962	15-Feb-2011	Vawter	
29	7865431	4-Jan-2011	Takayama	
30	7848504	7-Dec-2010	Lynam	
31	7848500	7-Dec-2010	Lynam	
32	7823772	2-Nov-2010	Vawter	
33	7822688	26-Oct-2010	Labrou	
34	7774076	10-Aug-2010	Skowronek	
35	7748618	6-Jul-2010	Vawter	
36	7708194	4-May-2010	Vawter	
37	7606560	20-Oct-2009	Labrou	
38	7562818	21-Jul-2009	Bierbaum	
39	7527194	5-May-2009	Truitt	
40	7512098	31-Mar-2009	Jiang	
41	7325132	29-Jan-2008	Takayama	
42	7322043	22-Jan-2008	Letsinger	
43	7255264	14-Aug-2007	De Leon	
44	7221939	22-May-2007	Ylitalo	
45	7054430	30-May-2006	Lynam	
46	6840448	11-Jan-2005	Fukushima	
47	6819219	16-Nov-2004	Bolle	
48	6697839	24-Feb-2004	Sini	
49	6622015	16-Sep-2003	Himmel	
50	6250557	26-Jun-2001	Forslund	
51	6736322	18-May-2004	Gobburu	
52	8333319	18-Dec-2012	Roth	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initials*	Cite No.	Publication Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	53	20070255620	1-Nov-2007	Tumminaro	
	54	20130080329	28-Mar-2013	Royyuru	
	55	20130080241	28-Mar-2013	Fisher	
	56	20130080240	28-Mar-2013	Fisher	
	57	20130080233	28-Mar-2013	Fisher	
	58	20130080232	28-Mar-2013	Fisher	
	59	20130080231	28-Mar-2013	Fisher	
	60	20130080230	28-Mar-2013	Fisher	
	61	20130080229	28-Mar-2013	Fisher	
	62	20130080228	28-Mar-2013	Fisher	
	63	20130073458	21-Mar-2013	Sherwin	
	64	20130073373	21-Mar-2013	Fisher	
	65	20130060618	7-Mar-2013	Barton	
	66	20130057392	7-Mar-2013	Bullock	
	67	20130054441	28-Feb-2013	Kamdar	
	68	20130054412	28-Feb-2013	Brendell	
	69	20130054337	28-Feb-2013	Brendell	
	70	20130054336	28-Feb-2013	Graylin	
	71	20130052952	28-Feb-2013	Fisher	
	72	20130048723	28-Feb-2013	King	
	73	20130046645	21-Feb-2013	Grigg	
	74	20130046634	21-Feb-2013	Grigg	
	75	20130046608	21-Feb-2013	Coppinger	
	76	20130041769	14-Feb-2013	Fisher	
	77	20130041745	14-Feb-2013	Coppinger	
	78	20130041744	14-Feb-2013	Coppinger	
	79	20130041743	14-Feb-2013	Coppinger	
	80	20130041736	14-Feb-2013	Coppinger	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

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

Application Number	13/484199
Filing Date	05/30/2012
First Named Inventor	Liberty, Michael A.
Art Unit	3691
Confirmation Number	4095
Examiner Name	Chang, Edward
Attorney Docket Number	18756.8.1.1

81	20130041700	14-Feb-2013	Fisher
82	20130041699	14-Feb-2013	Fisher
83	20130040569	14-Feb-2013	Fisher
84	20130040568	14-Feb-2013	Fisher
85	20130035970	7-Feb-2013	Fisher
86	20130035969	7-Feb-2013	Fisher
87	20130035968	7-Feb-2013	Fisher
88	20130035967	7-Feb-2013	Fisher
89	20130035087	7-Feb-2013	Fisher
90	20130035072	7-Feb-2013	Fisher
91	20130035071	7-Feb-2013	Fisher
92	20130035070	7-Feb-2013	Fisher
93	20130035069	7-Feb-2013	Fisher
94	20130035068	7-Feb-2013	Fisher
95	20130035037	7-Feb-2013	Fisher
96	20130035036	7-Feb-2013	Fisher
97	20130035035	7-Feb-2013	Fisher
98	20130030997	31-Jan-2013	Spodak
99	20130030960	31-Jan-2013	Kashanian
100	20130030828	31-Jan-2013	Pourfallah
101	20130029646	31-Jan-2013	Chowdhury
102	20130024372	1/214/13	Spodak
103	20130024371	24-Jan-2013	Hariramani
104	20130024364	24-Jan-2013	Fisher
105	20130024280	24-Jan-2013	Fisher
106	20130024223	24-Jan-2013	Thomas
107	20130024221	24-Jan-2013	Fisher
108	20130024220	24-Jan-2013	Fisher
109	20130023294	24-Jan-2013	Singh
110	20130023208	24-Jan-2013	Fisher

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

111	20130018793	17-Jan-2013	Wong	
112	20130018742	17-Jan-2013	Fisher	
113	20130018740	17-Jan-2013	Fisher	
114	20130018738	17-Jan-2013	Faires	
115	20130017784	17-Jan-2013	Fisher	
116	20130013501	10-Jan-2013	Rackley	
117	20130013499	10-Oct-2013	Kalgi	
118	20130013498	10-Jan-2013	Fisher	
119	20130013490	10-Jan-2013	Keller	
120	20130013434	10-Jan-2013	Fisher	
121	20130013432	10-Jan-2013	Fisher	
122	20130013355	10-Jan-2013	Fisher	
123	20130013353	10-Jan-2013	Fisher	
124	20130013352	10-Jan-2013	Fisher	
125	20130012131	10-Jan-2013	Fisher	
126	20130012126	10-Jan-2013	Fisher	
127	20130012125	10-Jan-2013	Fisher	
128	20120330792	27-Dec-2012	Kashanian	
129	20120330737	27-Dec-2012	Liberty	
130	20120329394	27-Dec-2012	Fisher	
131	20120323777	20-Dec-2012	Liberty	
132	20120323670	20-Dec-2012	Fisher	
133	20120323664	20-Dec-2012	Klems	
134	20120323653	20-Dec-2012	Fisher	
135	20120317019	13-Dec-2012	Carnes	
136	20120316992	13-Dec-2012	Oborne	
137	20120316951	13-Dec-2012	Fisher	
138	20120316950	13-Dec-2012	LaPorte	
139	20120310826	6-Dec-2012	Chatterjee	
140	20120310824	6-Dec-2012	Liberty	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

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

Application Number	13/484199
Filing Date	05/30/2012
First Named Inventor	Liberty, Michael A.
Art Unit	3691
Confirmation Number	4095
Examiner Name	Chang, Edward
Attorney Docket Number	18756.8.1.1

141	20120310760	6-Dec-2012	Phillips
142	20120310720	6-Dec-2012	Balsan
143	20120303425	29-Nov-2012	Katzin
144	20120302204	29-Nov-2012	Gupta
145	20120297204	22-Nov-2012	Buer
146	20120296741	22-Nov-2012	Dykes
147	20120296722	22-Nov-2012	Gosavi
148	20120296720	22-Nov-2012	Pirillo
149	20120296708	22-Nov-2012	Bachmann
150	20120293303	22-Nov-2012	Khan
151	20120290449	15-Nov-2012	Mullen
152	20120290376	15-Nov-2012	Dryer
153	20120286928	15-Nov-2012	Mullen
154	20120284131	8-Nov-2012	Soffer
155	20120271712	25-Oct-2012	Katzin
156	20120265685	18-Oct-2012	Brudnicki
157	20120265677	18-Oct-2012	Rackley
158	20120259732	11-Oct-2012	Sasankan
159	20120259698	11-Oct-2012	Yurrow
160	20120259686	11-Oct-2012	Yurrow
161	20120253852	4-Oct-2012	Pourfallah
162	20120232977	13-Sep-2012	Calman
163	20120232937	13-Sep-2012	Calman
164	20120231425	13-Sep-2012	Calman
165	20120231424	13-Sep-2012	Calman
166	20120229657	13-Sep-2012	Calman
167	20120229647	13-Sep-2012	Calman
168	20120226610	6-Sep-2012	Gill
169	20120221475	8/310/12	Grigg
170	20120221421	30-Aug-2012	Hammad

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

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

Application Number	13/484199
Filing Date	05/30/2012
First Named Inventor	Liberty, Michael A.
Art Unit	3691
Confirmation Number	4095
Examiner Name	Chang, Edward
Attorney Docket Number	18756.8.1.1

	171	20120215701	23-Aug-2012	Mehta	
	172	20120209749	16-Aug-2012	Hammad	
	173	20120209688	16-Aug-2012	Lamothe	
	174	20120203632	9-Aug-2012	Blum	
	175	20120197787	2-Aug-2012	Grigg	
	176	20120197745	2-Aug-2012	Fisher	
	177	20120197743	2-Aug-2012	Grigg	
	178	20120197740	2-Aug-2012	Grigg	
	179	20120197691	2-Aug-2012	Grigg	
	180	20120196586	2-Aug-2012	Grigg	
	181	20120191612	26-Jul-2012	Spodak	
	182	20120191557	26-Jul-2012	Fisher	
	183	20120174189	5-Jul-2012	Lim	
	184	20120172089	5-Jul-2012	Bae	
	185	20120172026	5-Jul-2012	Kwon	
	186	20120171992	5-Jul-2012	Cheong	
	187	20120158589	21-Jun-2012	Katzin	
	188	20120150669	14-Jun-2012	Langley	
	189	20120143752	7-Jun-2012	Wong	
	190	20120123937	17-May-2012	Spodak	
	191	20120123935	17-May-2012	Brudnicki	
	192	20120123880	17-May-2012	Craft	
	193	20120123868	17-May-2012	Brudnicki	
	194	20120123841	17-May-2012	Taveau	
	195	20120122447	17-May-2012	Craft	
	196	20120095855	19-Apr-2012	Sterling	
	197	20120084203	5-Apr-2012	Mehew	
	198	20120078735	29-Mar-2012	Bauer	
	199	20120074232	29-Mar-2012	Spodak	
	200	20120029990	2-Feb-2012	Fisher	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

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

Application Number	13/484199
Filing Date	05/30/2012
First Named Inventor	Liberty, Michael A.
Art Unit	3691
Confirmation Number	4095
Examiner Name	Chang, Edward
Attorney Docket Number	18756.8.1.1

	201	20120028612	2-Feb-2012	Hurst
	202	20120011063	12-Jan-2012	Killian
	203	20110320345	29-Dec-2011	Taveau
	204	20110320294	29-Dec-2011	Votaw
	205	20110320293	29-Dec-2011	Khan
	206	20110320243	29-Dec-2011	Khan
	207	20110302406	8-Dec-2011	Machani
	208	20110302016	8-Dec-2011	Haddad
	209	20110295750	1-Dec-2011	Rammal
	210	20110276417	10-Nov-2011	Campbell
	211	20110258115	20-Oct-2011	Mulhim
	212	20110251941	13-Oct-2011	Dunwoody
	213	20110250866	13-Oct-2011	Fisher
	214	20110246284	6-Oct-2011	Chaikin
	215	20110218911	8-Sep-2011	Spodak
	216	20110179113	21-Jul-2011	Thomas
	217	20110145049	16-Jun-2011	Hertel
	218	20110113473	12-May-2011	Corda
	219	20110105022	5-May-2011	Vawter
	220	20110087610	14-Apr-2011	Batada
	221	20110087529	14-Apr-2011	Angell
	222	20110057025	10-Mar-2011	Denzer
	223	20100260388	14-Oct-2010	Garrett
	224	20100250436	30-Sep-2010	Loevenguth
	225	20100248710	30-Sep-2010	Sklovsky
	226	20100235283	16-Sep-2010	Gerson
	227	20100223110	2-Sep-2010	Slavin
	228	20100125510	20-May-2010	Smith
	229	20100125495	20-May-2010	Smith
	230	20100088188	8-Apr-2010	Kumar

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	231	20100057624	4-Mar-2010	Hurt	
	232	20100057614	4-Mar-2010	Rainey	
	233	20100051685	4-Mar-2010	Royyuru	
	234	20100049599	25-Feb-2010	Owen	
	235	20100048226	25-Feb-2010	Owen	
	236	20100023449	28-Jan-2010	Skowronek	
	237	20100010964	14-Jan-2010	Skowronek	
	238	20090307132	10-Dec-2009	Phillips	
	239	20090288012	19-Nov-2009	Hertel	
	240	20090222358	3-Sep-2009	Bednarek	
	241	20090210308	20-Aug-2009	Toomer	
	242	20090156190	18-Jun-2009	Fisher	
	243	20090132392	21-May-2009	Davis	
	244	20090132362	21-May-2009	Fisher	
	245	20090104888	23-Apr-2009	Cox	
	246	20090098854	16-Apr-2009	Park	
	247	20090063312	5-Mar-2009	Hurst	
	248	20090055322	26-Feb-2009	Bykov	
	249	20090037326	5-Feb-2009	Chitti	
	250	20080281737	13-Nov-2008	Fajardo	
	251	20080255947	16-Oct-2008	Friedman	
	252	20080249933	9-Oct-2008	Rethorn	
	253	20080249930	9-Oct-2008	Hill	
	254	20080249927	9-Oct-2008	Rethorn	
	255	20080197190	21-Aug-2008	Fujita	
	256	20080143487	19-Jun-2008	Hulvey	
	257	20080126929	29-May-2008	Bykov	
	258	20080126145	29-May-2008	Rackley	
	259	20080052192	28-Feb-2008	Fisher	
	260	[illegible]	[illegible]	Rackley	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

261	20080010215	10-Jan-2008	Rackley	
262	20080010204	10-Jan-2008	Rackley	
263	20080010196	10-Jan-2008	Rackley	
264	20080010191	10-Jan-2008	Rackley	
265	20080006685	10-Jan-2008	Rackley	
266	20070241189	18-Oct-2007	Slavin	
267	20070162471	12-Jul-2007	Samuelsson	
268	20070123305	31-May-2007	Chen	
269	20060165060	27-Jul-2006	Dua	
270	20060116892	1-Jun-2006	Grimes	
271	20050222961	6-Oct-2005	Staib	
272	20040205618	14-Oct-2004	Sini	
273	20040181531	16-Sep-2004	Becker	
274	20030055735	20-Mar-2003	Cameron	
275	20020141586	3-Oct-2002	Margalit	
276	20020060246	23-May-2002	Gobburu	
277	20010037264	1-Nov-2001	Husemann	
278	20010011248	2-Aug-2001	Himmel	
279	20130024377	24-Jan-2013	Stong	
280	20130041701	14-Feb-2013	Roth	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.	Foreign Patent Document	Country Code	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T [1]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

NON PATENT LITERATURE DOCUMENTS			
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, page(s), volume-issue number(s), publisher, city and/or country where published	T [1]
	281	International Search Report for PCT/US2012/066013 dated January 29, 2013	☐
	282	Written Opinion for PCT/US2012/066013 dated January 29, 2013	☐

OFFICE ACTION / NOTICE OF ALLOWANCE DOCUMENTS				
Examiner Initials*	Cite No.	Application Number	Mail Date	Document

EXAMINER SIGNATURE			
Examiner Signature	/Edward Chang/	Date Considered	07/24/2013

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

[1]Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

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.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

☒ The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to Deposit Account No. 23-3178: (1) any filing fees required under 37 CFR § 1.16; and/or (2) any patent application and reexamination processing fees under 37 CFR § 1.17.

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		Date	6/5/2013
Name/Print	John C. Stringham	Registration Number	40831

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.

2113423_1.DOC

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

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

22913 7590 06/07/2013

Workman Nydegger
60 East South Temple
Suite 1000
Salt Lake City, UT 84111

EXAMINER	
CHANG, EDWARD	
ART UNIT	PAPER NUMBER
3691	

DATE MAILED: 06/07/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/484,199	05/30/2012	Michael A. Liberty	18756.8.1.1	5095

TITLE OF INVENTION: MONETARY TRANSACTION SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1780	$300	$0	$2080	09/09/2013

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 and an extra copy of the form should be submitted. 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: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 47 of 1360

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (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)

22913 7590 06/07/2013
Workman Nydegger
60 East South Temple
Suite 1000
Salt Lake City, UT 84111

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/484,199	05/30/2012	Michael A. Liberty	18756.8.1.1	5095

TITLE OF INVENTION: MONETARY TRANSACTION SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEES DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1780	$300	$0	$2080	09/09/2013

EXAMINER	ART UNIT	CLASS SUBCLASS
CHANG, EDWARD	3691	705-035000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 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, 1
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. 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. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number (enclose an extra copy of this form).

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 48 of 1360

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29	NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
❑ Applicant asserting small entity status. See 37 CFR 1.27	NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
❑ Applicant changing to regular undiscounted fee 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: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature	Date
Typed or printed name	Registration No.

This collection of information 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 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, 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.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 49 of 1360

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.
13/484,199	05/30/2012	Michael A. Liberty	18756.8.1.1	5095

22913 7590 06/07/2013

Workman Nydegger
60 East South Temple
Suite 1000
Salt Lake City, UT 84111

EXAMINER	
CHANG, EDWARD	
ART UNIT	PAPER NUMBER
3691	

DATE MAILED: 06/07/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 50 of 1360

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.

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	13/484,199	LIBERTY, MICHAEL A.	
	Examiner	Art Unit	
	EDWARD CHANG	3691	

All participants (applicant, applicant's representative, PTO personnel):

(1) *EDWARD CHANG*. (3)_____.

(2) *Gregory R. Lunt*. (4)_____.

Date of Interview: *30 May 2013*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *n/a*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant and examiner discussed necessary amendment to move the case to allowance. Examiner recommended some necessary change to claim 1 and applicant agreed. Examiner will enter the change by examiner's amendment and move the case to allowance.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Edward Chang/ Examiner, Art Unit 3691	

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 52 of 1360

Notice of Allowability	Application No. 13/484,199	Applicant(s) LIBERTY, MICHAEL A.	
	Examiner EDWARD CHANG	Art Unit 3691	AIA (First Inventor to File) 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 *April 26, 2013*.
   ☐ 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 *1-3,15 and 21-23*. 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: _____.

   Interim copies:

   a) ☐ All b) ☐ Some c) ☐ None of the: Interim copies of the priority documents have been 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 05/05/2013
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20130531* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/Edward Chang/
Examiner, Art Unit 3691

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 53 of 1360

DETAILED ACTION

Status of Claims

1. This action is in reply to the response filed on 26th of April 2013.

2. Claims 1 and 15 were amended.

3. Claims 4-14 and 16-20 were canceled.

4. Claims 21-23 were newly added.

5. Claims 1-3, 15, and 21-23 were allowable.

Information Disclosure Statement

6. The Information Disclosure Statement filed 05/05/2013 has been considered. Initialed copy of the Form 1449 is enclosed herewith.

EXAMINER'S AMENDMENT

7. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Gregory R. Lunt on May 30, 2013.

The Application has been amended as follows:

Claim 1:

A monetary transaction system for conducting monetary transactions between unbanked subscribers and other entities, the system comprising: a mobile device configured to run a monetary transaction system application; an unbanked monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the unbanked subscriber indicates, via the monetary transaction system application, one or more specified transactions

that are to be performed using the monetary transaction system;

a monetary transaction system processor that performs the one or more transactions specified by the unbanked subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile;

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system; and

wherein the monetary transaction system is implemented to deposit funds at an agent branch through a mobile wallet, including performing the following steps:

receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system, the agent communication indicating that the unbanked subscriber desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account;

validating the status of the unbanked subscriber's mobile wallet account; determining if the agent branch is authorized to receive deposited money; performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account, the limit check determining whether sufficient funds are available to make the deposit amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period;

crediting the unbanked subscriber's mobile wallet account with the specified amount of funds ***when the agent bank is authorized to receive the deposited money****;*

returning a notification to the agent branch confirming the deposit; and notifying the subscriber that the specified amount of funds was deposited in the unbanked subscriber's mobile wallet account over at least one of the plurality of channels connected to the monetary transaction system.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance: The instant application is directed towards conducting monetary transaction between unbanked subscribers and other entities. More specifically, the applicants' claims system comprising: *a mobile device configured to run a monetary transaction system application; an unbanked monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the unbanked subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system; a monetary transaction system processor that performs the one or more transactions specified by the unbanked subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile; at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system; and wherein the monetary transaction system is implemented to deposit funds at an agent branch through a mobile wallet, including performing the following steps: receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system, the agent communication indicating that the unbanked subscriber desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account; validating the status of the unbanked subscriber's mobile wallet account; determining if the agent branch is authorized to receive deposited money; performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account, the limit check determining whether sufficient funds are available to make the deposit amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period; crediting the unbanked subscriber's mobile wallet account with the specified amount of funds when the agent bank is authorized to receive the deposited money; returning a notification to the agent branch confirming the deposit; and notifying the subscriber that the specified amount of funds was deposited in the unbanked subscriber's mobile wallet account over at least one of the plurality of channels connected to the monetary transaction system.* Furthermore, Labrou [US 2005/0187873 A1] discloses mobile phone system of initializing, at a secure transaction

server (STS), a mobile payment software with a software authentication parameter, as an authentic mobile payment software. Valdes [US 2011/0145149 A1] discloses a method for detecting in real-time when a user of a prepaid telecommunications account tries to complete a data, voice or financial transaction to purchase a product or service but cannot, due to insufficient funds in in the Prepaid Account. Sykes's (NPL#1) discloses consolidation of the smartphone market in favor of devices running the BlakcBerry, Apple iOS, and Android operating systems has helped in providing a large user base for financial institutions that offer an HTML based mobile browser interface. Clarke's (NPL #2) discloses targeting marketing where mobile offers the opportunity to personalize messages to various segments, based upon time and location, by altering both sight and sound. Wei's (NPL #3) discloses the development of mobile commerce (m-commerce) environments that have user-friendly features is important to accelerate the adoption of m-commerce.

However, in the instant application none of prior arts of record either individually or in combination teach or suggest "*a mobile device configured to run a monetary transaction system application; an unbanked monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the unbanked subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system; a monetary transaction system processor that performs the one or more transactions specified by the unbanked subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile; at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system; and wherein the monetary transaction system is implemented to deposit funds at an agent branch through a mobile wallet, including performing the following steps: receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system, the agent communication indicating that the unbanked subscriber desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account; validating the status of the unbanked subscriber's mobile wallet account; determining if the agent branch is authorized to receive deposited money;*

performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account, the limit check determining whether sufficient funds are available to make the deposit amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period; crediting the unbanked subscriber's mobile wallet account with the specified amount of funds when the agent bank is authorized to receive the deposited money; returning a notification to the agent branch confirming the deposit; and notifying the subscriber that the specified amount of funds was deposited in the unbanked subscriber's mobile wallet account over at least one of the plurality of channels connected to the monetary transaction system."

For these reasons claims 1, 15, and 21 are deemed to be allowable over the prior art of record, and claims 2-3 and 22-23 are allowed by dependency on an allowed claim.

8. 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

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **Edward Chang** whose telephone number is **571.270.3092.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **ALEXANDER KALINOWSKI** can be reached at **571.272.6771**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair <http://pair-direct.uspto.gov >. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

P.O. Box 1450
Alexandria, VA 22313-1450

or faxed to **571-273-8300.**

Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window:**

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

May 31, 2013
/Edward Chang/ Examiner, Art Unit 3691

Notice of References Cited	Application/Control No. 13/484,199	Applicant(s)/Patent Under Reexamination LIBERTY, MICHAEL A.	
	Examiner EDWARD CHANG	Art Unit 3691	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0187873	08-2005	Labrou et al.	705/040
*	B	US-2011/0145149	06-2011	Valdes et al.	705/44
*	C	US-2008/0204358	08-2008	Sato et al.	345/2.2
*	D	US-7,819.307	10-2010	Lyons et al.	235/379
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Sykes, Quintin: Daley, Tim: "Securing Mobile Banking": Nov 2010. Credit Union Management; ISSN: 0273-9267.
	V	Clarke, Irvine III. "Emerging Value Propositions for M-commerce"; Fall 2008: Journal of Business Strategies. ISSN: 0887-2058.
	W	Wei. June; Ozok. Ant, "Development of a web-based mobile airline ticketing model with usability features": 2005: Industrial Management + Data Systems; v105n9; ISSN: 0263-5577.
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 60 of 1360

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

U.S. PATENT APPLICATIONS

Examiner Initials*	Cite No.	Document Number	Filing Date	Name of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	13/680824	19-Nov-2012	Liberty, Michael A.	

U.S. PATENTS

Examiner initials*	Cite No.	Patent Number	Issue Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	2	8041338	18-Oct-2011	Chen, Yuqun	
	3	7248855	24-Jul-2007	Joyce	
	4	7275685	2-Oct-2007	Gray	
	5	7822688	26-Oct-2010	Labrou	
	6	8160959	17-Apr-2012	Rackley	
	7	7699218	20-Apr-2010	Garcia	
	8	6714797	30-Mar-2004	Rautila	
	9	7461010	2-Dec-2008	Kwan	
	10	7107247	12-Sep-2006	Kinoshita	
	11	6185545	6-Feb-2001	Resnick	
	12	7100821	5-Sep-2006	Rasti	
	13	8016185	13-Sep-2011	Modi	
	14	7677973	16-Mar-2010	Van Luchene	
	15	6957342	18-Oct-2005	Vantanen	
	16	7774231	10-Aug-2010	Pond	
	17	5828739	27-Oct-1998	Nakanishi	
	18	7240836	10-Jul-2007	Vrotsos	
	19	6415156	2-Jul-2002	Stadelmann	
	20	7069001	27-Jun-2006	Rupp	
	21	7089208	8-Aug-2006	Levchin	
	22	7099850	29-Aug-2006	Mann	
	23	7347361	25-Mar-2008	Lovett	
	24	7494055	24-Feb-2009	Fernandes	
	25	7464028	2-Dec-2008	Wronski	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1 99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	26	7657489	2-Feb-2010	Stambaugh	
	27	7708194	4-May-2010	Vawter	
	28	7958052	7-Jun-2011	Powell	
	29	8095113	10-Jan-2012	Kean	
	30	7988060	2-Aug-2011	Killian	
	31	7865414	4-Jan-2011	Fung	
	32	7024174	4-Apr-2006	Nagy	
	33	7784684	31-Aug-2010	Labrou	
	34	7606560	20-Oct-2009	Labrou	
	35	8073783	6-Dec-2011	Felsted	
	36	5991749	23-Nov-1999	Morrill	
	37	8052042	8-Nov-2011	Kolinski-Schultz	
	38	5717374	10-Feb-1998	Smith	
	39	8090945	3-Jan-2012	Singhal	
	40	7877605	25-Jan-2011	Labrou	
	41	7801826	21-Sep-2010	Labrou	
	42	7822688	26-Oct-2010	Labrou	
	43	7353382	1-Apr-2008	Labrou	
	44	7349871	25-Mar-2008	Labrou	
	45	7363261	22-Apr-2008	Whitehead	
	46	7729963	1-Jun-2010	Lego	
	47	7937302	3-May-2011	Lego	
	48	7937305	3-May-2011	Lego	
	49	7729987	1-Jun-2010	Wakim	
	50	7890424	15-Feb-2011	Wakim	
	51	7110972	19-Sep-2006	Handa	
	52	6873974	29-Mar-2005	Schutzer	

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initials*	Cite No	Publication Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	53	20020052754	2-May-2002	Joyce	
	54	20060179452	10-Aug-2006	Amodeo	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	55	20070244811	18-Oct-2007	Tumminaro	
	56	20070255653	1-Nov-2007	Tumminaro	
	57	20120095856	19-Apr-2012	Sanjeev	
	58	20120245986	27-Sep-2012	Regan	
	59	20070106564	10-May-2007	Matotek	
	60	20090157546	18-Jun-2009	Garcia	
	61	20090177578	9-Jul-2009	Garcia	
	62	20090177581	9-Jul-2009	Garcia	
	63	20090254479	8-Oct-2009	Pharris	
	64	20090254440	8-Oct-2009	Pharris	
	65	20090281904	12-Nov-2009	Pharris	
	66	20120047070	23-Feb-2012	Pharris	
	67	20030071115	17-Apr-2003	Horn	
	68	20020069123	6-Jun-2002	Soderlind	
	69	20030154165	14-Aug-2003	Horn	
	70	20070179885	2-Aug-2007	Bird	
	71	20060287004	21-Dec-2006	Fuqua	
	72	20030001010	2-Jan-2003	Schmidt	
	73	20050199709	15-Sep-2005	Linior	
	74	20020152177	17-Oct-2002	Wolf	
	75	20040248554	9-Dec-2004	Khan	
	76	20080011825	17-Jan-2008	Giordano	
	77	20020161708	31-Oct-2002	Offer	
	78	20020131404	19-Sep-2002	Mehta	
	79	20050070265	31-Mar-2005	Korpinen	
	80	20070033285	8-Feb-2007	Shiigi	
	81	20070244811	18-Oct-2007	Tumminaro	
	82	20020042776	11-Apr-2002	Woo	
	83	20020065774	30-May-2002	Young	
	84	20030195842	16-Oct-2003	Reece	
	85	20050222961	6-Oct-2005	Stein	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	86	20060136901	22-Jun-2006	Nichols	
	87	20060200427	7-Sep-2006	Morrison	
	88	20070125838	7-Jun-2007	Law	
	89	20070125840	7-Jun-2007	Law	
	90	20070203850	30-Aug-2007	Singh	
	91	20080017704	24-Jan-2008	VanDeburg	
	92	20080040285	14-Feb-2008	Wankmueller	
	93	20080208743	28-Aug-2008	Arthur	
	94	20080208744	28-Aug-2008	Arthur	
	95	20080208762	28-Aug-2008	Arthur	
	96	20080210751	4-Sep-2008	Kim	
	97	20080249928	9-Oct-2008	Hill	
	98	20080255947	16-Oct-2008	Friedman	
	99	20080275779	6-Nov-2008	Lakshminarayanan	
	100	20090108015	30-Apr-2009	Kreamer	
	101	20090138366	28-May-2009	Bemmel	
	102	20090144161	4-Jun-2009	Fisher	
	103	20090248537	1-Oct-2009	Sarkeshik	
	104	20100044430	25-Feb-2010	Song	
	105	20100057619	4-Mar-2010	Weller	
	106	20100063895	11-Mar-2010	Dominguez	
	107	20090063312	5-Mar-2009	Hurst	
	108	20090222353	3-Sep-2009	Guest	
	109	20090106148	23-Apr-2009	Prada	
	110	20050080697	14-Apr-2005	Foss	
	111	20110313924	22-Dec-2011	Carrell	
	112	20100197326	5-Aug-2010	Ngo	
	113	20040235450	25-Nov-2004	Rosenberg	
	114	20070255620	1-Nov-2007	Tumminaro	
	115	20090119190	7-May-2009	Realini	
	116	20060253335	9-Nov-2006	Keena	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	117	20090265272	22-Oct-2009	Dill	
	118	20090081989	26-Mar-2009	Wuhrer	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.	Foreign Patent Document	Country Code	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[1]
	119	102073958	CN	25-May-2011	Tianjin ZTE Software Corp.		☐
	120	0171627	WO	27-Sep-2001	Qualcomm Incorporated		☐
	121	2003012717	WO	13-Feb-2003	C-SAM, Inc.		☐
	122	2004010393	WO	29-Jan-2004	Partner Communications Company Ltd.		☐
	123	2004023353	WO	18-Mar-2004	Tynevale Pty. Limited		
	124	2004088641	WO	14-Oct-2004	Way Systems, Inc.		
	125	2004053640	WO	24-Jun-2004	Way Systems, Inc.		
	126	9913636	WO	18-Mar-1999	Tekton Communications Limited		
	127	2002071354	WO	12-Sep-2002	Soft Tracks Enterprises Ltd.		
	128	2001-357164	JP	26-Dec-2001	NTT Data Corp.		
	129	2001097118	WO	20-Dec-2001	JOGU		
	130	199834203	WO	6-Aug-1998	Qualcomm Incorporated		
	131	2005079254	WO	1-Sep-2005	Fujitsu Limited		
	132	2005086593	WO	22-Sep-2005	A Little World Private Limited		
	133	2007145500	WO	21-Dec-2007	Mobile Money International SDN BHD		
	134	2008008735	WO	17-Jan-2008	Ibreva Corporation		
	135	101606400	CN	16-Dec-2009	Deloitte Services Pty. Ltd.		
	136	2666616	CA	24-Apr-2008	Fruitful Technologies Pty. Ltd.		
	137	1280115	EP	29-Jan-2003	NTT Docomo, Inc.		
	138	10-2007-0092400	KR	13-Sep-2007	Shin H. Bank		
	139	10-2003-0068603	KR	25-Aug-2003	Naru System Co.		
	140	10-2002-0065989	KR	14-Aug-2002	Starbridge Communications Co., Ltd.		
	141	[illegible]	[illegible]	12-Sep-2002	[illegible]		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	142	2002-99716	JP	5-Apr-2002	Kuninobu Masanao			
	143	2001-297198	JP	26-Oct-2001	Miwa Ginko KK (MIWAN)			

NON PATENT LITERATURE DOCUMENTS

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, page(s), volume-issue number(s), publisher, city and/or country where published	T[1]
	144	Chen, Jiajun Jim et al, Short-Range Wireless Technologies with Mobile Payments Systems. Proceedings of the 6th International Conference on Electronic Commerce [Online] 2004, pp. 649-656	☐
	145	Labrou, Yannis et al, Wireless Wallet. Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services [Online] 2004, pp.1-10	☐
	146	Motorola, Motorola M-Wallet Solution. [Online] 2006 http://www.motorola.com/networkoperators/pdfs/M-Wallet-Brochure.pdf (Accessed October 4, 2012)	☐
	147	Vaicourt, E. et al., "Investigating Mobile Payment," Wireless And Mobile Computing, Networking and Communications, 2005. (WiMob'2005). IEEE International Conference on 22-24 Aug. 2005. August 2005, Volume 4, pages 29-36.	
	148	Gao, Jerry, et al., "P2P-Paid: A Peer-to-Peer Wireless Payment System," Proceedings of the 2005 Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05) July 2005, 10 pages.	
	149	Edwin, et al., "Technobiography," October 2004, 29 pages.	
	150	International Search Report for PCT/US2012/066013 dated Jan. 29, 2013	
	151	Written Opinion for PCT/US2012/066013 dated Jan. 29, 2013	
	152	International Search Report for PCT/US2012/040131 Dated Jan. 29, 2013	
	153	Written Opinion for PCT/US2012/040131 dated Jan. 29, 2013	

OFFICE ACTION / NOTICE OF ALLOWANCE DOCUMENTS

Examiner Initials*	Cite No.	Application Number	Mail Date	Document

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

EXAMINER SIGNATURE

Examiner Signature	/Edward Chang/	Date Considered	05/31/2013

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

[1]Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1

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.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

☒ The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to Deposit Account No. 23-3178: (1) any filing fees required under 37 CFR § 1.16; and/or (2) any patent application and reexamination processing fees under 37 CFR § 1.17.

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	John C. Stringham	Date	5/3/12
Name/Print	John C. Stringham	Registration Number	40831

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.**

2113423_1.DOC

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.C./

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

BIB DATA SHEET

CONFIRMATION NO. 5095

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/484,199	05/30/2012 RULE	705	3691	18756.8.1.1

APPLICANTS
Michael A. Liberty, Windermere, FL;

**** CONTINUING DATA ***************************
This appln claims benefit of 61/522,099 08/10/2011
and claims benefit of 61/493,064 06/03/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
06/08/2012

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
❑ Yes ☑ No	❑ Yes ☑ No	/EDWARD CHANG/ Examiner's Signature	❑ Initials	FL	21	20	3

ADDRESS

Workman Nydegger
60 East South Temple
Suite 1000
Salt Lake City, UT 84111
UNITED STATES

TITLE

MONETARY TRANSACTION SYSTEM

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
1380	No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 69 of 1360

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13484199	LIBERTY, MICHAEL A.
	Examiner	Art Unit
	EDWARD CHANG	3691

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
705	40	6/1/2013	EC
705	35	6/1/2013	EC

SEARCH NOTES		
Search Notes	Date	Examiner
EAST - Keyword Search	6/1/2013	EC
Assignee Search	6/1/2013	EC
Backward/Forward Search of Main East Search	6/1/2013	EC
Inventor Search	6/1/2013	EC
Interference Search	6/1/2013	EC
Dialog - NPL search	6/1/2013	EC

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
705	40	6/1/2013	EC
705	35	6/1/2013	EC

/EDWARD CHANG/ Examiner.Art Unit 3691	

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 70 of 1360

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13484199	LIBERTY, MICHAEL A.
	Examiner	Art Unit
	EDWARD CHANG	3691

CPC		
Symbol	Type	Version

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
705	35	G	0	6	Q	40/00 (2012.01.01)					
CROSS REFERENCE(S)											
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)										
705	40										

/EDWARD CHANG/ Examiner.Art Unit 3691 (Assistant Examiner)	(Date)	Total Claims Allowed: 7	
/EDWARD CHANG/ Examiner.Art Unit 3691 (Primary Examiner)	06/01/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 71 of 1360

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13484199	LIBERTY, MICHAEL A.
	Examiner	Art Unit
	EDWARD CHANG	3691

/EDWARD CHANG/ Examiner.Art Unit 3691 (Assistant Examiner)	(Date)	Total Claims Allowed: 7	
/EDWARD CHANG/ Examiner.Art Unit 3691 (Primary Examiner)	06/01/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

U.S. Patent and Trademark Office

Part of Paper No. 20130531

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13484199	LIBERTY, MICHAEL A.
	Examiner	Art Unit
	EDWARD CHANG	3691

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		17												
2	2		18												
3	3		19												
	4		20												
	5	5	21												
	6	6	22												
	7	7	23												
	8														
	9														
	10														
	11														
	12														
	13														
	14														
4	15														
	16														

/EDWARD CHANG/ Examiner.Art Unit 3691 (Assistant Examiner)	(Date)	Total Claims Allowed: 7	
/EDWARD CHANG/ Examiner.Art Unit 3691 (Primary Examiner)	06/01/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 73 of 1360

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13484199	LIBERTY, MICHAEL A.
	Examiner	Art Unit
	EDWARD CHANG	3691

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/16/2012	06/01/2013							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
	4	✓	-							
	5	✓	-							
	6	✓	-							
	7	✓	-							
	8	✓	-							
	9	✓	-							
	10	✓	-							
	11	✓	-							
	12	✓	-							
	13	✓	-							
	14	✓	-							
4	15	✓	=							
	16	✓	-							
	17	✓	-							
	18	✓	-							
	19	✓	-							
	20	✓	-							
5	21		=							
6	22		=							
7	23		=							

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 74 of 1360

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	9891	(705/35).ccls.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/06/01 01:40
S1	100	("20120209762" "6142369" "6725303" "6976011" "20060265339" "20070063017" "20070106564" "20080270253" "20080314971" "20100030651" "7819307" "7822688" "20030004876" "20050187873" "20070095892" "20080162318" "20100088188" "20120197794" "20120259698" "20090055913" "20100274678" "20110137791" "20110145086" "20110145139" "20110145140" "20110145149" "20110313924" "20120226611" "20120290449" "6338140" "20100023417" "20040169073" "5315636" "5514862" "5848161" "5943624" "6038548" "6178335" "6185436" "6726092" "6913191" "7546944" "7784693" "20010007132" "20030078789" "20030121967" "20030177088" "20040243477" "20050164739" "20060173776" "20070123305" "20090106119" "20090233577" "20120036067" "20120108204" "20120172089" "20040039651" "20090097658" "5557518" "5621797" "5642419" "5815657" "5878139" "5963924" "6016484" "6019284" "6116506" "6230971" "4260055" "4992646" "5221838" "5671280" "5703949" "5745886" "5890052" "5940510" "5949880" "5949045" "6029151" "6068183" "6081790" "6088797" "6112984" "6175921" "6205436" "6315195" "6394343" "6425522" "6450407" "6502748" "6702181" "6905072" "6913193" "6970852" "7040533" "7140550" "7201313" "7207477" "7216800" "7344066").pn.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/12/14 13:15
S2	391	exceed with number with account	US-PGPUB; USPAT; USOCR	OR	OFF	2012/12/15 14:40
S3	4	exceed with number with account with allowable	US-PGPUB; USPAT; USOCR	OR	OFF	2012/12/15 14:40
S4	3699	(705/40).ccls.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/12/16 00:43

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 75 of 1360

L2	10170	(705/35).ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/06/01 01:40
L3	4020	(705/40).ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/06/01 01:40
L4	28	Perform$3 with limit with check with velocity with check	US-PGPUB; USPAT; UPAD	OR	OFF	2013/06/01 01:41
L5	3	Perform$3 with limit with check with velocity with check with unbanked	US-PGPUB; USPAT; UPAD	OR	OFF	2013/06/01 01:41
L6	3	Perform$3 with limit with check with velocity with check with unbanked with subscriber	US-PGPUB; USPAT; UPAD	OR	OFF	2013/06/01 01:42

6/1/2013 1:46:37 AM
C:\Users\echang1\Documents\EAST\Workspaces\Applicaiton -- 13484199 -- Monetary Transaction System.wsp

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 76 of 1360

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

U.S. PATENT APPLICATIONS

Examiner Initials*	Cite No.	Document Number	Filing Date	Name of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENTS

Examiner Initials*	Cite No.	Patent Number	Issue Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	8396793	12-Mar-2013	Hill	
	2	8374916	12-Feb-2013	White	
	3	8360329	29-Jan-2013	Grigg	
	4	8359265	22-Jan-2013	Van Rensburg	
	5	8355670	15-Jan-2013	White	
	6	8352323	1/8/2013	Fisher	
	7	8332272	12/11/2012	Fisher	
	8	8290433	16-Oct-2012	Fisher	
	9	8275312	25-Sep-2012	Fisher	
	10	8239325	7-Aug-2012	Schwarz	
	11	8213470	3-Jul-2012	Gu	
	12	8229354	24-Jul-2012	Sklovsky	
	13	8196131	5-Jun-2012	von Behren	
	14	8195576	5-Jun-2012	Grigg	
	15	8190087	29-May-2012	Fisher	
	16	8170485	1-May-2012	Hulvey	
	17	8160959	17-Apr-2012	Rackley	
	18	8145568	27-Mar-2012	Rackley	
	19	8121945	21-Feb-2012	Rackley	
	20	8116773	14-Feb-2012	Chitrapu	
	21	8116734	14-Feb-2012	Vawter	
	22	8095113	10-Jan-2012	Kean	
	23	8077042	13-Dec-2011	Peeters	
	24	8060012	15-Nov-2011	Sklovsky	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

25	8019365	13-Sep-2011	Fisher
26	7979026	12-Jul-2011	Hulvey
27	7967196	28-Jun-2011	Bierbaum
28	7886962	15-Feb-2011	Vawter
29	7865431	4-Jan-2011	Takayama
30	7848504	7-Dec-2010	Lynam
31	7848500	7-Dec-2010	Lynam
32	7823772	2-Nov-2010	Vawter
33	7822688	26-Oct-2010	Labrou
34	7774076	10-Aug-2010	Skowronek
35	7748618	6-Jul-2010	Vawter
36	7708194	4-May-2010	Vawter
37	7606560	20-Oct-2009	Labrou
38	7562818	21-Jul-2009	Bierbaum
39	7527194	5-May-2009	Truitt
40	7512098	31-Mar-2009	Jiang
41	7325132	29-Jan-2008	Takayama
42	7322043	22-Jan-2008	Letsinger
43	7255264	14-Aug-2007	De Leon
44	7221939	22-May-2007	Ylitalo
45	7054430	30-May-2006	Lynam
46	6840448	11-Jan-2005	Fukushima
47	6819219	16-Nov-2004	Bolle
48	6697839	24-Feb-2004	Sini
49	6622015	16-Sep-2003	Himmel
50	6250557	26-Jun-2001	Forslund
51	6736322	18-May-2004	Gobburu
52	8333319	18-Dec-2012	Roth

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initials*	Cite No.	Publication Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	53	20070255620	1-Nov-2007	Tumminaro	
	54	20130080329	28-Mar-2013	Royyuru	
	55	20130080241	28-Mar-2013	Fisher	
	56	20130080240	28-Mar-2013	Fisher	
	57	20130080233	28-Mar-2013	Fisher	
	58	20130080232	28-Mar-2013	Fisher	
	59	20130080231	28-Mar-2013	Fisher	
	60	20130080230	28-Mar-2013	Fisher	
	61	20130080229	28-Mar-2013	Fisher	
	62	20130080228	28-Mar-2013	Fisher	
	63	20130073458	21-Mar-2013	Sherwin	
	64	20130073373	21-Mar-2013	Fisher	
	65	20130060618	7-Mar-2013	Barton	
	66	20130057392	7-Mar-2013	Bullock	
	67	20130054441	28-Feb-2013	Kamdar	
	68	20130054412	28-Feb-2013	Brendell	
	69	20130054337	28-Feb-2013	Brendell	
	70	20130054336	28-Feb-2013	Graylin	
	71	20130052952	28-Feb-2013	Fisher	
	72	20130048723	28-Feb-2013	King	
	73	20130046645	21-Feb-2013	Grigg	
	74	20130046634	21-Feb-2013	Grigg	
	75	20130046608	21-Feb-2013	Coppinger	
	76	20130041769	14-Feb-2013	Fisher	
	77	20130041745	14-Feb-2013	Coppinger	
	78	20130041744	14-Feb-2013	Coppinger	
	79	20130041743	14-Feb-2013	Coppinger	
	80	20130041736	14-Feb-2013	Coppinger	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

81	20130041700	14-Feb-2013	Fisher
82	20130041699	14-Feb-2013	Fisher
83	20130040569	14-Feb-2013	Fisher
84	20130040568	14-Feb-2013	Fisher
85	20130035970	7-Feb-2013	Fisher
86	20130035969	7-Feb-2013	Fisher
87	20130035968	7-Feb-2013	Fisher
88	20130035967	7-Feb-2013	Fisher
89	20130035087	7-Feb-2013	Fisher
90	20130035072	7-Feb-2013	Fisher
91	20130035071	7-Feb-2013	Fisher
92	20130035070	7-Feb-2013	Fisher
93	20130035069	7-Feb-2013	Fisher
94	20130035068	7-Feb-2013	Fisher
95	20130035037	7-Feb-2013	Fisher
96	20130035036	7-Feb-2013	Fisher
97	20130035035	7-Feb-2013	Fisher
98	20130030997	31-Jan-2013	Spodak
99	20130030960	31-Jan-2013	Kashanian
100	20130030828	31-Jan-2013	Pourfallah
101	20130029646	31-Jan-2013	Chowdhury
102	20130024372	1/214/13	Spodak
103	20130024371	24-Jan-2013	Hariramani
104	20130024364	24-Jan-2013	Fisher
105	20130024280	24-Jan-2013	Fisher
106	20130024223	24-Jan-2013	Thomas
107	20130024221	24-Jan-2013	Fisher
108	20130024220	24-Jan-2013	Fisher
109	20130023294	24-Jan-2013	Singh
110	20130023209	24-Jan-2013	Fisher

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

111	20130018793	17-Jan-2013	Wong
112	20130018742	17-Jan-2013	Fisher
113	20130018740	17-Jan-2013	Fisher
114	20130018738	17-Jan-2013	Faires
115	20130017784	17-Jan-2013	Fisher
116	20130013501	10-Jan-2013	Rackley
117	20130013499	10-Oct-2013	Kalgi
118	20130013498	10-Jan-2013	Fisher
119	20130013490	10-Jan-2013	Keller
120	20130013434	10-Jan-2013	Fisher
121	20130013432	10-Jan-2013	Fisher
122	20130013355	10-Jan-2013	Fisher
123	20130013353	10-Jan-2013	Fisher
124	20130013352	10-Jan-2013	Fisher
125	20130012131	10-Jan-2013	Fisher
126	20130012126	10-Jan-2013	Fisher
127	20130012125	10-Jan-2013	Fisher
128	20120330792	27-Dec-2012	Kashanian
129	20120330737	27-Dec-2012	Liberty
130	20120329394	27-Dec-2012	Fisher
131	20120323777	20-Dec-2012	Liberty
132	20120323670	20-Dec-2012	Fisher
133	20120323664	20-Dec-2012	Klems
134	20120323653	20-Dec-2012	Fisher
135	20120317019	13-Dec-2012	Carnes
136	20120316992	13-Dec-2012	Oborne
137	20120316951	13-Dec-2012	Fisher
138	20120316950	13-Dec-2012	LaPorte
139	20120310826	6-Dec-2012	Chatterjee
140	20120310824	6-Dec-2012	Liberty

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

141	20120310760	6-Dec-2012	Phillips
142	20120310720	6-Dec-2012	Balsan
143	20120303425	29-Nov-2012	Katzin
144	20120302204	29-Nov-2012	Gupta
145	20120297204	22-Nov-2012	Buer
146	20120296741	22-Nov-2012	Dykes
147	20120296722	22-Nov-2012	Gosavi
148	20120296720	22-Nov-2012	Pirillo
149	20120296708	22-Nov-2012	Bachmann
150	20120293303	22-Nov-2012	Khan
151	20120290449	15-Nov-2012	Mullen
152	20120290376	15-Nov-2012	Dryer
153	20120286928	15-Nov-2012	Mullen
154	20120284131	8-Nov-2012	Soffer
155	20120271712	25-Oct-2012	Katzin
156	20120265685	18-Oct-2012	Brudnicki
157	20120265677	18-Oct-2012	Rackley
158	20120259732	11-Oct-2012	Sasankan
159	20120259698	11-Oct-2012	Yurrow
160	20120259686	11-Oct-2012	Yurrow
161	20120253852	4-Oct-2012	Pourfallah
162	20120232977	13-Sep-2012	Calman
163	20120232937	13-Sep-2012	Calman
164	20120231425	13-Sep-2012	Calman
165	20120231424	13-Sep-2012	Calman
166	20120229657	13-Sep-2012	Calman
167	20120229647	13-Sep-2012	Calman
168	20120226610	6-Sep-2012	Gill
169	20120221475	8/310/12	Grigg
170	20120221421	30-Aug-2012	Hammad

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	171	20120215701	23-Aug-2012	Mehta	
	172	20120209749	16-Aug-2012	Hammad	
	173	20120209688	16-Aug-2012	Lamothe	
	174	20120203632	9-Aug-2012	Blum	
	175	20120197787	2-Aug-2012	Grigg	
	176	20120197745	2-Aug-2012	Fisher	
	177	20120197743	2-Aug-2012	Grigg	
	178	20120197740	2-Aug-2012	Grigg	
	179	20120197691	2-Aug-2012	Grigg	
	180	20120196586	2-Aug-2012	Grigg	
	181	20120191612	26-Jul-2012	Spodak	
	182	20120191557	26-Jul-2012	Fisher	
	183	20120174189	5-Jul-2012	Lim	
	184	20120172089	5-Jul-2012	Bae	
	185	20120172026	5-Jul-2012	Kwon	
	186	20120171992	5-Jul-2012	Cheong	
	187	20120158589	21-Jun-2012	Katzin	
	188	20120150669	14-Jun-2012	Langley	
	189	20120143752	7-Jun-2012	Wong	
	190	20120123937	17-May-2012	Spodak	
	191	20120123935	17-May-2012	Brudnicki	
	192	20120123880	17-May-2012	Craft	
	193	20120123868	17-May-2012	Brudnicki	
	194	20120123841	17-May-2012	Taveau	
	195	20120122447	17-May-2012	Craft	
	196	20120095855	19-Apr-2012	Sterling	
	197	20120084203	5-Apr-2012	Mehew	
	198	20120078735	29-Mar-2012	Bauer	
	199	20120074232	29-Mar-2012	Spodak	
	200	20120029990	2-Feb-2012	Fisher	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	201	20120028612	2-Feb-2012	Hurst
	202	20120011063	12-Jan-2012	Killian
	203	20110320345	29-Dec-2011	Taveau
	204	20110320294	29-Dec-2011	Votaw
	205	20110320293	29-Dec-2011	Khan
	206	20110320243	29-Dec-2011	Khan
	207	20110302406	8-Dec-2011	Machani
	208	20110302016	8-Dec-2011	Haddad
	209	20110295750	1-Dec-2011	Rammal
	210	20110276417	10-Nov-2011	Campbell
	211	20110258115	20-Oct-2011	Mulhim
	212	20110251941	13-Oct-2011	Dunwoody
	213	20110250866	13-Oct-2011	Fisher
	214	20110246284	6-Oct-2011	Chaikin
	215	20110218911	8-Sep-2011	Spodak
	216	20110179113	21-Jul-2011	Thomas
	217	20110145049	16-Jun-2011	Hertel
	218	20110113473	12-May-2011	Corda
	219	20110105022	5-May-2011	Vawter
	220	20110087610	14-Apr-2011	Batada
	221	20110087529	14-Apr-2011	Angell
	222	20110057025	10-Mar-2011	Denzer
	223	20100260388	14-Oct-2010	Garrett
	224	20100250436	30-Sep-2010	Loevenguth
	225	20100248710	30-Sep-2010	Sklovsky
	226	20100235283	16-Sep-2010	Gerson
	227	20100223110	2-Sep-2010	Slavin
	228	20100125510	20-May-2010	Smith
	229	20100125495	20-May-2010	Smith
	230	20100088188	8-Apr-2010	Kumar

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	231	20100057624	4-Mar-2010	Hurt	
	232	20100057614	4-Mar-2010	Rainey	
	233	20100051685	4-Mar-2010	Royyuru	
	234	20100049599	25-Feb-2010	Owen	
	235	20100048226	25-Feb-2010	Owen	
	236	20100023449	28-Jan-2010	Skowronek	
	237	20100010964	14-Jan-2010	Skowronek	
	238	20090307132	10-Dec-2009	Phillips	
	239	20090288012	19-Nov-2009	Hertel	
	240	20090222358	3-Sep-2009	Bednarek	
	241	20090210308	20-Aug-2009	Toomer	
	242	20090156190	18-Jun-2009	Fisher	
	243	20090132392	21-May-2009	Davis	
	244	20090132362	21-May-2009	Fisher	
	245	20090104888	23-Apr-2009	Cox	
	246	20090098854	16-Apr-2009	Park	
	247	20090063312	5-Mar-2009	Hurst	
	248	20090055322	26-Feb-2009	Bykov	
	249	20090037326	5-Feb-2009	Chitti	
	250	20080281737	13-Nov-2008	Fajardo	
	251	20080255947	16-Oct-2008	Friedman	
	252	20080249933	9-Oct-2008	Rethorn	
	253	20080249930	9-Oct-2008	Hill	
	254	20080249927	9-Oct-2008	Rethorn	
	255	20080197190	21-Aug-2008	Fujita	
	256	20080143487	19-Jun-2008	Hulvey	
	257	20080126929	29-May-2008	Bykov	
	258	20080126145	29-May-2008	Rackley	
	259	20080052192	28-Feb-2008	Fisher	
	260	20080040265	14-Feb-2008	Rackley	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

261	20080010215	10-Jan-2008	Rackley	
262	20080010204	10-Jan-2008	Rackley	
263	20080010196	10-Jan-2008	Rackley	
264	20080010191	10-Jan-2008	Rackley	
265	20080006685	10-Jan-2008	Rackley	
266	20070241189	18-Oct-2007	Slavin	
267	20070162471	12-Jul-2007	Samuelsson	
268	20070123305	31-May-2007	Chen	
269	20060165060	27-Jul-2006	Dua	
270	20060116892	1-Jun-2006	Grimes	
271	20050222961	6-Oct-2005	Staib	
272	20040205618	14-Oct-2004	Sini	
273	20040181531	16-Sep-2004	Becker	
274	20030055735	20-Mar-2003	Cameron	
275	20020141586	3-Oct-2002	Margalit	
276	20020060246	23-May-2002	Gobburu	
277	20010037264	1-Nov-2001	Husemann	
278	20010011248	2-Aug-2001	Himmel	
279	20130024377	24-Jan-2013	Stong	
280	20130041701	14-Feb-2013	Roth	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.	Foreign Patent Document	Country Code	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T [1]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

NON PATENT LITERATURE DOCUMENTS			
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, page(s), volume-issue number(s), publisher, city and/or country where published	T [1]
	281	International Search Report for PCT/US2012/066013 dated January 29, 2013	☐
	282	Written Opinion for PCT/US2012/066013 dated January 29, 2013	☐

OFFICE ACTION / NOTICE OF ALLOWANCE DOCUMENTS				
Examiner Initials*	Cite No.	Application Number	Mail Date	Document

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

[1]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	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Confirmation Number	4095
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

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.

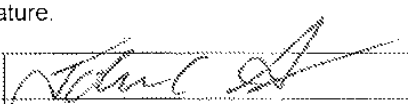
☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

☒ The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to Deposit Account No. 23-3178: (1) any filing fees required under 37 CFR § 1.16; and/or (2) any patent application and reexamination processing fees under 37 CFR § 1.17.

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		Date	6/5/2012
Name/Print	John C. Stringham	Registration Number	40831

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.

2113423_1.DOC

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN C. STRINGHAM
60 EAST SOUTH TEMPLE, SUITE 1000
SALT LAKE CITY, UT 84111

DOCKETED
Atty. JCS File # 18756.37.1a
By MS On 2/4/13
Action Article 19 Amendments
Response Due 3/29/13

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing *(day/month/year)*	29 JAN 2013
Applicant's or agent's file reference 18756.37.1A	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US 12/66013	International filing date *(day/month/year)* 20 November 2012 (20.11.2012)
Applicant MOZIDO, LLC	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 – 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer Lee W. Young PCT Helpdesk: 571-272-4300 Telephone No. PCT OSP: 571-272-7774

Form PCT/ISA/220 (July 2010)

Verified
By: [signature] On: 2/4/13

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 18756.37.1A	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US 12/66013	International filing date *(day/month/year)* 20 November 2012 (20.11.2012)	(Earliest) Priority Date *(day/month/year)* 21 November 2011 (21.11.2011)
Applicant MOZIDO, LLC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (see Box No. II).

3. ☐ **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 2

☐ as suggested by the applicant.

☒ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 90 of 1360

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 12/66013

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 20/00 (2013.01)
USPC - 705/78
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 20/00 (2013.01)
USPC -705/78

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 705/64; 705/39 (See Keywords Below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Patbase; Google Scholar
Search Terms: Mobile wallet, payment, third party, other provider, different provider, payment, transaction, purchase, deposit, withdraw, transfer, authorization code, point of sale, agent, operator, cloud, network, confirmation, notify, wallet provider, bill payment, ...

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008/0208762 A1 (ARTHUR et al.), 28 August 2008 (28.08.2008), entire document, especially Abstract; para [0016], [0057], [0065], [0068]-[0069], [0071]-[0074], [0080], [0082], [0119], [0140]	1-20
Y	US 6,873,974 B1 (SCHUTZER), 29 March 2005 (29.03.2005), entire document, especially Abstract; col 3, ln 40 to col 4, ln 20; col 8, ln 60 to col 9, ln 40	1-20
Y	US 2007/0125840 A1 (LAW et al.), 07 June 2007 (07.06.2007), entire document, especially Abstract; para [0033]-[0035], [0042], [0117]-[0120], [0150]-[0152]	9-11 and 15-17
A	US 2009/0234751 A1 (CHAN et al), 17 September 2009 (17.09.2009), entire document	1-20
A	US 2011/0196788 A1 (LU et al.), 11 August 2011 (11.08.2011), entire document	1-20

☐ 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
15 January 2013 (15.01.2013)	29 JAN 2013
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: JOHN C. STRINGHAM
60 EAST SOUTH TEMPLE, SUITE 1000
SALT LAKE CITY, UT 84111

DOCKETED
Atty JCS File # 18756.37.1a
By MS On 2/4/13
Action Written opinion
Response Due 4/29/13

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	29 JAN 2013
Applicant's or agent's file reference 18756.37.1A	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 12/66013	20 November 2012 (20.11.2012)	21 November 2011 (21.11.2011)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06Q 20/00 (2013.01)
USPC - 705/78

Applicant MOZIDO, LLC

1. This opinion contains indications relating to the following items:

- [X] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [X] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1 *bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	16 January 2013 (16.01.2013)	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

Verified
By: [signature] On: 2/4/13

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 12/66013

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 93 of 1360

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 12/66013

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-20	YES
	Claims	None	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-20	NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-8, 12-14 and 18-20 lack an inventive step under PCT Article 33(3) as being obvious over US 2008/0208762 A1 to Arthur et al. (hereinafter 'Arthur') in view of US 6,873,974 B1 (Schutzer).

Regarding claim 1, Arthur teaches a cloud-based transaction platform including (Abstract): one or more processors (para [0016], [0065]); system memory (para [0065]); one or more computer-readable storage media having stored thereon computer executable instructions that, when executed by the one or more processors, cause the computing system to perform a method for performing a transaction using a mobile wallet, the method comprising the following (Abstract; para [0016], [0057], [0140]): an act of receiving communication from an agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that a customer desires to perform a mobile wallet transaction using their mobile wallet (para [0068]-[0069], [0071]-[0074], [0080], [0082], [0119]); an act of sending the agent communication to a mobile wallet platform (para [0080]-[0082], [0120]-[0123]); an act of receiving communication from the mobile wallet platform confirming processing of the transaction (para [0087]-[0090], [0121]-[0125]); and an act of sending communication to the agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the communication indicating confirmation of the processing of the transaction (para [0087]-[0090], [0121]-[0125]). Arthur does not specifically teach the mobile wallet is a third party mobile wallet. However, Schutzer teaches a payment processing system, wherein the payment system accepts and process account transaction requests from third party mobile wallets (Abstract; col 3, ln 40 to col 4, ln 20; col 8, ln 60 to col 9, ln 40). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur with those of Schutzer since doing so would enhance the flexibility of mobile users by allowing payments using third party mobile wallets.

Regarding claim 2, Schutzer teaches a transaction is performed by a second, different customer using a second, different third party mobile wallet (col 7, ln 7-53; col 8, ln 60 to col 9, ln 40).

Regarding claim 3, Schutzer teaches the third party mobile wallet platform comprises a third party processor (col 9, ln 5-63).

Regarding claim 4, Schutzer teaches the transaction using a third party mobile wallet comprises one or more of a deposit, a withdrawal, a transfer, a purchase, a bill payment, or topping up of a prepaid mobile account (col 5, ln 57 to col 6, ln 10 - purchase).

Regarding claim 5, Arthur teaches comprising an act of notifying the customer of confirmation of the processing of the transaction using the mobile wallet over at least one of the plurality of communication channels connected to the cloud-based transaction platform (para [0121]-[0125]).

Regarding claim 6, Schutzer teaches the third party mobile wallet is provided by a third party mobile wallet provider (Abstract; col 3, ln 40 to col 4, ln 20; col 8, ln 60 to col 9, ln 40).

Regarding claim 7, Arthur teaches each mobile wallet provider has their own point of sale (POS) processing system (para [00068]-[0072], [0087]-[0090]).

Regarding claim 8, Arthur teaches the mobile wallet providers' POS processing systems communicate with each other using the cloud-based transaction platform to process the transaction (para [0068]-[0072], [0083]-[0087]).

Regarding claim 12, Arthur teaches the transaction comprises making a purchase from a mobile wallet managed by a mobile wallet platform, including: an act of receiving communication from the customer over one of the plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's mobile wallet (para [0080]-[0082], [0120]-[0123]); an act of returning a secure, perishable purchase code to the customer over at least one of the plurality of channels connected to the cloud-based transaction platform (para [0067]-[0070], [0073]-[0074]); an act of receiving communication from the agent terminal over at least one of the plurality of channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code has been presented to an agent (para [0067]-[0070], [0073]-[0074]); an act of debiting the customer's mobile wallet by the specified amount of funds (para [0087]-[0090], [0121]-[0125]).

--- (See Continuation in Supplemental Box) ---

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 94 of 1360

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2 Citations and Explanations.

Regarding claim 13, Arthur teaches a cloud-based transaction platform including: one or more processors (para [0016], [0065]); system memory (para [0065]); one or more computer-readable storage media having stored thereon computer- executable instructions that, when executed by the one or more processors, cause the computing system to perform a method for performing a transaction using a point of sale (POS) system, the method comprising (Abstract; para [0016], [0057], [0140]): an act of receiving communication from a specified POS system implemented at an agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the POS communication indicating that a customer has initiated a mobile wallet transaction using their mobile wallet (para [0068]-[0069], [0071]-[0074], [0080], [0082], [0119]); an act of sending the POS communication to a corresponding transaction processing system that has been established to process POS transactions from the specified POS system (para [0080]-[0082], [0120]-[0123]); an act of receiving communication from the POS transaction processing system confirming processing of the transaction (para [0087]-[0090], [0121]-[0125]); and an act of sending communication to the specified POS system implemented at the agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the communication indicating confirmation of the processing of the transaction (para [0087]-[0090], [0121]-[0125]). Arthur does not specifically teach the mobile wallet is a third party mobile wallet. However, Schutzer teaches a payment processing system, wherein the payment system accepts and process account transaction requests from third party mobile wallets (Abstract; col 3, ln 40 to col 4, ln 20; col 8, ln 60 to col 9, ln 40). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur with those of Schutzer since doing so would enhance the flexibility of mobile users by allowing payments using third party mobile wallets.

Regarding claim 14, Arthur teaches the act of receiving a transaction fee paid by the specified POS system to the cloud-based transaction platform (para [0063]-[0068], [0084]-[0087]).

Regarding claim 18, Arthur teaches the transaction comprises making a purchase from a mobile wallet provided by a mobile wallet provider, including: an act of receiving communication from the customer over one of the plurality of communication channels connected to the mobile wallet platform, the customer communication indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's mobile wallet (para [0080]-[0082], [0120]-[0123]); an act of returning a secure, perishable purchase code to the customer over at least one of the plurality of communication channels connected to the cloud based transaction platform and an act of receiving subsequent agent terminal communication over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code.has been presented to an agent (para [0067]-[0070], [0073]-[0074]); an act of validating the status of the specified payment method and an act of determining if the specified payment method can accommodate a purchase for the specified amount (para [0067]-[0070], [0073]-[0074]); an act of performing one or more of a limit check and a velocity check on the specified payment method and an act of debiting the customer's mobile wallet by the specified amount of funds by sending communication to the mobile wallet provider and an act of returning a notification to the POS system at the agent terminal authorizing the purchase (para [0087]-[0090], [0121]-[0125]); an act of sending a receipt to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform (para [0121]-[0125]).

Regarding claim 19, Arthur teaches a cloud-based transaction platform including: one or more processors (para [0016], [0065]); system memory (para [0065]); one or more computer-readable storage media having stored thereon computer-executable instructions that, when executed by the one or more processors, cause the computing system to perform a method for making a purchase from a mobile wallet provided by a mobile wallet provider, the method comprising the following (Abstract; para [0016], [0057], [0140]): an act of receiving communication from a customer over one of a plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's mobile wallet (para [0068]-[0069], [0071]-[0074], [0080], [0082], [0119]); an act of returning a secure, perishable purchase code to the customer over at least one the plurality of communication channels connected to the cloud-based transaction platform (para [0080]-[0082], [0120]-[0123]); an act of receiving communication from an agent terminal over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code has been presented to an agent (para [0087]-[0090], [0121]-[0125]); and an act of debiting the customer's mobile wallet by the specified amount of funds (para [0087]-[0090], [0121]-[0125]). Arthur does not specifically teach the mobile wallet is a third party mobile wallet. However, Schutzer teaches a payment processing system, wherein the payment system accepts and process account transaction requests from third party mobile wallets (Abstract; col 3, ln 40 to col 4, ln 20; col 8, ln 60 to col 9, ln 40). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur with those of Schutzer since doing so would enhance the flexibility of mobile users by allowing payments using third party mobile wallets.

Regarding claim 20, Schutzer teaches the item purchased by the customer comprises at least one of the following: health care services, music, games, and movies (col 6, ln 10-36 - purchase goods or services available on the web site).

--- (See Continuation in Supplemental Box) ---

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 95 of 1360

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2 Citations and Explanations.

Claims 9-11 and 15-17 lack an inventive step under PCT Article 33(3) as being obvious over Arthur in view of Schutzer and further in view of US 2007/0125840 A1 to Law et al. (hereinafter 'Law').

Regarding claim 9, neither Arthur nor Schutzer teaches the transaction comprises depositing funds into a mobile wallet owned by an entity different than the customer, including: an act of receiving communication from the agent terminal over one of the plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that the customer desires to deposit a specified amount of funds into their mobile wallet; and an act of crediting the mobile wallet with the specified amount of funds. However, Law teaches the transaction comprises depositing funds into a mobile wallet owned by an entity different than the customer, including: an act of receiving communication from the agent terminal over one of the plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that the customer desires to deposit a specified amount of funds into their mobile wallet (para [0033]-[0035], [0150]-[0152]); and an act of crediting the mobile wallet with the specified amount of funds (para [0042], [0150]-[0152]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe deposit of money to mobile wallet account.

Regarding claim 10, neither Arthur nor Schutzer teaches the transaction comprises withdrawing funds from a third party mobile wallet owned by an entity different than the customer, including: an act of receiving communication from the customer over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet; an act of returning a secure, perishable withdrawal code to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform; an act of receiving communication from the agent terminal over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the withdrawal code has been presented to an agent; and an act of debiting the third party mobile wallet by the specified amount of funds. However, Law teaches the transaction comprises withdrawing funds from a mobile wallet owned by an entity different than the customer, including: an act of receiving communication from the customer over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the mobile wallet (para [0149]-[0152]); an act of returning a secure, perishable withdrawal code to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform and an act of receiving communication from the agent terminal over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the withdrawal code has been presented to an agent (para [0040]-[0043], [0117]-[0120]) an act of debiting the mobile wallet by the specified amount of funds (para [0102]-[0103], [0150]-[0151]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe withdrawal of money to mobile wallet account.

Regarding claim 11, neither Arthur nor Schutzer teaches the transaction comprises transferring money from a third party mobile wallet within the cloud-based transaction platform to a recipient at a second third party mobile wallet provided by a second mobile wallet provider, the method comprising: an act of receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that a customer desires to transfer a specified amount of funds to a specified recipient using a specified payment method from the third party mobile wallet; an act of debiting the third party mobile wallet by the specified amount of funds; and an act of transferring the specified amount of funds from the cloud-based transaction platform to the second different third party mobile wallet platform for delivery to the specified recipient, the specified amount of funds being transferred over at least one of the plurality of channels connected to the second third party mobile wallet platform. However, Law teaches the transaction comprises transferring money from a mobile wallet within the cloud-based transaction platform to a recipient at a second mobile wallet provided by a second mobile wallet provider, the method comprising: an act of receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that a customer desires to transfer a specified amount of funds to a specified recipient using a specified payment method from the mobile wallet (para [0114]-[0118], [0140]-[0143]); an act of debiting the mobile wallet by the specified amount of funds and an act of transferring the specified amount of funds from the cloud-based transaction platform to the second different mobile wallet platform for delivery to the specified recipient, the specified amount of funds being transferred over at least one of the plurality of channels connected to the second mobile wallet platform (para [0114]-[0118], [0140]-[0143]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe transfer of money to mobile wallet account.

--- (See Continuation in Supplemental Box) ---

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 96 of 1360

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2 Citations and Explanations.

Regarding claim 15, neither Arthur nor Schutzer the transaction comprises depositing funds into a third party mobile wallet provided by a third party mobile wallet provider, including: an act of receiving communication from the specified POS system implemented at the agent terminal over one of the plurality of channels connected to the cloud-based transaction platform, the POS communication indicating that the customer desires to deposit a specified amount of funds into the third party mobile wallet provided by the third party mobile wallet provider; an act of validating the status of the third party mobile wallet provided by the third party mobile wallet provider; an act of determining if the specified POS system implemented at the agent terminal is authorized to deposit money; an act of performing one or more of a limit check and a velocity check on the third party mobile wallet provided by the third party mobile wallet provider; an act of crediting the third party mobile wallet provided by the third party mobile wallet provider with the specified amount of funds; an act of returning a notification to the specified POS system implemented at the agent terminal confirming the deposit; and an act of notifying the customer that the specified amount of funds were deposited in the third party mobile wallet provided by the third party mobile wallet provider over at least one of the plurality of communication channels connected to the cloud-based transaction platform. However, Law teaches the transaction comprises depositing funds into a mobile wallet provided by a mobile wallet provider, including: an act of receiving communication from the specified POS system implemented at the agent terminal over one of the plurality of channels connected to the cloud-based transaction platform, the POS communication indicating that the customer desires to deposit a specified amount of funds into the mobile wallet provided by the mobile wallet provider (para [0033]-[0035], [0150]-[0152]); an act of validating the status of the mobile wallet provided by the mobile wallet provider and an act of determining if the specified POS system implemented at the agent terminal is authorized to deposit money and an act of performing one or more of a limit check and a velocity check on the mobile wallet provided by the mobile wallet provider (para [0040]-[0043], [0118]-[0123]); an act of crediting the mobile wallet provided by the mobile wallet provider with the specified amount of funds (para [0042], [0150]-[0152]); an act of returning a notification to the specified POS system implemented at the agent terminal confirming the deposit and an act of notifying the customer that the specified amount of funds were deposited in the mobile wallet provided by the mobile wallet provider over at least one of the plurality of communication channels connected to the cloud-based transaction platform (para [0147]-[0151]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe deposit of money to mobile wallet account.

Regarding claim 16, neither Arthur nor Schutzer teaches the transaction comprises withdrawing funds from a third party mobile wallet provided by a third party mobile wallet provider, including: an act of receiving communication from a customer over one of the plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet provided by the third party mobile wallet provider; an act of validating the status of the third party mobile wallet provided by the third party mobile wallet provider; an act of determining if the balance of the third party mobile wallet provided by the third party mobile wallet provider is sufficient to accommodate the requested withdrawal for the specified amount of funds; an act of performing one or more of a limit check and a velocity check on the third party mobile wallet; an act of returning a secure, perishable withdrawal code to the customer over at least one of the plurality of channels connected to the cloud-based transaction platform; an act of receiving subsequent POS communication over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the POS communication indicating that the withdrawal code has been presented to an agent; an act of debiting the third party mobile wallet provided by the third party mobile wallet provider by the specified amount of funds; an act of returning a notification to the POS system at the agent terminal confirming the withdrawal; and an act of notifying the customer that the specified amount of funds were withdrawn from the third party mobile wallet over at least one of the plurality of communication channels connected to the cloud-based transaction platform. However, Law teaches the transaction comprises withdrawing funds from a mobile wallet provided by a mobile wallet provider, including: an act of receiving communication from a customer over one of the plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the mobile wallet provided by the mobile wallet provider (para [0149]-[0152]); an act of validating the status of the mobile wallet provided by the mobile wallet provider and an act of determining if the balance of the mobile wallet provided by the mobile wallet provider is sufficient to accommodate the requested withdrawal for the specified amount of funds and an act of performing one or more of a limit check and a velocity check on the mobile wallet and an act of returning a secure, perishable withdrawal code to the customer over at least one of the plurality of channels connected to the cloud-based transaction platform (para [0040]-[0043], [0118]-[0123]); an act of receiving subsequent POS communication over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the POS communication indicating that the withdrawal code has been presented to an agent (para [0040]-[0043], [0117]-[0120]); an act of debiting the mobile wallet provided by the mobile wallet provider by the specified amount of funds (para [0102]-[0103], [0150]-[0151]); an act of returning a notification to the POS system at the agent terminal confirming the withdrawal and an act of notifying the customer that the specified amount of funds were withdrawn from the mobile wallet over at least one of the plurality of communication channels connected to the cloud-based transaction platform (para [0147]-[0151]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe withdrawal of money to mobile wallet account.

--- (See Continuation in Supplemental Box) ---

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 97 of 1360

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of:
Box V.2 Citations and Explanations.

Regarding claim 17, neither Arthur nor Schutzer teaches the transaction comprises transferring money using a third party mobile wallet provided by a third party mobile wallet provider, including: an act of receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to transfer a specified amount of funds to a specified recipient having a third party mobile wallet, the transfer using a specified payment method from the customer's third party mobile wallet at the cloud-based transaction platform; an act of validating the status of the specified payment method; an act of performing one or more of a limit check and a velocity check on the specified payment method; an act of performing a check on the specified recipient having a third party mobile wallet to comply with the office of foreign assets control; an act of debiting the customer's mobile wallet at the cloud-based transaction platform by the specified amount of funds; an act of transferring the specified amount of funds to third party mobile wallet provider for delivery to the third party mobile wallet of the specified recipient over at least one of the plurality of channels connected between the cloud-based transaction platform and the third party mobile wallet provider; an act of notifying the customer that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the cloud-based transaction platform. However, Law teaches the transaction comprises transferring money using a mobile wallet provided by a mobile wallet provider, including: an act of receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to transfer a specified amount of funds to a specified recipient having a mobile wallet, the transfer using a specified payment method from the customer's mobile wallet at the cloud-based transaction platform (para [0114]-[0118], [0140]-[0143]); an act of validating the status of the specified payment method and an act of performing one or more of a limit check and a velocity check on the specified payment method and an act of performing a check on the specified recipient having a mobile wallet to comply with the office of foreign assets control; an act of debiting the customer's mobile wallet at the cloud-based transaction platform by the specified amount of funds (para [0040]-[0043], [0118]-[0123]); an act of transferring the specified amount of funds to mobile wallet provider for delivery to the mobile wallet of the specified recipient over at least one of the plurality of channels connected between the cloud-based transaction platform and the mobile wallet provider (para [0114]-[0118], [0140]-[0143]); an act of notifying the customer that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the cloud-based transaction platform (para [0147]-[0151]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe transfer of money to mobile wallet account.

Claims 1-20 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used in industry.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 98 of 1360

Electronic Patent Application Fee Transmittal	
Application Number:	13484199
Filing Date:	30-May-2012
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Filer:	John C. Stringham/Michelle Stringham
Attorney Docket Number:	18756.8.1.1
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt	
EFS ID:	15962346
Application Number:	13484199
International Application Number:	
Confirmation Number:	5095
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Customer Number:	22913
Filer:	John C. Stringham/Michelle Stringham
Filer Authorized By:	John C. Stringham
Attorney Docket Number:	18756.8.1.1
Receipt Date:	05-JUN-2013
Filing Date:	30-MAY-2012
Time Stamp:	20:30:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	7117
Deposit Account	233178
Authorized User	STRINGHAM, JOHN C.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 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	Information Disclosure Statement (IDS) Form (SB08)	IDSJune13.pdf	63702	no	12
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	37a_1ISR.pdf	177027	no	3
Warnings:					
Information:					
3	Non Patent Literature	37a_1WO.pdf	524933	no	7
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30103	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1369095		

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13/484199
Filing Date	05/30/2012
First Named Inventor	Liberty, Michael A
Art Unit	3691
Examiner Name	Chang, Edward
Attorney Docket Number	18756.8.1.1

U.S. PATENT APPLICATIONS

Examiner Initials*	Cite No.	Document Number	Filing Date	Name of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	13/680824	19-Nov-2012	Liberty, Michael A.	

U.S. PATENTS

Examiner Initials*	Cite No.	Patent Number	Issue Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	2	8041338	18-Oct-2011	Chen, Yuqun	
	3	7248855	24-Jul-2007	Joyce	
	4	7275685	2-Oct-2007	Gray	
	5	7822688	26-Oct-2010	Labrou	
	6	8160959	17-Apr-2012	Rackley	
	7	7699218	20-Apr-2010	Garcia	
	8	6714797	30-Mar-2004	Rautila	
	9	7461010	2-Dec-2008	Kwan	
	10	7107247	12-Sep-2006	Kinoshita	
	11	6185545	6-Feb-2001	Resnick	
	12	7100821	5-Sep-2006	Rasti	
	13	8016185	13-Sep-2011	Modi	
	14	7677973	16-Mar-2010	Van Luchene	
	15	6957342	18-Oct-2005	Vantanen	
	16	7774231	10-Aug-2010	Pond	
	17	5828739	27-Oct-1998	Nakanishi	
	18	7240836	10-Jul-2007	Vrotsos	
	19	6415156	2-Jul-2002	Stadelmann	
	20	7069001	27-Jun-2006	Rupp	
	21	7089208	8-Aug-2006	Levchin	
	22	7099850	29-Aug-2006	Mann	
	23	7347361	25-Mar-2008	Lovett	
	24	7494055	24-Feb-2009	Fernandes	
	25	7461028	2-Dec-2008	Wronski	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1 99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	26	7657489	2-Feb-2010	Stambaugh	
	27	7708194	4-May-2010	Vawter	
	28	7958052	7-Jun-2011	Powell	
	29	8095113	10-Jan-2012	Kean	
	30	7988060	2-Aug-2011	Killian	
	31	7865414	4-Jan-2011	Fung	
	32	7024174	4-Apr-2006	Nagy	
	33	7784684	31-Aug-2010	Labrou	
	34	7606560	20-Oct-2009	Labrou	
	35	8073783	6-Dec-2011	Felsted	
	36	5991749	23-Nov-1999	Morrill	
	37	8052042	8-Nov-2011	Kolinski-Schultz	
	38	5717374	10-Feb-1998	Smith	
	39	8090945	3-Jan-2012	Singhal	
	40	7877605	25-Jan-2011	Labrou	
	41	7801826	21-Sep-2010	Labrou	
	42	7822688	26-Oct-2010	Labrou	
	43	7353382	1-Apr-2008	Labrou	
	44	7349871	25-Mar-2008	Labrou	
	45	7363261	22-Apr-2008	Whitehead	
	46	7729963	1-Jun-2010	Lego	
	47	7937302	3-May-2011	Lego	
	48	7937305	3-May-2011	Lego	
	49	7729987	1-Jun-2010	Wakim	
	50	7890424	15-Feb-2011	Wakim	
	51	7110972	19-Sep-2006	Handa	
	52	6873974	29-Mar-2005	Schutzer	

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initials*	Cite No	Publication Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	53	20020052754	2-May-2002	Joyce	
	54	20060179452	10-Aug-2006	Amodeo	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	55	20070244811	18-Oct-2007	Tumminaro		
	56	20070255653	1-Nov-2007	Tumminaro		
	57	20120095856	19-Apr-2012	Sanjeev		
	58	20120245986	27-Sep-2012	Regan		
	59	20070106564	10-May-2007	Matotek		
	60	20090157546	18-Jun-2009	Garcia		
	61	20090177578	9-Jul-2009	Garcia		
	62	20090177581	9-Jul-2009	Garcia		
	63	20090254479	8-Oct-2009	Pharris		
	64	20090254440	8-Oct-2009	Pharris		
	65	20090281904	12-Nov-2009	Pharris		
	66	20120047070	23-Feb-2012	Pharris		
	67	20030071115	17-Apr-2003	Horn		
	68	20020069123	6-Jun-2002	Soderlind		
	69	20030154165	14-Aug-2003	Horn		
	70	20070179885	2-Aug-2007	Bird		
	71	20060287004	21-Dec-2006	Fuqua		
	72	20030001010	2-Jan-2003	Schmidt		
	73	20050199709	15-Sep-2005	Linior		
	74	20020152177	17-Oct-2002	Wolf		
	75	20040248554	9-Dec-2004	Khan		
	76	20080011825	17-Jan-2008	Giordano		
	77	20020161708	31-Oct-2002	Offer		
	78	20020131404	19-Sep-2002	Mehta		
	79	20050070265	31-Mar-2005	Korpinen		
	80	20070033285	8-Feb-2007	Shiigi		
	81	20070244811	18-Oct-2007	Tumminaro		
	82	20020042776	11-Apr-2002	Woo		
	83	20020065774	30-May-2002	Young		
	84	20030195842	16-Oct-2003	Reece		
	85	20050222961	6-Oct-2005	Staib		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	86	20060136901	22-Jun-2006	Nichols	
	87	20060200427	7-Sep-2006	Morrison	
	88	20070125838	7-Jun-2007	Law	
	89	20070125840	7-Jun-2007	Law	
	90	20070203850	30-Aug-2007	Singh	
	91	20080017704	24-Jan-2008	VanDeburg	
	92	20080040285	14-Feb-2008	Wankmueller	
	93	20080208743	28-Aug-2008	Arthur	
	94	20080208744	28-Aug-2008	Arthur	
	95	20080208762	28-Aug-2008	Arthur	
	96	20080210751	4-Sep-2008	Kim	
	97	20080249928	9-Oct-2008	Hill	
	98	20080255947	16-Oct-2008	Friedman	
	99	20080275779	6-Nov-2008	Lakshminarayanan	
	100	20090108015	30-Apr-2009	Kreamer	
	101	20090138366	28-May-2009	Bemmel	
	102	20090144161	4-Jun-2009	Fisher	
	103	20090248537	1-Oct-2009	Sarkeshik	
	104	20100044430	25-Feb-2010	Song	
	105	20100057619	4-Mar-2010	Weller	
	106	20100063895	11-Mar-2010	Dominguez	
	107	20090063312	5-Mar-2009	Hurst	
	108	20090222353	3-Sep-2009	Guest	
	109	20090106148	23-Apr-2009	Prada	
	110	20050080697	14-Apr-2005	Foss	
	111	20110313924	22-Dec-2011	Carrell	
	112	20100197326	5-Aug-2010	Ngo	
	113	20040235450	25-Nov-2004	Rosenberg	
	114	20070255620	1-Nov-2007	Tumminaro	
	115	20090119190	7-May-2009	Realini	
	116	20060253335	9-Nov-2006	Keena	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	117	20090265272	22-Oct-2009	Dill		
	118	20090081989	26-Mar-2009	Wuhrer		

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.	Foreign Patent Document	Country Code	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T [1]
	119	102073958	CN	25-May-2011	Tianjin ZTE Software Corp.		☐
	120	0171627	WO	27-Sep-2001	Qualcomm Incorporated		☐
	121	2003012717	WO	13-Feb-2003	C-SAM, Inc.		☐
	122	2004010393	WO	29-Jan-2004	Partner Communications Company Ltd.		☐
	123	2004023353	WO	18-Mar-2004	Tynevale Pty. Limited		
	124	2004088641	WO	14-Oct-2004	Way Systems, Inc.		
	125	2004053640	WO	24-Jun-2004	Way Systems, Inc.		
	126	9913636	WO	18-Mar-1999	Tekton Communications Limited		
	127	2002071354	WO	12-Sep-2002	Soft Tracks Enterprises Ltd.		
	128	2001-357164	JP	26-Dec-2001	NTT Data Corp.		
	129	2001097118	WO	20-Dec-2001	JOGU		
	130	199834203	WO	6-Aug-1998	Qualcomm Incorporated		
	131	2005079254	WO	1-Sep-2005	Fujitsu Limited		
	132	2005086593	WO	22-Sep-2005	A Little World Private Limited		
	133	2007145500	WO	21-Dec-2007	Mobile Money International SDN BHD		
	134	2008008735	WO	17-Jan-2008	Ibreva Corporation		
	135	101606400	CN	16-Dec-2009	Deloitte Services Pty. Ltd.		
	136	2666616	CA	24-Apr-2008	Fruitful Technologies Pty. Ltd.		
	137	1280115	EP	29-Jan-2003	NTT Docomo, Inc.		
	138	10-2007-0092400	KR	13-Sep-2007	Shin H. Bank		
	139	10-2003-0068603	KR	25-Aug-2003	Naru System Co.		
	140	10-2002-0065989	KR	14-Aug-2002	Starbridge Communications Co., Ltd.		
	141	10119808	DE	12-Sep-2002	Holland Chris		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1.1

	142	2002-99716	JP	5-Apr-2002	Kuninobu Masanao			
	143	2001-297198	JP	26-Oct-2001	Miwa Ginko KK (MIWAN)			

NON PATENT LITERATURE DOCUMENTS			
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, page(s), volume-issue number(s), publisher, city and/or country where published	T[1]
	144	Chen, Jiajun Jim et al, Short-Range Wireless Technologies with Mobile Payments Systems. Proceedings of the 6th International Conference on Electronic Commerce [Online] 2004, pp. 649-656	☐
	145	Labrou, Yannis et al, Wireless Wallet. Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services [Online] 2004, pp.1-10	☐
	146	Motorola, Motorola M-Wallet Solution. [Online] 2006 http://www.motorola.com/networkoperators/pdfs/M-Wallet-Brochure.pdf (Accessed October 4, 2012)	☐
	147	Vaicourt, E. et al., "Investigating Mobile Payment," Wireless And Mobile Computing, Networking and Communications, 2005. (WiMob'2005). IEEE International Conference on 22-24 Aug. 2005. August 2005, Volume 4, pages 29-36.	
	148	Gao, Jerry, et al., "P2P-Paid: A Peer-to-Peer Wireless Payment System," Proceedings of the 2005 Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05) July 2005, 10 pages.	
	149	Edwin, et al., "Technobiography," October 2004, 29 pages.	
	150	International Search Report for PCT/US2012/066013 dated Jan. 29, 2013	
	151	Written Opinion for PCT/US2012/066013 dated Jan. 29, 2013	
	152	International Search Report for PCT/US2012/040131 Dated Jan. 29, 2013	
	153	Written Opinion for PCT/US2012/040131 dated Jan. 29, 2013	

OFFICE ACTION / NOTICE OF ALLOWANCE DOCUMENTS				
Examiner Initials*	Cite No.	Application Number	Mail Date	Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A
	Art Unit	3691
	Examiner Name	Chung, Edward
	Attorney Docket Number	18756.8.1.1

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

[1]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	13/484199
	Filing Date	05/30/2012
	First Named Inventor	Liberty, Michael A.
	Art Unit	3691
	Examiner Name	Chang, Edward
	Attorney Docket Number	18756.8.1

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.

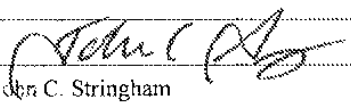
☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

☒ The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to Deposit Account No. 23-3178: (1) any filing fees required under 37 CFR § 1.16; and/or (2) any patent application and reexamination processing fees under 37 CFR § 1.17.

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		Date	5/3/12
Name/Print	John C. Stringham	Registration Number	40831

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.**

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 110 of 1360

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-108341**
(43)Date of publication of application : **11.04.2003**

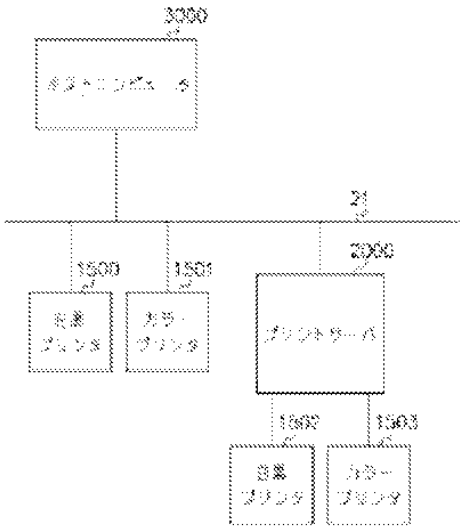
(51)Int.Cl. G06F 3/12
B41J 29/38
B41J 29/46

(21)Application number : **2001-297198**
(22)Date of filing : **27.09.2001**

(71)Applicant : **CANON INC**
(72)Inventor : **OYA SUSUMU**

(54) **APPARATUS, SYSTEM AND METHOD FOR INFORMATION PROCESSING, AND RECORDING MEDIUM AND PROGRAM**

(57)Abstract:
PROBLEM TO BE SOLVED: To achieve a high-speed output processing by performing distributed printing by using other image output device with a re-selection of other distributed printing when it is impossible to use an output device to be an output destination for the selected method for distributed printing.
SOLUTION: A host computer 3000 comprises a plurality of printer drivers to provide printing data to an applicable group of output devices and to perform distributed outputs of the printing data. When receiving a notification about disapproval of outputs of the printing data from output devices 1500 and 1501 forming the group of output devices to which the distributed outputs are instructed by one of the printer drivers, the host computer 3000 switches processing on distributed processing on the printing data to another printer driver to make another group of output devices (output devices 1502 and 1503) perform the distributed processing in the printing data.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－297198
（P2001－297198A）
(43)公開日　平成13年10月26日(2001.10.26)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　17/60	２５０	Ｇ０６Ｆ　17/60	２５０	３Ｅ０４０
	２３４		２３４Ｚ	５Ｂ０４９
	２３６		２３６Ａ	５Ｂ０５５
	２３８		２３８	５Ｋ０２７
	５０６		５０６	５Ｋ１０１

審査請求　有　　請求項の数８　ＯＬ　（全　６　頁）　最終頁に続く

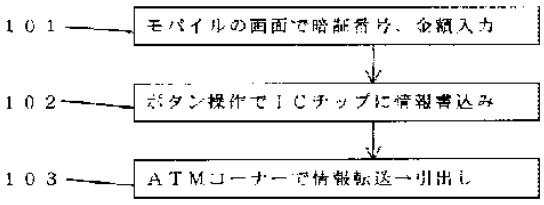
(21)出願番号　特願2000－113414(P2000－113414)
(22)出願日　平成12年４月14日(2000.4.14)

(71)出願人　599175026
株式会社三和銀行
大阪府大阪市中央区伏見町三丁目５番６号
(72)発明者　芦崎　武志
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内
(72)発明者　三砂　仁
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内
(74)代理人　100095267
弁理士　小島　高城郎　（外１名）

最終頁に続く

(54)【発明の名称】　携帯電話に組み込まれる金融処理システム

(57)【要約】
【課題】　携帯電話に種々の金融コンテンツを組込むことにより、携帯電話を利用してＡＴＭからの迅速な現金引出し、各種入出金処理の実行等を容易に行う。
【解決手段】　携帯電話に組み込まれる金融処理システムにおいて、携帯電話がＩＣチップを内蔵すると共に、ＩＣチップからＡＴＭへ非接触にてデータ転送するためのデータ転送手段を設け、暗証番号及びＡＴＭにおける金融処理情報を前記携帯電話に入力した後ＩＣチップに書込み、データ転送手段を介してＩＣチップからＡＴＭへ転送し、ＡＴＭは転送された入力情報に基づいて金融処理を実行する。



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 112 of 1360

【特許請求の範囲】
【請求項１】　ＡＴＭにおける金融処理を実行するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、
前記携帯電話がＩＣチップを内蔵すると共に、該ＩＣチップから前記ＡＴＭへ非接触にてデータ転送するためのデータ転送手段を設け、
前記入力手段を用いて銀行口座に係る暗証番号及び前記ＡＴＭにおける金融処理に係る情報を前記携帯電話に入力した後、該入力した情報を前記ＩＣチップに書込み、
前記データ転送手段を介して前記携帯電話の前記ＩＣチップから前記入力情報を前記ＡＴＭへ転送し、
前記ＡＴＭは転送された前記入力情報に基づいて前記銀行口座に係る前記金融処理を実行することを特徴とする携帯電話に組み込まれる金融処理システム。
【請求項２】　前記金融処理が、残高照会、引出し、入出金明細照会、振込み及び振替を含む群の中から選択されることを特徴とする請求項１に記載の携帯電話に組み込まれる金融処理システム。
【請求項３】　銀行口座の入出金状況を確認するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、
前記携帯電話により前記銀行口座の入出金状況に係る情報を格納したデータベースへ電話回線によりアクセスしデータを取得し、
前記取得したデータを前記表示手段に表示することを特徴とする携帯電話に組み込まれる金融処理システム。
【請求項４】　前記銀行口座の入出金状況に係る情報が、該銀行口座からの引落しに関する情報であって、引落日、引落内容及び引落金額を含むことを特徴とする請求項３に記載の携帯電話に組み込まれる金融処理システム。
【請求項５】　家計の収入支出状況を入力するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、
家計の収入支出状況に係る情報を前記入力手段により入力し、
前記家計の収入支出状況に係る情報を格納したデータベースへ電話回線によりアクセスすることにより前記入力されたデータを格納することを特徴とする携帯電話に組み込まれる金融処理システム。
【請求項６】　現在地及び最寄りのＡＴＭ設置場所に関する情報を取得するべく表示手段を具備する携帯電話に組み込まれるシステムにおいて、
電話回線により携帯基地局へアクセスし、携帯基地局がＧＰＳを実施することにより前記現在地及び前記最寄りのＡＴＭ設置場所に関する情報を取得し、
前記取得した情報を前記携帯電話へ返送し、
前記返送された情報を前記表示手段により表示することを特徴とする携帯電話に組み込まれるシステム。
【請求項７】　前記表示手段による表示に地図が含まれることを特徴とする請求項６に記載の携帯電話に組み込まれるシステム。
【請求項８】　請求項１乃至請求項７のいずれかに記載のシステムを組み込まれたことを特徴とする携帯電話
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、携帯電話に組み込まれるアプリケーションシステム、特に、金融処理機能及び金融処理に関連する機能を具備するアプリケーションシステムに関する。
【０００２】
【従来の技術】昨今、携帯電話の機能は目覚しく発展してきており、インターネットのウェブページの閲覧や電子メールの送受信等、様々な機能が提供されている。その中には、個人の銀行口座の入出金処理いわゆるテレフォンバンキング機能も含まれる。テレフォンバンキングでは、利用者が電話機のプッシュボタンにより暗証番号等を入力した後、入出金処理の種類（振込み、振替等）や金額の入力操作を行うことにより所望する処理が行われる。入力操作に当たっては、自動音声案内または携帯電話の表示画面に表示される指示に従ってプッシュボタンにより適宜の項目を選択する。
【０００３】
【発明が解決しようとする課題】このように、携帯電話における金融処理機能いわゆる金融コンテンツを提供するアプリケーションが種々提供されているが、未だ、口座からの現金の引出し及び口座からの出金による商品代金の決済並びに当該口座の入出金データの整理・保存による家計簿機能等の総合的な個人バンキング処理を実行するアプリケーションは提示されていない。
【０００４】一方、口座からの現金の引出しは、専らＡＴＭを利用して行われることが多いが、キャッシュカードをＡＴＭに挿入してから、暗証番号や引出し金額等の必要な情報をＡＴＭの入力装置に入力しなければならない。現状では、接触型のキャッシュカードが一般的に用いられており、カード挿入及びその後の入力操作に所定の時間が掛かるため、ＡＴＭの混雑時にはいっそうその混雑を増長させることとなる。
【０００５】以上の現状に鑑み、本発明は、携帯電話のアプリケーションとして個人バンキング処理を含めた総合的な機能を具備する金融コンテンツを組込むことにより、携帯電話を利用してＡＴＭからの迅速な現金引出し、各種入出金処理の実行、商品代金の決済、商品受渡し、入出金データの管理を容易に行うことを目的とする。
【０００６】
【課題を解決するための手段】上記の目的を達成するべく、本発明は以下の構成を提供する。
【０００７】（１）ＡＴＭにおける金融処理を実行する

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 113 of 1360

べく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、前記携帯電話がＩＣチップを内蔵すると共に、該ＩＣチップから前記ＡＴＭへ非接触にてデータ転送するためのデータ転送手段を設け、前記入力手段を用いて銀行口座に係る暗証番号及び前記ＡＴＭにおける金融処理に係る情報を前記携帯電話に入力した後、該入力した情報を前記ＩＣチップに書込み、前記データ転送手段を介して前記携帯電話の前記ＩＣチップから前記入力情報を前記ＡＴＭへ転送し、前記ＡＴＭは転送された前記入力情報に基づいて前記銀行口座に係る前記金融処理を実行する。

【０００８】（２）上記（１）の構成において、前記金融処理が、残高照会、引出し、入出金明細照会、振込み及び振替を含む群の中から選択される。

【０００９】（３）銀行口座の入出金状況を確認するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、前記携帯電話により前記銀行口座の入出金状況に係る情報を格納したデータベースへ電話回線によりアクセスしデータを取得し、前記取得したデータを前記表示手段に表示する。

【００１０】（４）上記（３）の構成において、前記銀行口座の入出金状況に係る情報が、該銀行口座からの引落しに関する情報であって、引落日、引落内容及び引落金額を含む。

【００１１】（５）家計の収入支出状況を入力するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、家計の収入支出状況に係る情報を前記入力手段により入力し、前記家計の収入支出状況に係る情報を格納したデータベースへ電話回線によりアクセスすることにより前記入力されたデータを格納する。

【００１２】（６）現在地及び最寄りのＡＴＭ設置場所に関する情報を取得するべく表示手段を具備する携帯電話に組み込まれるシステムにおいて、電話回線により携帯基地局へアクセスし、携帯基地局がＧＰＳを実施することにより前記現在地及び前記最寄りのＡＴＭ設置場所に関する情報を取得し、前記取得した情報を前記携帯電話へ返送し、前記返送された情報を前記表示手段により表示する。

【００１３】（７）上記（６）の構成において、前記表示手段による表示に地図が含まれる。

【００１４】（８）上記（１）乃至上記（７）のいずれかに記載のシステムを組み込まれた携帯電話である。

【００１５】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。本発明における携帯電話（図中では、「モバイル」と称する）は、ＩＣカードに内蔵されると同様のＩＣチップを内蔵し、非接触にてＩＣチップへデータを入出力するために手段を具備する。ＩＣチップは、磁気記録媒体と比べてセキュリティ性が高くかつ大量の情報を記憶できることで知られている。さらに、この携帯電話は、データを入力するためのプッシュボタンまたは類似の入力手段並びにデータを表示するためのディスプレイを具備する。

【００１６】一方、自動取引装置すなわちＡＴＭは、通常、タッチパネルまたはプッシュボタン等のデータの入力手段と表示手段を具備するが、本発明においては特に、非接触にて携帯電話のＩＣチップへデータを書込みまたデータを読取るための手段もまた具備する。

【００１７】斯かる携帯電話の所有者は、ＡＴＭを設置している銀行またはその銀行と提携する銀行に、口座を保有するものとする。当該口座に関連して、口座保有者のみが認知する暗証番号が設定されている。通常、口座保有者はキャッシュカードを所有しており、キャッシュカードをＡＴＭに適用することにより現金の引出しを行うことができる。

【００１８】図１は、本発明による携帯電話における金融処理システムの１つである現金引出し機能を利用する場合の操作フローを示す概略的な流れ図である。ステップ１０１において、口座保有者は、携帯電話の入力手段を用いて暗証番号を入力する。暗証番号は高度の機密事項であるので、入力の際に画面上には暗証番号は明示されず、代わりに「＊」等の記号により入力字数のみが表示される。暗証番号の入力後、口座保有者は、引出し金額を入力する。

【００１９】入力後、ステップ１０２において携帯電話上に設けられた所定のボタンを押すことにより、あるいは他の適宜の操作により、携帯電話に内蔵されたＩＣチップに入力された情報を書込む。

【００２０】ステップ１０１及び１０２は、ＡＴＭ設置場所へ赴く前に予め行っておくことが好ましい。本発明の利点の１つは、ＡＴＭ設置場所以外の任意の場所で、予め現金引出しのための必要な操作を行うことができることである。

【００２１】ステップ１０３において、口座保有者はＡＴＭに赴き、携帯電話のＩＣチップ内の情報をＡＴＭの読取り手段に読取らせることにより、ＩＣチップ内の情報を転送する。これは、非接触にて行われる。ＡＴＭからオンラインにてホストコンピュータへの照会が実行され、暗証番号により本人確認できたならば、ＡＴＭから入力情報で指定された金額の現金が出金される。

【００２２】図２は、携帯電話での現金引出し操作における携帯電話のディスプレイ上の表示例を示した図である。先ず、初期画面においては、携帯電話に組み込まれる金融コンテンツの一覧が示される。例えば、残高照会、引出し、入出金明細照会、振込み、振替、マネーカレンダーである、マネーカレンダーについては後述する。ここでは「２．引出し」を選択するとする。すると、次画面で、暗証番号と引出し金額の入力が促される。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 114 of 1360

【0023】図3は、図2の初期画面において「4．振込み」を選択する場合の表示例を示した図である。次画面において、本人確認のための暗証番号、振込み金額及び振込先を入力する。さらに、振込み操作においては、振込み相手に対するメッセージを添付することができる。メッセージを添付したい場合は、メッセージ内容及び相手のメールアドレスを入力する。これらの入力を終えたならば、入力情報をICチップに書込む。その後、ATMにおいて入力情報をATMに読取らせると、直ちに振込みが実行される。メッセージがある場合は、相手にメッセージが送られる。この振込み機能により、ショッピングが可能となる。例えば、商品販売する店舗の口座へ振込みを行うと共に、所望する商品内容をメッセージにて店舗に伝えることにより、商品代金の決済が完了し、後日商品が届けられることとなる。

【0024】図4は、図2の初期画面において「6．マネーカレンダー」を選択する場合の表示例を示した図である。「マネーカレンダー」においては、銀行口座の入出金状況の確認及び家計の収入支出に関する情報の入出力を行う。図4では、マネーカレンダーの項目として、引落日情報及び家計簿入力が挙げられている。「1．引落日情報」を選択した場合、電話回線を通して銀行のホストコンピュータの管理するデータベースへアクセスすることにより、近日中に口座引落しされる項目の情報を取得し、それが表示される。情報には、引落しの日付、内容及び金額が示されている。これにより口座保有者は、必要な口座残高を確保するよう注意することができる。

【0025】マネーカレンダーの「2．家計簿入力」を選択した場合は、家計簿へ記録すべき内容すなわち家計における収入支出状況を入力することができる。図5は、家計簿入力を選択した場合の表示例を示した図である。入力は、画面に表示された指示に沿って行えば容易に行える。先ず、利用金額を入力し、次に利用用途を複数の項目から選択することにより入力すると、確認画面が表示される。確認画面では、入力内容がまとめて示され、間違いなければ、「2．追加入力」を選択することにより、電話回線を通して銀行のホストコンピュータの管理するデータベースへアクセスし、入力データが送られ、データベースに入力データが格納される。家計簿情報は、入力を修正する場合は、「PDAで編集」を選択することにより編集する。尚、ショッピング内容を家計簿入力する場合、店舗のPOSと携帯電話が互いに通信し、店舗のPOSから入力データが転送されることにより、自動入力してもよい。

【0026】本発明に係る携帯電話は、好適にはJAVA言語を搭載しており、入力操作及びメモ・編集操作を効率的に行うことができる。

【0027】種々の金融コンテンツからなる金融処理システムを組み込んだ本発明の携帯電話は、近年、コンビニエンスストアに設置されるようになったATMや24時間営業ATMにおいて利用する場合に特に有用である。場所や時間を限定されること無く、いつでも容易にバンキング処理が可能となるからである。

【0028】従って、図6に示すATM設置場所情報提供機能を付加することにより、本発明に係る携帯電話は、さらに効果的に利用されることとなる。図6は、ATMの設置場所情報を提供する機能を具備する携帯電話のディスプレイ表示例を示す。ディスプレイ上には、現在地の周辺地図が表示されると共に、最も近い24時間営業の銀行ATM、及び、ATM設置コンビニエンスストアが表示されている。具体的な実施方法としては、携帯電話の基地局を活用してGPS（広域位置情報機能）サービスを実施する。携帯電話はJAVA言語を搭載しており、先ず、利用者が携帯電話を用いて基地局のホストへアクセスする。基地局のホストは、GPSを実施することにより携帯電話の現在位置情報を取得し、最寄りのキャッシュポイントすなわちATM設置場所の情報を地図及びテキストデータで携帯電話へ返送する。利用者はディスプレイに表示された地図を見て最寄りのATMを知ることができる。

【0029】

【発明の効果】本発明においては、携帯電話自体がICチップを搭載し、ICチップに書込んだ情報を非接触にてATMに読取らせることができる。従って、携帯電話をキャッシュカードの代わり用いてATM操作することができる。携帯電話のICチップには、予め必要な入力情報を書込んでおくことができるため、ATM設置場所においては、現金引出しや振込み等の処理を容易にかつ速やかに行うことができる。よってATMの混雑緩和に多大に寄与することとなる。

【0030】振込み機能にはメッセージ添付機能があり、オンラインショッピングの代金決済が可能であると同時に、商品の受渡しに関する情報をメッセージで伝えることができる。

【0031】また、携帯電話により、銀行口座の入出金及び家計の収入支出に関する情報の入力及び出力を行うことができるため、いつでも、どこでも簡単に日々のお金の利用状況を確認したり編集したりすることが可能となる。家計簿を継続的につけることは面倒であり長続きしないことが多いが、本発明のシステムを用いれば、クレジットカード等の引落日を確認しながら、無駄なく上手にお金を消費することができる。

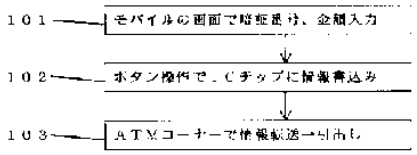
【0032】さらに、携帯電話を通して24時間営業のATMや、ATMを設置したコンビニエンスストアの位置情報を得られるため、携帯電話に組み込まれた金融コンテンツを利用できる場所へ利用者を用意に導くことができ、極めて利便性の高いしシステムが実現される。

【図面の簡単な説明】

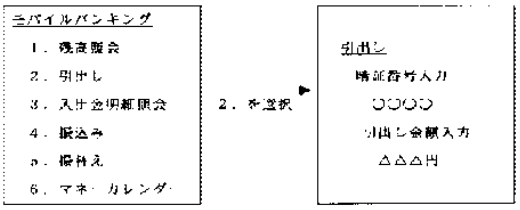
【図1】本発明による携帯電話における金融処理システ

ムの1つである現金引出し機能を利用する場合の操作フローを示す概略的な流れ図である。
【図2】携帯電話での現金引出し操作における携帯電話のディスプレイ上の表示例を示した図である。
【図3】図2の初期画面において「4．振込み」を選択する場合の表示例を示した図である。
【図4】図2の初期画面において「6．マネーカレンダー」を選択する場合の表示例を示した図である。
【図5】図4の次画面において「2．家計簿入力」を選択した場合の表示例を示した図である。
【図6】ATMの設置場所情報を提供する機能を具備する携帯電話のディスプレイ表示例を示す図である。
【符号の説明】
10 携帯電話
12 ディスプレイ

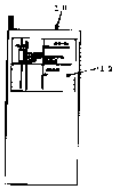
【図1】



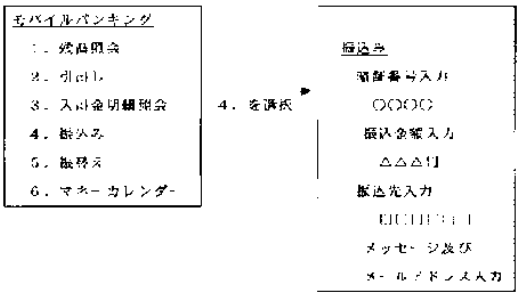
【図2】



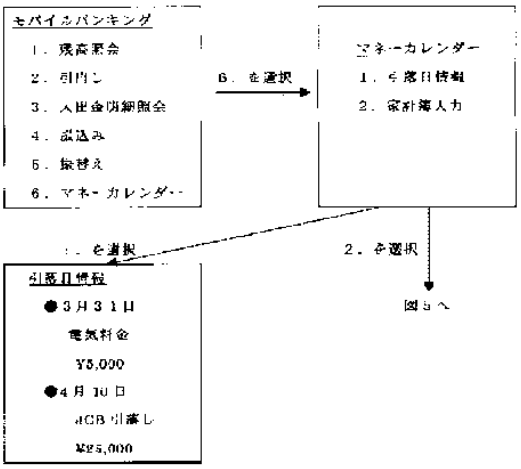
【図6】



【図3】

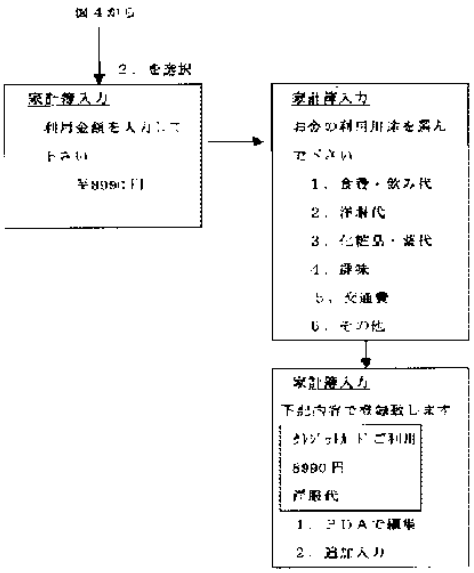


【図4】



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 116 of 1360

【図5】



フロントページの続き

(51)Int.Cl.⁷		識別記号
G07D	9/00	451
G07F	19/00	
H04M	1/00	
	1/725	
	11/00	303

F I		テーマコード（参考）
G07D	9/00	451C 9A001
H04M	1/00	R
	1/725	
	11/00	303
G07D	9/00	476

(72)発明者 中村 喜治
東京都千代田区大手町1丁目1番1号 株式会社三和銀行内
(72)発明者 山本 泰三
東京都千代田区大手町1丁目1番1号 株式会社三和銀行内
(72)発明者 森田 直樹
東京都千代田区大手町1丁目1番1号 株式会社三和銀行内

Fターム(参考) 3E040 BA07 BA18 CA14 EA01 EA02 FH05
5B049 AA02 BB46 CC36 GG06
5B055 BB03 CB01 CB08 CB09 PA05 PA11
5K027 AA11 FF01 FF22
5K101 KK11 KK15 LL12 NN01 NN18 9A001 JJ64 KK56 KK58

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 February 2003 (13.02.2003)

PCT

(10) International Publication Number
WO 03/012717 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US01/23899

(22) International Filing Date: 30 July 2001 (30.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: C-SAM, INC. [US/US]; Suite 2060, One Tower Lane, Oakbrook Terrace, IL 60181 (US).

(72) Inventor: PITRODA, Satyan, G.; Suite 2060, One Tower Lane, Oakbrook Terrace, IL 60181 (US).

(74) Agent: SHEKLETON, Gerald, T.; Welsh & Katz, Ltd., 120 S. Riverside Plaza, 22nd Floor, Chicago, IL 60606 (US).

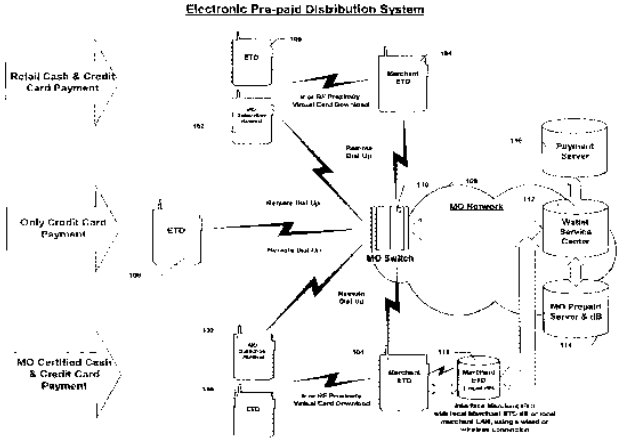
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM FOR DISTRIBUTION AND USE OF VIRTUAL STORED VALUE CARDS



(57) Abstract: A method of exchanging payment information in an electronic transaction includes a first electronic transaction device (106) transferring payment information to a second electronic transaction device (106), the second electronic transaction device (104) transferring value information to the first electronic transaction device (106), and the second electronic transaction device (104) transferring value information and payment information to a service consolidation centre (112). A method of tracking retail sales of pre paid telephone cards to cash subscribers is also provided. This method comprises entering value purchased information and subscriber information in a retailer electronic transaction device (104), the retailer electronic transaction device (104) transferring the value purchased information and subscriber information to a mobile operator (102), and the mobile operator (102) adding value corresponding to the value purchased information to an account corresponding to the subscriber information.

WO 03/012717 A1

SYSTEM FOR DISTRIBUTION AND USE OF VIRTUAL STORED VALUE CARDS

BACKGROUND OF THE INVENTION

This invention relates to a new and improved system for distribution and use of virtual stored value cards. One particular example where the invention may be used is in pre-paid virtual cards for mobile voice and data services.

Wireless or mobile phone operators typically have post-pay and pre-paid subscribers for their voice & data services. Post-pay subscribers pay for airtime they use at the end of a billing period, typically at a pre-determined rate, once a month. Pre-paid subscribers, in contrast pay for a pre-set amount of airtime, at a pre-determined rate, before they start using the airtime purchased. Pre-paid subscribers essentially create a stored-value account, from which they can use the minutes that they have purchased. The mobile operator's system keeps track of the minutes purchased and subsequently used by pre-paid subscribers and prompts them as their stored-value amounts near depletion. At this point pre-paid subscribers have the option to replenish their airtime. The operation of adding more minutes of airtime to an existing pre-paid account is typically referred to as the "top-up" or "top-off" operation.

Pre-paid services are one of the fastest growing segments of the mobile telephone operator business (mobile operators or MO). Pre-paid customers require no credit, no deposits, no contracts, no account fee, no age limit, but simply a periodic top up. Pre-paid customers do not need to demonstrate established credit or provide any details to mobile operators.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 119 of 1360

As the cost of mobile handsets and associated infrastructure has steadily decreased over time, many markets have seen an exponential increase in mobile users. As the current trend continues, the number of mobile installations may outgrow existing landlines. As the mobile handsets improve (hardware - processing power and memory, software, display – size and resolution, form factor, battery life, etc.) and the bandwidth offered by the mobile operator's increase, the new services offered by mobile operators will increase substantially. Because of decreasing costs of the handsets and the potential of value added services, mobile operators have been able to subsidize handset costs and offer pre-paid services to a large number of new customers to increase market share substantially. In some markets pre-paid customers account for as much as 70 to 80% of the total customer base. The pre-paid services have become popular for several reasons.

Pre-paid subscribers do not have to deal with long-term contracts – an element typical to a lot of calling plans offered by mobile operators to essentially allow them to subsidize the cost of the mobile handset. As the cost of handsets has continued to drop, and also as handset churn rates continue to climb, subscribers have the opportunity of purchasing second hand devices, further increasing the number of overall wireless subscribers. Owing to these factors, the mobile operators can now afford to offer pre-paid calling plans without any rigorous long-term contracts.

Since pre-paid calling plans do not require the subscriber to pay the charges at the end of the billing cycle, cash starved subscribers do not have to set aside any funds. This allows the subscriber to purchase service, without any elaborate budgeting.

Pre-paid subscribers do not have to deal with any unused airtime on fixed plans. For instance, typical plans will have a preset number of minutes of airtime for

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 120 of 1360

a certain value, which would expire at the end of the month. If these minutes are not used, they expire and the subscriber loses the value associated with the unused airtime.

Pre-paid subscribers do not require a credit account, or in many cases even a bank account, allowing them to purchase the service over the counter using cash, at various retail outlets and mobile operator certified distribution centers in the form of "scratch-off" plastic cards. This is ideal for the lower and middle income groups, students, and also for pre-dominantly cash economies, in emerging markets, where the pre-paid product has been very successful.

Mobile Operators ("MO") typically distribute their handsets (or alternately SIM cards) to pre-paid subscribers through controlled distribution channels – certified distribution outlets and/or participating retailers. The handsets come with some airtime preinstalled, as an incentive to the subscriber, and also allowing them to call the mobile operator to setup and "top-up" an account. The top-up operation to replenish airtime for pre-paid accounts may be accomplished in one of the following ways (Figure 1 and Figure 2):

The subscriber may top-up a pre-paid account by dialing into the MO's system, using their established payment account – credit, debit, etc. This may be done manually by speaking to a MO customer service representative, by using an automated voice activated response ("VAR") system, or through the Internet.

To manually top-up a pre-paid account, the subscriber calls an MO customer service representative, reads the pre-paid account number, and states the additional airtime required and the preferred payment method, which involves reading the credit card account number, expiry date, etc. This typically involves a dedicated session

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 121 of 1360

between the subscriber and the customer service representative, which is cumbersome, labor intensive and expensive.

In contrast, the automated VAR procedure involves dialing into the MO's system, selecting the number of minutes or airtime required, and entering or setting up a payment account, typically using the MO's automated voice activated response system.

One of the channels for top-up is through the Internet. Pre-paid subscribers may top-up their accounts by connecting to the mobile operator's pre-paid system through the Internet, entering a password to access their account and top-up using a credit account.

In addition, a subscriber may setup a new pre-paid account, or alternately top-up an existing account by going to a MO certified distribution center. These distribution centers may either be a retail environment, or possibly a certified bank that allows the subscribers to top-up their accounts using their ATM infrastructure or bank checks.

One of the more popular methods of top-up, especially for people who do not have a credit card or bank account or established credit and want to use just cash, requires purchasing a plastic card with a code for cash, which typically would be scratched off by the purchaser. These cards are distributed at the retail establishment – grocery stores, gas stations, etc. – in various denominations such as $10, $20, $50, $100, etc., where the subscriber would purchase a plastic card for the amount of required airtime. This plastic card is distributed in a tamper proof package, and is purchased from a retailer. The subscriber then scratches off the code, enters this code manually through the mobile handset into the MO's system, which in turn replenishes the amount of airtime purchased by the subscriber.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 122 of 1360

There are several disadvantages to present methods of topping-off pre-paid accounts. The mobile operators' cost for offering pre-paid airtime is as high as 20-30%. These costs are essentially incurred at various levels, for printing, packaging and distributing the cards, commissions for various intermediaries, depending on the distribution channel and process adopted. The manual system incurs additional labor costs, since it requires a dedicated customer service representative to walk the subscriber through the entire setup and top-up process. Add to this, the credit card issuer's fees for the transaction ("Card Holder Not Present" (CHNP) transactions), and the overall cost incurred by the mobile operator to support this distribution channel is very high.

The automated VAR channel may reduce a fraction of the cost by removing the labor component from the manual system. But this process has proven to be extremely cumbersome. Topping-up the account from the mobile device handset is awkward for the user, given the state of the handset's form factor, user interface, screen and keypad sizes. Thus, errors occur, especially during the setup operation, when the user must alternatively hold the handset near the ear to hear the VAR system and then hold it in front of the eyes to dial appropriate numbers. This eventually drives impatient subscribers to less cumbersome distribution channels, which in turn have a higher cost associated to the model for the mobile operator.

Certified MO distributors typically provide over-the-counter service for pre-paid subscribers, which incurs retail costs, in addition to the costs mention above. Because there are only a limited number of certified centers, the overall reach of such distribution centers is limited. Since many of these certified centers have a direct hook-up into the MO's back-end system, adding on such centers require more direct

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 123 of 1360

hook-ups, increasing the potential of fraud and adds to the accounting and inventory management costs.

Neutral distributors who support several mobile operators' products, typically charge a high margin for shelf space, increasing the distribution cost for the mobile operator.

One of the most popular channels of distribution for pre-paid products is through existing retail distribution channels - gas stations, grocery and department stores, etc. The reach of these channels, along with the ability to use cash, are the top most reasons for its popularity, but are also the most expensive for the mobile operator to support.

The mobile operator incurs some cost for producing the plastic cards, packaging and distributing them. In addition, the mobile operator incurs costs for tracking and managing physical inventory, ironically for a non-physical or virtual product such as airtime.

Retailers charge the mobile operators a very high margin for the distribution of these plastic cards, as they take up expensive shelf space. These margins form one of the integral components of the overall costs incurred by the mobile operator for the distribution of plastic pre-paid cards. Cash handling expenses, and credit card fees add to the overall cost, along with other cost elements typical to a retail environment.

Regarding transactions in general, the cost of a transaction, in the existing credit or debit environments supported by the widely accepted banking networks, typically ranges between 1.2 to 5.0% of the transaction, plus an additional 10 to 35 cents. The cost these transactions renders existing credit and debit transaction systems impractical for "sub to single digit dollar" transactions, typically referred to as micro-payments. Many transactions, especially proximity transactions for applications such

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 124 of 1360

as vending machines, toll, parking and transit, fall under this category which could be well supported by a stored cash value payment system.

The current stored value payment systems are inefficient, due to the lack of interoperability across payment worlds and end to end security. Consequently, the existing stored value payment systems have not been able to successfully cater to the eCommerce and mCommerce environments. In the brick and mortar retail environment, again the lack of a truly global interoperable and secure system has been responsible for less acceptance by merchants and consequently less penetration among users. The existing systems have also failed to provide an effective payment system for minors, who typically do not qualify for a credit or debit card, for credit challenged individuals and for person to person transactions.

Because existing credit and debit transaction systems are impractical for micropayments, cash is the predominant form of payment. Cash may be cumbersome, subject to theft or loss, and in some cases owing to the lack of local currency, impractical and extremely inconvenient. In terms of the merchants, owing to the high potential of fraud and theft, cash transactions are associated with a very high cost of handling and collection. Thus need exists for a suitable payment system to address the above outlined issues, and at the same time reduce cash transactions for the convenience of the users and merchants alike.

DESCRIPTION OF THE DRAWINGS

Figure 1 is a diagram of a prior-art pre-paid distribution system.

Figure 2 is a flow chart of a prior art pre-paid distribution system.

Figure 3 is a diagram depicting a preferred embodiments of the electronic pre-paid distribution system of the present invention.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 125 of 1360

Figure 4 is a diagram depicting a preferred embodiment of the Retail & MO Certified Cash & Credit Card Payment of the present invention.

Figure 5 is a diagram depicting a preferred embodiment of the Retail & MO Certified Cash & Credit Card Payment Through MO Network of the present invention.

Figure 6 is a diagram depicting a preferred embodiment of the Retail & MO Certified Cash & Credit Card Payment Through Proximity of the present invention.

Figure 7 is a diagram depicting a preferred embodiment of the Only Credit Card Payment of the present invention.

Figure 8 is a diagram depicting a preferred embodiment of the Only Credit Card Payment Setup Sequence Flow Chart of the present invention.

Figure 9 is a diagram depicting a preferred embodiment of the Only Credit Card Payment "Top-Off" Sequence Flow Chart of the present invention.

Figure 10 is a diagram depicting a preferred embodiment of the Only Credit Card Payment Sample User Interfaces is of the present invention.

Figure 11 is a diagram depicting a preferred embodiment of the Only Credit Card Payment Sample User Interfaces of the present invention.

Figure 12 is a diagram depicting a preferred embodiment of the Merchant Wallet Architecture of the present invention.

Figure 13 is a diagram depicting a preferred embodiment of the Merchant Wallet Sample User Interfaces is of the present invention.

Figure 14 is a diagram depicting a preferred embodiment of the Wallet Service Center Value Added Services of the present invention.

Figure 15 is a diagram of examples of virtual card generation and download.

Figure 16 is a diagram of a stored value application of the present invention.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 126 of 1360

Figure 17 is a diagram of a preferred embodiment of a stored value transaction system Through MO Network of the present invention.

Figure 18 is a flow chart of a preferred embodiment of a stored value transaction system Through MO Network of the present invention.

Figure 19 is a diagram of a stored value transaction system proximity model of the present invention.

Figure 20 is a flow chart of a preferred embodiment of a stored value transaction system of the present invention.

Figure 21 is a diagram of a multiple MO example of the present invention.

Figure 22 is a diagram of examples of user interfaces for a multiple MO environment of the present invention.

Figure 23 is a diagram of an Existing Transaction System and a Wireless Transaction System.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

For purposes of reference, Figures 1 and 2 are diagrams that generally depict various aspects of prior art distribution of pre-paid air time. Figure 1 shows existing channels of distribution for pre-paid airtime, the setup and top-up operations using a mobile handset and the mobile operator's manual or automated systems, using the mobile operator certified locations and the retail outlet model to procure plastic pre-paid "scratch-off cards."

Figure 2 is a flowchart depicting current distribution processes for a mobile handset with pre-paid airtime.

As shown in Figure 1, MO Network 20 includes MO Switch 22 and MO Pre-paid Server and Database 24. MO Certified Distribution Center 26 is coupled to the MO Pre-paid Server and Database 24. MO Subscriber Handset 28 is in electronic

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 127 of 1360

communication with MO Switch 22. Pre-paid Plastic Card Retail Distribution Centers 30 are not connected to the MO Network 20. MO Subscribers may connect to the MO Network 20 by way of a Computer 32 connected to the Internet 34.

Figure 3 illustrates examples of the pre-paid distribution systems of the present invention. A MO Subscriber Handset 102 may be topped up by way of an electronic transaction device (ETD) adapted to the functions of a Merchant (hereinafter Merchant ETD 104). Electronic transaction devices include, but are not limited to, devices such as the Universal Electronic Transaction Card as disclosed in U.S. Patent Nos. 5,590,038 and 5,884,271, which are incorporated by reference. To facilitate the transaction. the MO Subscriber may also have a MO Subscriber ETD 106 adapted to communicate with the Merchant ETD 104. The MO Subscriber ETD 106. It may be a separate device as illustrated, or it may be embedded in the MO Subscriber Handset 102. Alternatively, the subscriber may communicate with Merchant ETD 104 as illustrated in Figures 12, 13, and 14. The Merchant ETD 104 is in electronic communication with MO Network 108. MO network 108 includes MO Switch 110, Wallet Service Centers 112, MO Pre-paid Server 114, and Payment Server 116.

Figure 3 illustrates three examples of the invention. The first example, which is labeled "Retail Cash & Credit Card Payment," permits the MO, using a Merchant ETD 104, to distribute pre-paid airtime by taking cash or credit cards, debit cards, etc. from their customers. This typically relates to retail environment –grocery stores, gas stations, department stores, etc. - where a merchant using the Merchant ETD 104 may distribute pre-paid airtime using the MOs network or a proximity method.

The merchant enters relevant information into the Merchant ETD 104, such as value purchased information and subscriber information. Value purchased

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 128 of 1360

information includes, for example, the quantity of airtime purchased, the quantity of funds transferred, mode of payment (*i.e.*, cash, credit, or other form of payment), authorization information, or other like information. Subscriber information includes, for example, an identification of a person providing a payment (including cash transactions), a telephone number for the MO subscriber handset, or other such information. Once the information is entered, the merchant transmits it in a secured manner to MO Switch 110, which, in turn transmits it to a payment consolidation center, such as Wallet Service Center ("WSC") 112 (See Figs. 4, 14). The WSC 112 authenticates the MO Subscriber Handset 102 and tops-up the MOs Pre-paid Server 114. The MO will then send a message, for example, a Short Message Service (SMS) message, to the MO Subscriber Handset 102 updating the available airtime. This method may be used with existing generation mobile handsets.

The Retail Cash & Credit Card Payment example also illustrates an example involving the transmission of a "virtual card" to the distribution outlets and, subsequently, to MO Subscriber Handsets 102. The MO distributes virtual pre-paid cards to distribution outlets, using the Wallet Service Center 112 and Merchant ETDs 104 at the respective distribution centers. The virtual cards may be distributed wirclessly and securely. The distribution outlet may use the Merchant ETD 104, upon payment for airtime, to directly "beam" into the MO Subscriber Handset 102 a virtual pre-paid card. "Beaming" may be accomplished using infrared, such as IrDA, proximity RF, or other suitable transmission protocols and circuits. For a secure transmission of the virtual pre-paid card from the Merchant ETD 104 to the MO Subscriber Handset 102, an electronic transaction device application may be installed on the MO Subscriber Handset 102. A MO Subscriber Handset 102 with an electronic transaction device application can also beam the payment directly into the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 129 of 1360

Merchant ETD 104, using either a stored value account, or an existing credit, debit, bank card, etc. account. The electronic transaction device application may store the transaction record, and upload the records to a custom transaction portal at the WSC 112.

The example labeled as "MO Certified Cash & Credit Card Payment" allows subscribers to replenish their pre-paid airtime using the same methods detailed above – i.e. using the MOs network or the proximity method. This example differs from the Retail Cash & Credit Card Payment in that the MO certified centers of distribution includes banks, ATM's, and other special outlets. Additionally, a Merchant ETD local database 118 is coupled to the MO Network 108. As outlined in Figure 3, these centers may also be equipped with Merchant ETDs 104. Subscribers with a regular mobile handset may top-up their pre-paid accounts using the MO network, and those with the electronic transaction device application installed may use the proximity method to top-up their pre-paid account. The Merchant ETD local database 118 allows the merchant to perform batch transactions, and allows the merchant to compile the subscriber usage information locally.

The Merchant ETD 104 is equipped to conduct a real-time, or batch mode transaction, for both the proximity method and the method using the MO network. The Merchant ETD local database 118 may have a wired or wireless connection with the Merchant ETD 104, or may be connected to a local area network (LAN) associated with a merchant. Where the MO certified distributors have a direct interface with the MO's pre-paid server and database, the Merchant ETD 104 integrates into their existing LAN structure.

In additional embodiments, the Merchant ETD 104 may be distributed to non traditional distribution outlets, such as taxi drivers, where the backend authentication

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 130 of 1360

hook-up may be wireless. The contemplated non-traditional distribution outlets would have the ability to do real-time or batch transactions.

The example labeled "Only Credit Card Payment," demonstrates the setup and top-up operations using a MO Subscriber Handset 102 having an embedded MO Subscriber ETD 106 and the MOs automated system for setup and top-up operations for pre-paid airtime. The electronic transaction device application user interface provides the MO subscriber with a user-friendly device to complete the setup and top-up operations for pre-paid airtime accounts. In one example, the electronic transaction device application may be configured to store payment information locally on the mobile handset and send payment information (credit card or debit card details, etc.) every time a transaction is conducted. This information is securely sent to the WSC, through the MO switch, and to the respective payment servers and MO pre-paid server and database. Based on this process, the transaction may be considered a "Card Holder Present Transaction." Card Holder Present Transactions typically have lower processing fees than Card Holder Not Present Transactions.

Figure 4 illustrates in more detail the Retail & MO Certified Cash & Credit Card Payment" example. The MO Subscriber Handset 102 may be configured with the electronic transaction device application (i.e., embedded MO Subscriber ETD 106). Electronic communication, such as via proximity RF (such as Bluetooth) or Infra Red (such as IrDA) is established with the Merchant ETD 104. The Merchant ETD 104 is in electronic communication, preferably wireless communication, with MO Gateway. The MO Gateway is coupled to the WSC. The WSC includes, for example, an interface and security module 122, having a MO Interface 124, a payment server interface 126, a content provider, interface 128, and a Merchant interface 130, the interface and security module 122 is coupled to a transaction portal

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 131 of 1360

132. The transaction portal 132 is coupled to a added services module 134, which is coupled to a profile engine 136. The profile engine 136 interfaces with databases 138 such as a MO database 138, a Subscriber database 140, and a Merchant database 142.

Figure 5 is a process flow-chart for the pre-paid application in a retail and MO certified environment, using either cash or credit cards as the form of payment, using the mobile operator's network. In step 150, the MO Subscriber gives the Merchant ETD 104 equipped retailer cash or a credit card and a telephone number of the MO Subscriber Handset. In step 152, the Retailer enters the telephone number and desired amount of the service to purchase. Alternatively, steps 150 and 152 may be performed electronically if the MO Subscriber Handset 102 includes the electronic transaction device application. In step 154, the Merchant ETD 104 may connect to the MO switch by dialing the MO or otherwise setting up communication over available data exchange formats, such as conventional CDPD, TDMA, CDMA and GSM formats, to connect to the WSC. In step 156, the WSC authenticates the MO Subscriber and updates the MO Pre-paid Server. Additionally, the WSC updates databases for the retailer, MO Subscriber, and MO. In step 158, the MO sends confirmation to the MO Subscriber, which may be by way of SMS (Short Message Service), and in step 160 the Merchant acknowledges payment.

Figure 6 is a flow-chart, for illustrating one example pre-paid application in a retail or MO certified environment, using either cash or credit cards as the form of payment, using the proximity transmission method. In step 162, the MO distributes virtual pre-paid cards merchants. In the illustrated example, the virtual pre-paid cards are distributed by the WSC to Merchant ETD 104s wirelessly. In step 164, the MO Subscriber may purchase a Virtual Card by electronically communicating cash or credit card information from the MO Subscriber Handset 102 to the Merchant ETD.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 132 of 1360

The electronic communication may be proximity RF or Infra Red optical. In step 166, the Merchant electronically transfers the Virtual Card to the MO Subscriber's Handset. A receipt may be included with the Virtual Card transfer. In step 168, the Merchant ETD 104 sends information pertaining to the Virtual Card transaction to the MO Server by way of the WSC. In step 170, the MO updates the value in the MO subscriber's account. In step 172, the WSC updates databases such as the Merchant database, the MO database, and the MO Subscriber database. In step 174, the electronic transaction device application on the MO handset may also update the available airtime and payment records. This example requires the MO Subscriber Handset 102 to be infra red or proximity RF enabled devices (the process flow-charts in Figures 5 & 6 relate to the configuration described in Figures 3 & 4).

Figure 7 is a more detailed illustration of the "Only Credit Card Payment" example for pre-paid applications. The MO Subscriber Handset 102, including the electronic transaction device application, is in direct communication with the MO switch. The MO switch is coupled to the WSC by MO switch 110 The WSC includes, for example, interface and security module 122, coupled to the MO interface 124, payment server interface 126, Content Provider Interface 128 and Merchant Interface 130. The interface and security module 122 is coupled to transaction portal 132. The transaction portal 132 is coupled to a valve added services module 134, which is coupled to a profile engine 136. The profile engine 136 interfaces with databases such as the MO database 138, Subscriber database 140, and Merchant database 142.

Figures 8 & 9 are process flow-charts which detail the setup and top-up operations for this particular pre-paid configuration.. Referring to Figure 8, an example of steps which may be used to initialize and use a MO Subscriber Handset

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 133 of 1360

102 with an electronic transaction device application is illustrated. In step 180, a first time user activates an ETD icon 180 and in step 182 enters a MO Subscriber Handset 102 personal identification number (PIN). In the illustrated example, in step 184, a sequence will halt further use of the MO Subscriber Handset 102 after three incorrect entries. This sequence may be performed off-line.

In step 186 the MO subscriber then enters a 4 digit personal identification number (PIN) into the MO Subscriber Handset. This is to "tie-up" the subscriber, the MO Subscriber Handset 102, and the electronic transaction device application. This PIN will be matched internally to the unique MO Subscriber Handset 102 identification number PIN and error message generated for incorrect PIN. The entry of a PIN also provides user validation for a "Card Holder Present" transaction. This sequence typically will not be repeated after the initial setup is completed successfully. On subsequent uses, only electronic transaction device PIN is required. This sequence may be performed off-line.

In step 188 the MO subscriber selects payment vendor and type, and in step 190 enters a payment PIN. A Payment PIN may be pre-assigned by Payment Vendor. A Payment vendor may create a "Digital Signature" for every account and/or PIN created at the server. On verification of Payment PIN, step 192, the server will download the card details to the MO Subscriber Handset 102. The card details may include the digital signature. The digital signature is stored locally on the MO Subscriber Handset 102 for subsequent use. This sequence may be performed on-line.

In step 194, the MO subscriber may then select a type of MO pre-paid card (Gold, Platinum, etc.) and in step 196 an amount for the pre-paid card. The MO Subscriber Handset 102 with ETD application may dial out to the Wallet Service Provider and/or MO Server and download Pre-Paid Account details from the Server.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 134 of 1360

This unique pre-paid account detail is stored on the MO Subscriber Handset 102 for subsequent use.

When the MO subscriber confirms payment in step 198, The MO Subscriber Handset 102 with ETD application may dial out to the Wallet Service Provider, debit the Payment account with the amount selected, and credit the Pre-Paid account at the WSC / MO server in step 200. A receipt acknowledging the request and confirming payment may be returned to the MO Subscriber Handset 102.

The Airtime minutes available, available Credit with the Payment Partner and Receipt for the transaction may all be stored on the device. Real time data is obtained from the respective servers during on-line sequence. All subsequent computations may be internal to the MO Subscriber Handset 102 having the ETD application.

Referring to Figure 9, an example of a credit card payment top off sequence flow chart is illustrated. The MO subscriber activates an ETD icon on the MO Subscriber Handset in step 202, and then enters a PIN in step 204. The PIN is verified as correct in step 206. The PIN is "tied-up" to the SIM Card on the MO Subscriber Handset 102. The PIN entered is matched to the PIN stored in the ETD application during the setup sequence, illustrated in Fig. 8.

In step 208, display may be activated to display current airtime available for use. In step 210, the MO subscriber may be queried as to whether to top off the pre-paid account. If yes, the MO subscriber may select the top off amount in step 212, select payment and vendor type in step 214, and enter a payment vendor PIN in step 216. PINs may be different for different payment vendors.

In step 218, if the PIN is correct, payment is confirmed in step 220. "PIN & Pay" triggers transmission of Digital Signature/Payment Account details stored on the device, along with the amount selected in step 222. This encrypted and secure

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 135 of 1360

information is sent to the WSC/Payment server. On verification, the amount is debited from the Payment Server & credited to the MO Pre-paid Server. This may be the only on-line activity during the "top-off" sequence.

Figures 10 & 11 illustrate some User Interface screens on the MO Subscriber Handset 102. Referring to Figure 10, a first screen display 224, the user interface may include a graphical log for the electronic transaction device 226, a logo for the MO 228, and a log for the Payment vendor 230. A second screen display 232 may include a graphical image of a pre-paid card 234 and icons for talk time 236, top-off 238, set up 240, and exit 242. A third screen display 244, which may be displayed when top-off is selected, includes a MO pre-paid card image 248 with icons 248 for selecting a value to purchase. Additional displayed icons include talk time 236, top-off 238, Cancel 250, and main 252. A Fourth screen display 254 may be displayed after an amount is selected. The fourth screen display includes a MO Pre-paid card image 256 having icons for calling credit 258, service credit 260, and combination 262. An additional icon is a Buy icon 264.

Once the Buy icon 264 is activated, a fifth screen display 266 (Fig. 11) may be displayed. The fifth screen display 266 may include an image of a conventional credit card 268. Icons on the fifth screen display may include available credit 270, Pay 272, Receipt 274, and Main 252.

Once the Pay icon 272 is activated, a sixth screen display 276 may be displayed. The sixth screen display 276 may display a confirmation that the transaction is complete 278, and icons for available credit 270, Pay 272, Receipt 274, and Cancel 250.

A seventh screen display 280 may include icons for receipt archives 282, available credit 270, and cancel 250. An eighth screen display 284 may include an

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 136 of 1360

image of a pre-paid card 286 having a display for available air time 288. Icons for the eighth screen display 284 include talk time 236, top-off 238, set up 240, and exit 242.

Figure 12 illustrates one example of the internal architecture of the Merchant ETD 104. The Merchant ETD 104 may comprise components similar to or the same as a mobile handset – keypad 300, internal hardware, such as system microprocessor, memory software & BIOS 302, the mobile operator's connectivity interface 304 (Analog, Digital, PCS, GSM, etc.) and the wireless interfaces for proximity transmission using infrared or possibly proximity RF 306. The Merchant ETD 104, in addition to the above components typical to mobile handsets, may also have the point of sale interfaces 308 for receipt printers and other peripherals commonly used in a retail environment, such as bar-code scanners, and a modem for conventional local-line access 310. In one example, the Merchant ETD 104 is a software application installed on an existing mobile handset. In alternative examples, the Merchant ETD 104 may be a personal digital assistant ("PDA") or dedicated hardware embodiment with the above outlined modules and enabling software, to conduct secure real-time or batch transactions.

The Merchant ETD 104 includes a software application loaded into the environment, which will allow it to exchange transaction information with another mobile handset with the electronic transaction device functionality (or alternately a UET Card – PDA's, etc., with electronic transaction device functionality), using a proximity method, or using the MO. The proximity method involves the beaming of a virtual pre-paid card from the Merchant ETD 104 to the subscriber's handset, and optionally, the electronic transaction device beaming payment information back into the Merchant ETD 104. The Merchant ETD 104 has the capability to capture this transmission through its infrared or proximity RF transceivers, and process it to

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 137 of 1360

complete the transaction. This information is transmitted between the two handsets using existing industry standards and protocols, but is a secure transmission. One example of a server transaction uses the exchange of public/private keys to encrypt/decrypt the data – a PKI scheme), using secure transaction technology ensuring data integrity between the two mobile handsets or devices.

Alternatively, the Merchant ETD 104 may also be programmed to securely upload or beam a "virtual pre-paid airtime card" to another mobile handset in a proximity transmission, maintaining the integrity of the mobile operator's card distribution schemes. The Virtual Card is an electronic version of the physical plastic card. The information, be it an authorization code which is scratched off or any other encoded data, would be transmitted to the Merchant ETD 104 and stored, and consequently delivered or re-transmitted to the receiving mobile handset. One possible configuration of a non-proximity model would include a series of SMS messages between the mobile operator's network and the Merchant ETD 104.

Figure 13 describes some User Interface potential screens for the Merchant ETD 104, which are based on the process flow charts detailed in Figures 5 & 6. A first display screen 320 for the Merchant MTD includes an ETD Logo 322 an a MO logo 324. A second display screen 326 includes a Form 328 for entering Merchant ID and PIN. Also included are icons for Exit 330 and Done 332.

A third display screen 334 includes a form for entry of a MO subscriber telephone number 336, icons for selecting an amount of value purchased 338, icons to select between Cash 340, Debit Card 342, Credit Card 344, or Other 346, and Icons for Previous 348 and Done 332. A Fourth display screen 350 includes a icon to select Mobile Operator 352 and an icon to beam a virtual card 354. A Fifth screen display 356 includes a display of the airtime available 358 for the given telephone number.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 138 of 1360

The Fourth display screen 356 also includes a display confirming completion of the transaction 360. On the MO subscriber handset, a screen display 362 including an identification of the Mobile Operator and logo 364 and available airtime 366 may be displayed.

Figure 14 illustrates one example of the architecture of the Wallet Service Center (WSC). The WSC connects to the MO Subscriber handsets or electronic transaction devices through the MO switch. The WSC also has interfaces to the MO servers and databases, the Banks or Payment Partners, the Merchants (retail, "e or m-tailers") and Content Providers. The WSC may use a PKI/wPKI based security scheme to secure all the information being transmitted between the various entities outlined above. Some of the core features of the WSC are to support electronic transaction device users and allow all users to create a personalized transaction portal - allow them to archive all transaction records, and setup personal, financial and health information. The WSC, based on the rich profiles it creates, then offers various value added services, such as Personal Services, Financial Services, Health Services, Merchant & Vendor Services, Business to Business Services, and Government, Corporate and Educational Services.

Figure 15 illustrates an example of a "Virtual Card" Generation & Download. A "Virtual Card" is an electronic version of plastic cards. The Virtual Card is a digital representation of the information which would be conventionally stored on a magnetic stripe, or smart card chip, or a bar code, etc., of a plastic card, along with the logo and branding information securely stored to prevent unauthorized duplication. This information may then be wirelessly transmitted to the MO Subscriber Handset 102, PDA, etc. with electronic transaction device application. The "Virtual Card" generation module 320 is responsible for the creation of Virtual Cards. In one

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 139 of 1360

example (labeled A), the "Virtual Card" Generation Module 320 may be hosted in the WSC. The WSC, which has access to the MOs Pre-paid Server and databases, would then create a virtual pre-paid card. This virtual pre-paid card may then be downloaded, or transmitted wirelessly using the MO's Switch to the Merchant ETD 104, or alternately directly into the subscriber's mobile phone. Secure batches of virtual pre-paid cards may be created and downloaded to the Merchant ETD 104, to then be distributed wirelessly by the Merchant ETD 104 using a proximity method (as outlined in Figures 4 & 6).

In another example, the Virtual Card generation module may be hosted outside the WSC, but within the MO's Network (labeled B). As may be the case with the generation of Credit Cards, Debit Cards, etc., the Banks and Financial Institutions may not be comfortable with another entity issuing their cards. In such a case, the Virtual Card generation module would be integrated with the Bank's or Financial Institution's payment server. These cards may still be wirelessly downloaded through the MO's Switch.

Figure 16 describes a "Stored Value Application." Similar to the examples illustrated in Fig. 3 to setup or replenish a pre-paid airtime account (or disable), the mobile operator may setup a stored value account for their subscribers in a MO stored value server and database 372. While a mobile telephone account is used as an example, the use of stored value cards is not limited to telephone applications. For example, stored value cards may be used for cash payments in proximity transactions, such as, but not limited to, vending machines, tolls, parking, and transportation.

The Wallet Service Center 112 may create and manage separate accounts for the MO Subscribers. For example, the Wallet Service Center 112 may create a stored value account, where the MO Subscriber would create a debit account by depositing

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 140 of 1360

funds with the mobile operator. The MO Subscriber may then purchase goods from a merchant that uses a Merchant ETD through the examples described earlier e.g., by using a proximity transaction method or using the MO Switch. For example, the MO Subscriber may purchase products and services provided by the merchant including, but not limited to, pre-paid airtime, using the MO Subscriber ETD 106. As in the examples given above, and in the examples that follow, the MO Subscriber ETD 106 may be embedded in the MO Subscriber Handset 102. The merchant follows the same methods described earlier, with the additional step of deducting the amount of the transaction from the stored value account the subscriber creates with the mobile operator.

The authentication of the transaction may involve both the merchant and the MO Subscriber through, for example, a messaging system operated by the mobile operator. A record of the transaction may be provided by the WSC, and/or through the mobile operator's messaging service. In another example, the Merchant ETD transfers a record of the transaction to the MO Subscriber ETD 106. The Wallet Service Center may create and track this account for the mobile operator, as the MO Subscriber uses the funds from this account to pay for products and services purchased from merchants.

In another example, MO Subscribers having a stored value account may obtain a cash advance from the Merchant ETD. In this example, the MO Subscriber liquidates a certain amount of the debit (or credit) account previously setup with the mobile operator. The Merchant ETD effectively becomes an ATM outlet.

In addition to the stored cash value accounts, the mobile operator may decide to add a credit functionality to this process, and become a credit account vendor as well.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 141 of 1360

The billing in any of these examples may be in the form of a consolidated or separate statements from the mobile operator. The consolidated statement details the airtime used followed by a section that details how the stored value account was depleted. Separate statements, on the other hand, provide separate statements for telephone usage and stored value account usage. The Wallet Service Center may use the mobile operator's messaging system to update the MO Subscriber ETD 106 with balance information. As in the above examples, the ETD may be embedded in a MO Subscriber Handset 102.

Figure 17 illustrates an example of the stored value transaction system using the mobile operator's network. MO Subscriber Handset 102 is in electronic communication with MO switch 110. A merchant POS terminal is also in electronic communication with the MO switch 110. In the illustrated example, the merchant POS is a Merchant ETD 104. Other POS equipment may be suitable. The MO switch 110 is coupled to Wallet Service Center 112. WSC is coupled to MO Stored Value Server 372, MO Prepaid Server 114, and Payment Server 116. This system does not necessarily require any modifications on the subscriber's mobile phone, but merely requires the subscriber to establish a stored value account with the mobile operator. The subscriber may setup a stored value account using, for example, the following methods:

Subscriber may deposit money at a mobile operator certified distribution outlet using cash, credit, debit, check, etc. to pay the merchant. The merchant then dials into the mobile operator's system to update the subscriber's account. The merchant may use the Merchant ETD to update the subscriber's stored value account.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 142 of 1360

The subscriber may directly access his/her account securely using the ETD to top-up his/her stored value account. The subscriber may replenish the account using a credit card, debit card, or any other acceptable payment product, from the ETD.

The subscriber may access his/her stored value account from the Internet, by paying using a credit card or a debit card.

The subscriber may pay the mobile operator directly, by including an extra payment over and above the billed amount for wireless services every month. This extra amount may then be credited to the stored value account housed by the mobile operator.

Once the MO Subscriber creates the stored value account with the mobile operator, the MO Subscriber may conduct a transaction by merely specifying the account number to the merchant with a Merchant ETD 104. The account number may be a telephone number corresponding to the MO Subscriber. Referring to Figure 18, in step 402, the MO Subscriber selects merchandise or services at a Merchant's POS location. In step 404, the merchant turns on the Merchant ETD, enters a password, enters the MO Subscriber's account details, and the amount of merchandise / services desired by the MO Subscriber. In step 406, the Merchant sends the information to the WSC, through the mobile operator's switch by the Merchant ETD. In step 408, the WSC authenticates the merchant, the MO Subscriber, and ensures that the stored value account has enough funds (alternately available credit balance, if the mobile operator offers a credit facility to the subscriber) to cover the transaction. The WSC also updates the internal databases on the merchant, subscriber and mobile operator. In step 410, once the transaction is approved, the WSC requests the mobile operator to send a unique transaction ID, for security purposes, in the form of a short message (if service available) to both the merchant and the MO Subscriber, completing the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 143 of 1360

transaction. In step 412, the Merchant acknowledges the MO Subscriber's payment. In step 414, the MO Subscriber received a message, for example, a SMS message, from the WSC specifying the new balance in the stored value account.

Figure 19 illustrates a proximity transaction based stored value system. MO Subscriber ETD 106 (which may be embedded in MO Subscriber handset 102) is in electronic communication with a merchant POS terminal. In the illustrated example, the merchant POS is a Merchant ETD 104. Other POS equipment may be suitable. The Merchant ETD is in electronic communication with MO switch 110, which is in turn coupled to Wallet Service Center 112. WSC is coupled to MO Stored Value Server 372, MO Prepaid Server 114, and Payment Server 116.

Referring to Figure 20, in use, the WSC distributes electronic, or virtual, stored value cards in step 420. The virtual stored value cards may be distributed directly to the MO Subscriber ETD. Alternatively, the virtual stored value cards may be distributed to the Merchant ETDs. Mobile operator certified distributors may be authorized to distribute these cards on a proximity basis to subscribers. These cards may be purchased at retail locations. In other examples, stored value accounts may be replenished using the methods described above to top off prepaid accounts. The virtual stored value cards may be issued wirelessly and securely, and may be stored in the MO Subscriber ETD, containing user information, issuer information, amount details, and other authentication information.

In step 422, to conduct a transaction using the stored value card, the MO Subscriber selects the card in the ETD, and transfers the desired amount into the merchant POS. Any suitable electronic communication may be used for the transfer, including, but not limited to, infrared or proximity RF. In step 424, the Merchant ETD authenticates the MO Subscriber's virtual stored value card and transfers a

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 144 of 1360

receipt of the transaction to the MO Subscriber ETD. In step 426, the merchant uploads relevant transaction information to the stored value server hosted by the WSC and the mobile operator. The upload may be performed at a later time in a batch of transactions. In step 428, the WSC updates the MO Subscriber's stored value account information. In step 430, the WSC updates the internal merchant, mobile operator, and subscriber databases.

The stored value system described herein provides a secure and cost effective transaction network. In part because the stored value system is hosted by the mobile operator and the WSC, wireless transactions are enabled. Also, by using the mobile operator's network, the administration cost of the transaction may be significantly reduced as the number of intermediaries is reduced. The WSC, along with the ETD and the Merchant ETD ensure end to end security, and global deployment. Since authentication may be enforced by the ETD and Merchant ETD at the POS, this system may drastically reduce fraud. The WSC, through its profiling capabilities, can reduce the customer acquisition costs.

The Merchant ETD may be deployed in markets where the existing banking networks do not have a presence, consequently increasing transaction volume for existing banking entities involved in the deployment of this solution. The stored value systems may be effectively extended to minors and credit challenged individuals, again increasing the addressable markets and consequently transaction volume. This system may also be extended for people to people payments, where two individuals with ETD's may transact directly on a proximity basis. The stored value system will also reduce cash transactions and associated costs. Even in markets where the transactions are predominantly cash based, the Merchant ETD, along with the tracking capabilities may be used to reduce fraud and theft.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 145 of 1360

Figure 21 illustrates an environment in which a single Merchant ETD 104 has the capability to interface with multiple mobile operator networks for the purposes of offering electronic pre-paid airtime or stored value applications, as outlined before, to their respective subscribers. An example would be a single merchant location, enabled with a single Merchant ETD unit, having the capability to electronically issue pre-paid airtime to Sprint PCS, Cellular One, AT&T, PrimeCO, Bell Atlantic, Bell South, etc. subscribers. This same Merchant ETD would also have the capability to allow all the different subscribers to use their respective stored value accounts hosted by the respective mobile operators.

Figure 22 illustrates examples of user interface screens for the Merchant ETD 104 in a Multiple MO environment. In a first screen 440, icons for a plurality of MO's 442 are displayed. In a second screen 444, a form for entering Merchant Identification and PIN 446 is displayed, along with icons for Exit 448 and Done 450. IN a third screen 452, a form for entry of the MO Subscriber telephone number 454 is displayed. Also displayed are icons for selecting an amount of value paid 456, and icons for form of payment, e.g., Cash 458, Credit Card 460, Debit Card 462, or Other 464. Additional displayed icons include Previous 466, and Done 450. In a fourth screen 468, icons for selecting between MO's 470 are displayed. Also, an icon for transferring the virtual card 472 is displayed.

Figure 23 describes an existing transaction system and a wireless transaction system. One of the purposes of this patent is to introduce a new transaction system, which includes the Merchant ETD at the POS (and possibly the ETD, in certain embodiments), along with the Wallet Service Center. The existing transaction system typically consists of a POS 380, or retail environment. This is connected, through a secure banking network 382 to the acquirers 384 and eventually back to the issuer 386

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 146 of 1360

of the payment product – Credit Cards, Bank Cards, Debit Cards, etc. The acquirers 384 and issuers 386 may possibly be controlled by the same organization, or may be different entities bound by an arrangement to clear transactions – American Express and DISCOVER are examples of the first kind, MasterCard and VISA are examples of the later. The new wireless transaction system consists of a Merchant ETD at a wireless POS 388, wirelessly connected to the Mobile Operator's switch 110, which in turn is connected to the Wallet Service Center 112. The Wallet Service Center may be connected either to the acquirer or directly to the issuer, or possibly both, based on the acquirer – issuer relationship. The nature of the connection between the Mobile Operator's switch, the Wallet Service Center, and the acquirer – issuer's systems may be a wired or wireless connection. The ETD, Merchant ETD and Wallet Service Center ensure the security of the transaction data as it wirelessly flows from the POS location, through the Mobile Operator's switch, eventually to the acquirer – issuer's systems.

Based on the nature of the electronic transaction device application transaction, whereby the payment information (credit card details, account number, etc.) is stored and transmitted from the mobile handset, only after being initiated by the user (user enters unique password, which along with a unique handset device number – SIM, WIM, etc. – is translated into a unique key, or treated as a "digital signature" to validate the transaction) – the transaction is of a "Card Holder Present" nature. The electronic transaction device application allows the subscriber to use a credit card to setup and top-up their pre-paid account, and at the same time allows the mobile operator to pick up the savings of the reduced credit card issuer fee for a "CHP" transaction.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 147 of 1360

Using the electronic transaction device application User Interface, the subscriber now has a simple menu driven, graphical, user friendly procedure of selecting the amount of airtime required, and the payment vendor and account (credit, debit, etc.) to be used. The electronic transaction device application on the mobile handset will also allow the subscriber to store the receipt of the transaction, show the updated airtime and payment account balances. Thus the mobile operator may now use the electronic transaction device application on mobile handsets, along with its automated system, to allow their pre-paid subscribers to setup & top-up their accounts using their handsets. This removes the requirement of a customer service representative to have a dedicated session with the subscriber, and also offers a lot less cumbersome alternative to the automated setup and top-up methods.

The Merchant ETD 104 may be used for distributing pre-paid airtime, either using the MO's network and existing mobile handsets, and later on by issuing "virtual pre-paid cards." The Merchant ETD 104 may be used in a retail environment or at the certified distribution centers – bank locations, ATMs, or over the counter locations. The Merchant ETD 104 supports cash, credit card, debit card, etc. transactions. The Merchant ETD 104 allows the mobile operator to immediately reduce all costs associated with the generation, packaging and distribution of physical plastic cards. The Merchant ETD 104 also allows the mobile operator to remotely issue and track the distribution of their pre-paid products, removing all costs associated with the physical tracking of inventory. This model also gives the mobile operator the flexibility to enhance the services and products, and at the same time rapidly deliver these new offerings to their subscribers.

The same set of advantages applies to the merchants in the retail and virtual (e & m-tailers) environments. The mobile operator may use the Merchant ETD 104 to

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 148 of 1360

distribute pre-paid "Virtual Cards", thereby immediately reducing all costs associated with the generation, packaging and distribution of plastic. Since the Merchant ETD 104 eliminates the requirement of shelf space, and also removes the element of "physical inventory management" on the retailers part, the mobile operator is essentially in a position to negotiate reduction in retailer margins.

The Merchant ETD 104 may also be used to enhance or upgrade the current offering of products and services, and rapidly and remotely deliver these to their subscribers, with minimal costs associated. Add to these savings, the savings associated with the card holder present transaction, when the electronic transaction device application is used by the subscriber, and subsequently reduction in cash handling costs, etc.

In conjunction with the electronic transaction device application and Merchant ETD 104 products, the Wallet Service Center (hereby incorporated by reference) also allows the mobile operator to create a trail of otherwise untraceable "cash" transactions/subscribers. This is beneficial in terms of allowing the mobile operator to better understand their subscribers and cater additional products and services to them. This also, in light of law enforcement requirements by government agencies, allows the mobile operator and law enforcement agencies to track unlawful use of pre-paid phones.

In summary, present invention is that it allows MO's to extract more value, and hence immediate profitability, from their existing distribution models – be it in terms of eliminating cost of producing and distributing plastic, or the high commission paid to the retailers, or the CHP nature of all credit card transactions. The present invention allows the mobile operator to create alternate distribution

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 149 of 1360

channels, giving them the ability to modify each existing mobile handset into a potential point of sale terminal.

The electronic transaction device application gives the mobile operator the presence on the subscriber's handset, the Merchant ETD 104 gives them the ability to distribute products and services in a retail environment, essentially taking the mobile operator beyond the m-commerce space. The WSC gives the mobile operator the ability to continuously keep adding on value added services for their subscribers, merchants and vendors. Thus, the mobile operator now has the ability to create a trace of their subscribers, including the subscribers that typically pay cash and leave no personal information behind. The WSC creates a profile for each subscriber, whether they use cash or credit cards, or debit cards, etc. to pay for the pre-paid airtime. This is also helpful for the law enforcement agencies to curb the misuse of pre-paid phones for unlawful activities. In addition, the WSC allows the mobile operator to efficiently track the airtime top-up for all their subscribers, independent of who the subscriber is or how they purchased their pre-paid airtime. The WSC creates a better and more efficient management system between the mobile operators and various distributors they use in the retail and non-retail environment.

The WSC, along with the electronic transaction device application and Merchant ETD 104, creates the optimum platform for the mobile operator to offer various value added services and products to their subscribers, merchants and services. The stored value application is an example of how the mobile operator may use the same infrastructure installed to electronically distribute pre-paid airtime, to allow their subscribers to buy products and services from the merchants equipped with a Merchant ETD.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 150 of 1360

The new wireless transaction system introduced, which includes the ETD, Merchant ETD and Wallet Service Center, would now make the entire transaction more secure and profitable. In one embodiment, the ETD securely and wirelessly transmits the payment information from the user to the Merchant ETD, or directly to the WSC. In another embodiment the Merchant ETD directly relays the transaction data to the WSC. Both these configurations reduce the element of fraud at the POS, where now the user of the ETD, or the merchant using the Merchant ETD are authenticated. The transaction data is also securely transmitted from the user to the POS to the acquirer – issuer's system, with less intermediaries, reducing the potential of fraud. The new system also reduces the cost of a transaction by reducing the intermediaries, thereby allowing the acquirer – issuers to channel the cost savings back to the user.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 151 of 1360

What is claimed is:

1. A method of exchanging payment information in an electronic transaction, comprising:

a) a first electronic transaction device transferring payment information to a second electronic transaction device;

b) the second electronic transaction device transferring value information to the first electronic transaction device;

c) the second electronic transaction device transferring value information and payment information to a service consolidation center.

2. The method of claim 1, wherein the value information comprises a virtual card.

3. The method of claim 2, wherein the virtual card comprises an authorization code.

4. The method of claim 2, wherein the virtual card comprises an image of a card.

5. The method of claim 1, wherein the value information comprises a quantity of minutes corresponding to a pre-paid telephone account.

6. The method of claim 1, wherein the payment information comprises cash payment information.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 152 of 1360

7. The method of claim 6, wherein the cash payment information includes an identification of a person providing a cash payment.

8. The method of claim 1, wherein the payment information comprises credit payment information.

9. A method of tracking retail sales of pre-paid telephone cards to cash subscribers comprising:

a) entering value purchased information and subscriber information in a retailer electronic transaction device;

b) the retailer electronic transaction device transferring the value purchased information and subscriber information to a mobile operator;

c) the mobile operator adding value corresponding to the value purchased information to an account corresponding to the subscriber information.

10. The method of claim 9, wherein the step of entering value purchased information and subscriber information in a retailer electronic transaction device further comprises electronically transferring the value purchased information and subscriber information from a MO subscriber handset to the retailer electronic transaction device.

11. The method of claim 9, wherein the step of entering value purchased information and subscriber information in a retailer electronic transaction device further comprises manually entering the value purchased information and subscriber information into the retailer electronic transaction device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 153 of 1360

12. A method of distributing virtual pre-paid cards comprising:

a) creating a virtual pre-paid card;

b) downloading the virtual pre-paid card to a retailer electronic transaction device,

c) transferring the virtual pre-paid card from the retailer electronic transaction device to a MO Subscriber Handset 102.

13. The method of claim 12, further comprising the step of transferring payment information from the MO subscriber handset to the retailer electronic transaction device.

14. The method of claim 12, wherein the step of creating a virtual card is performed by an electronic transaction device service center.

15. The method of claim 14, further comprising the steps of:

a) transferring payment information and subscriber information from the MO subscriber handset to the retailer electronic transaction device; and

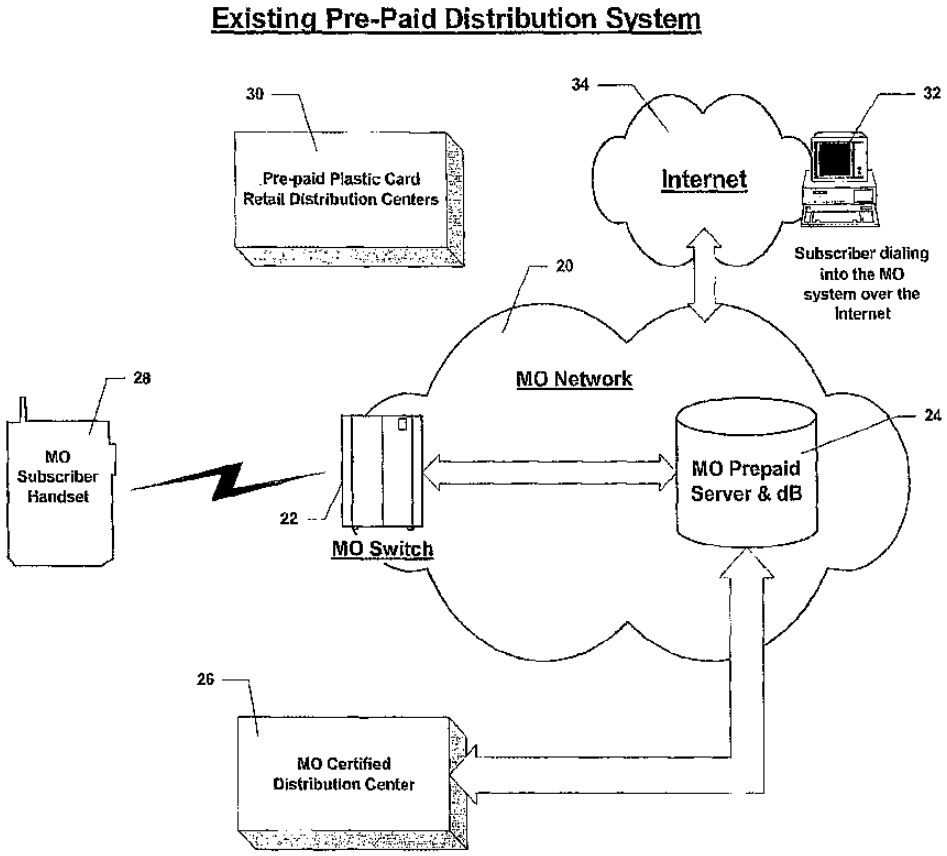
b) transferring the payment information and subscriber information from the retailer electronic transaction device to the electronic transaction device service center.

16. The method of claim 14, wherein the step of downloading the virtual card to a retailer electronic transaction device occurs via a MO switch.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 154 of 1360

17. The method of claim 12, wherein the step of creating a virtual card comprises creating a plurality of virtual cards and the step of downloading the virtual card to a retailer electronic transaction device comprises downloading batches of virtual transaction cards to the retailer electronic transaction device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 155 of 1360

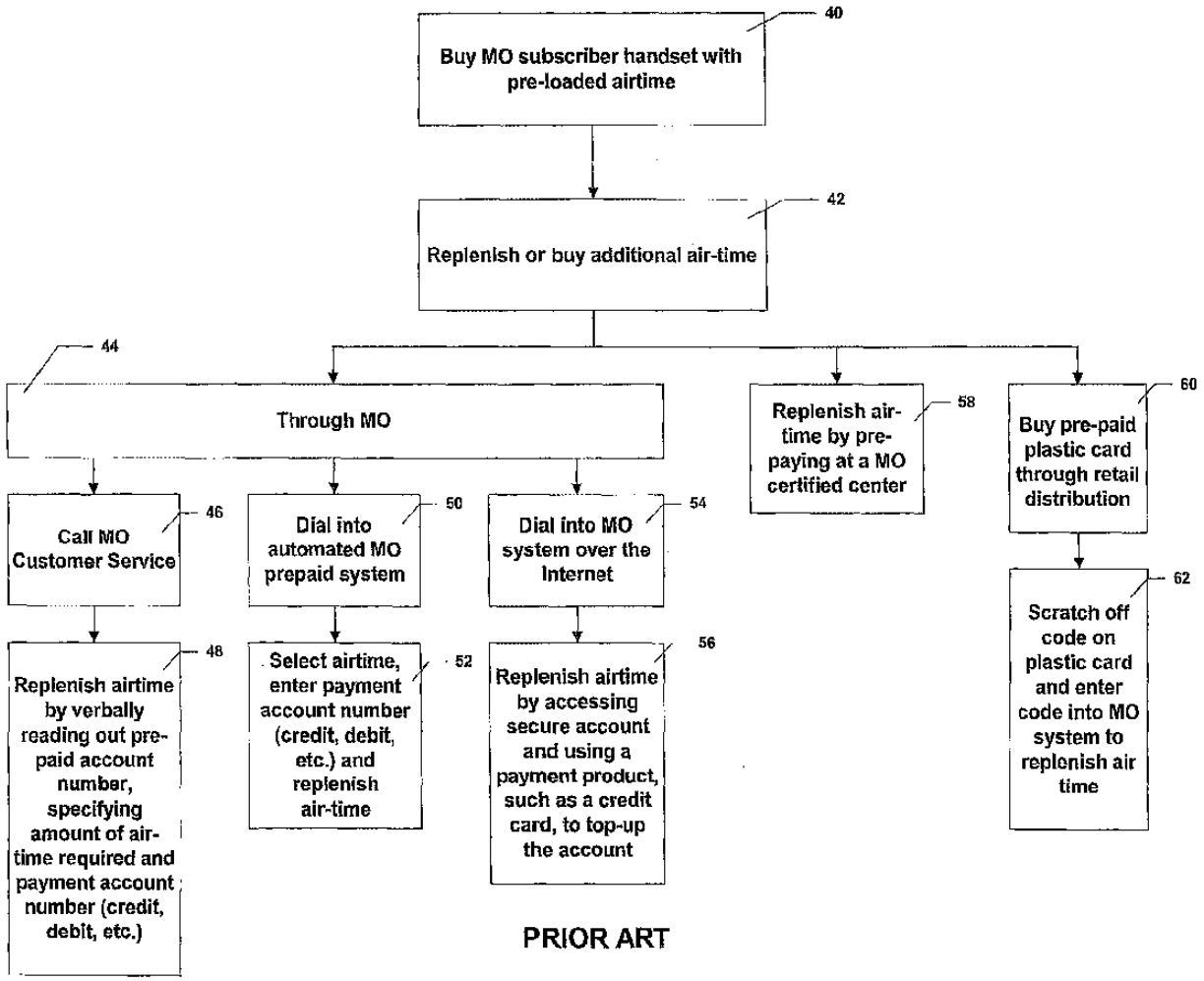


PRIOR ART

Figure 1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 156 of 1360

Existing Pre-Paid Distribution Flow



PRIOR ART

Figure 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 157 of 1360

Electronic Pre-paid Distribution System

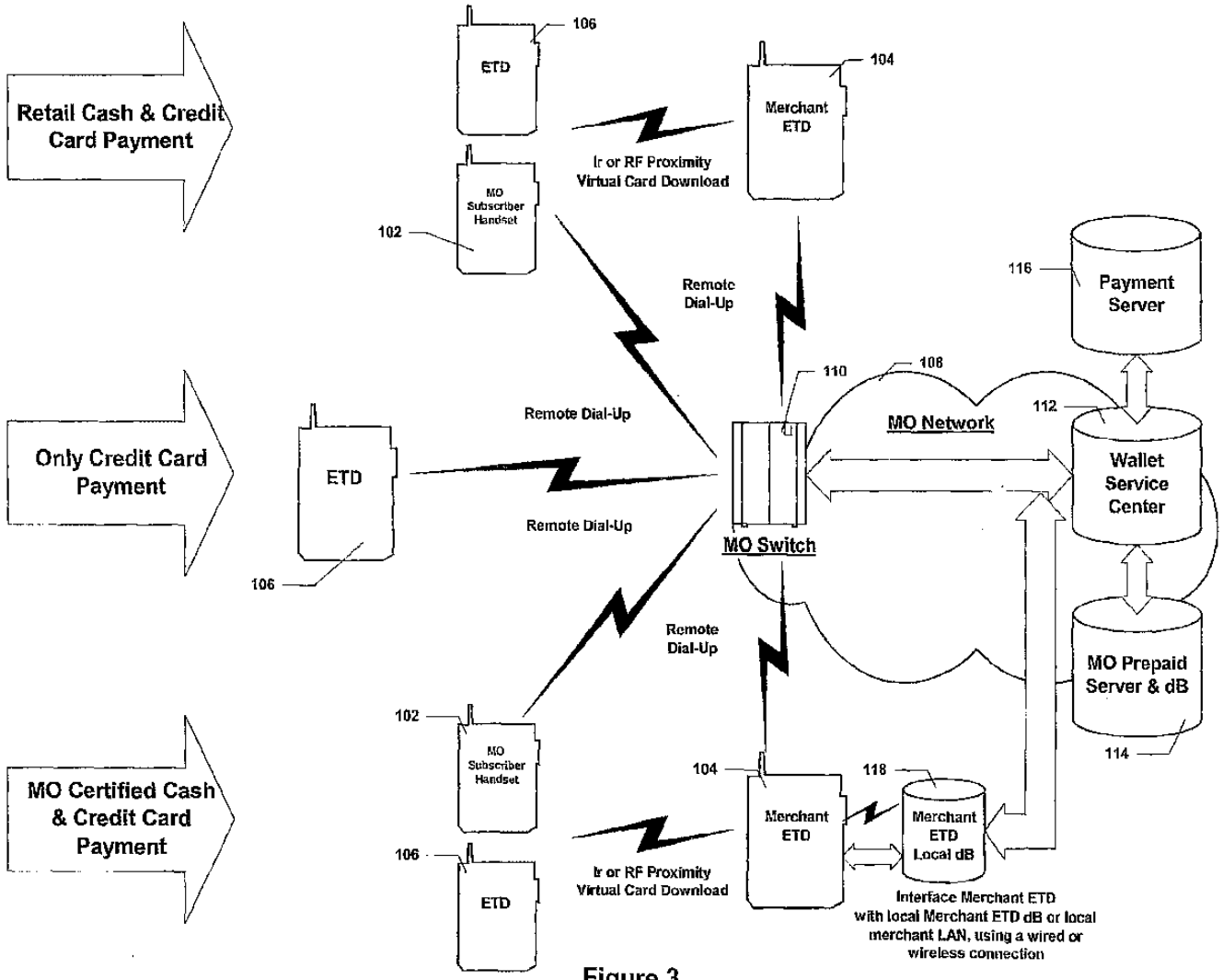


Figure 3

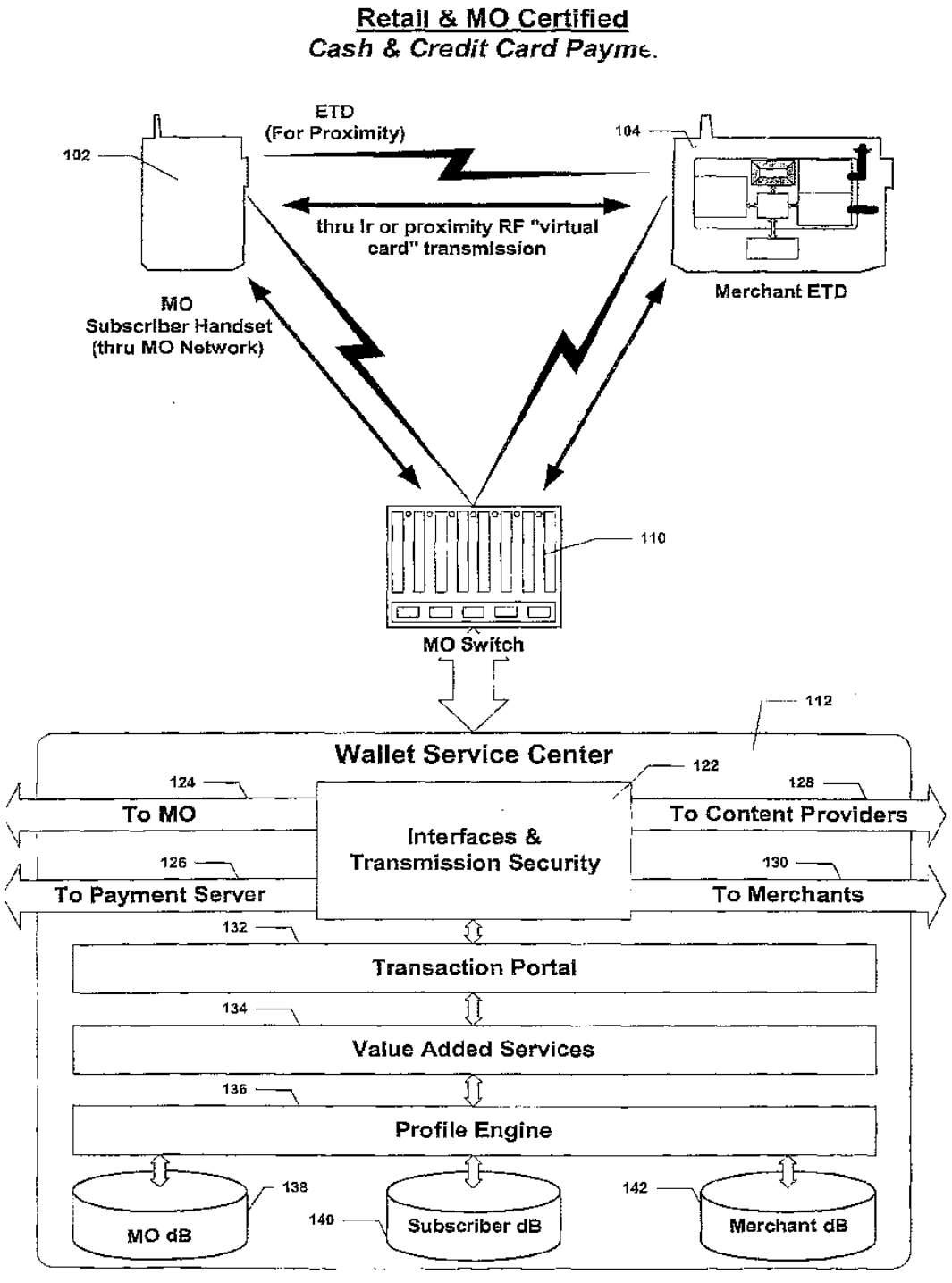

Retail & MO Certified
Cash & Credit Card Payme.
ETD
(For Proximity)
102
104
thru Ir or proximity RF "virtual card" transmission
MO
Subscriber Handset
(thru MO Network)
Merchant ETD
110
MO Switch
112
Wallet Service Center
122
124
128
To MO
Interfaces &
Transmission Security
To Content Providers
126
130
To Payment Server
To Merchants
132
Transaction Portal
134
Value Added Services
136
Profile Engine
138
142
MO dB
140
Subscriber dB
Merchant dB

Figure 4

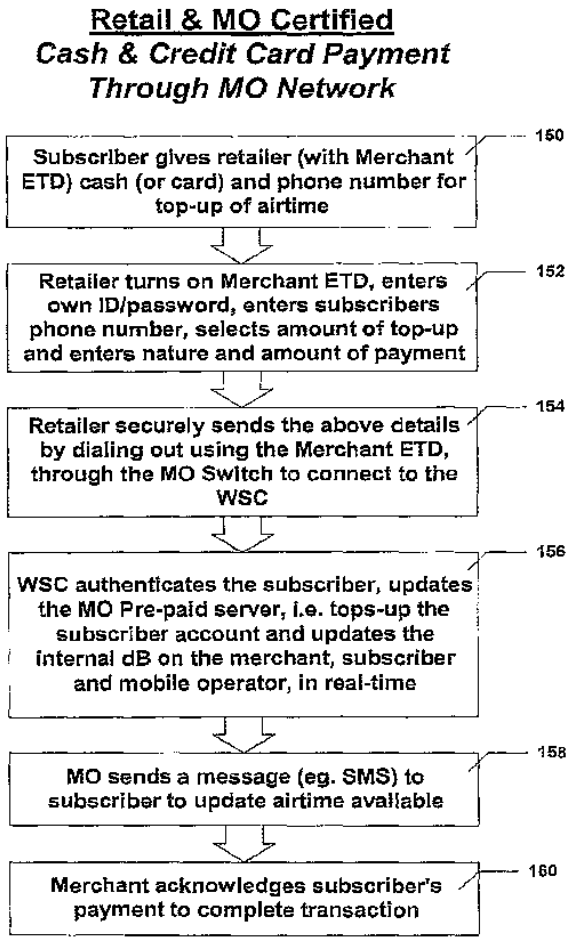

Retail & MO Certified
Cash & Credit Card Payment
Through MO Network
Subscriber gives retailer (with Merchant ETD) cash (or card) and phone number for top-up of airtime
150
Retailer turns on Merchant ETD, enters own ID/password, enters subscribers phone number, selects amount of top-up and enters nature and amount of payment
152
Retailer securely sends the above details by dialing out using the Merchant ETD, through the MO Switch to connect to the WSC
154
WSC authenticates the subscriber, updates the MO Pre-paid server, i.e. tops-up the subscriber account and updates the internal dB on the merchant, subscriber and mobile operator, in real-time
156
MO sends a message (eg. SMS) to subscriber to update airtime available
158
Merchant acknowledges subscriber's payment to complete transaction
160

Figure 5

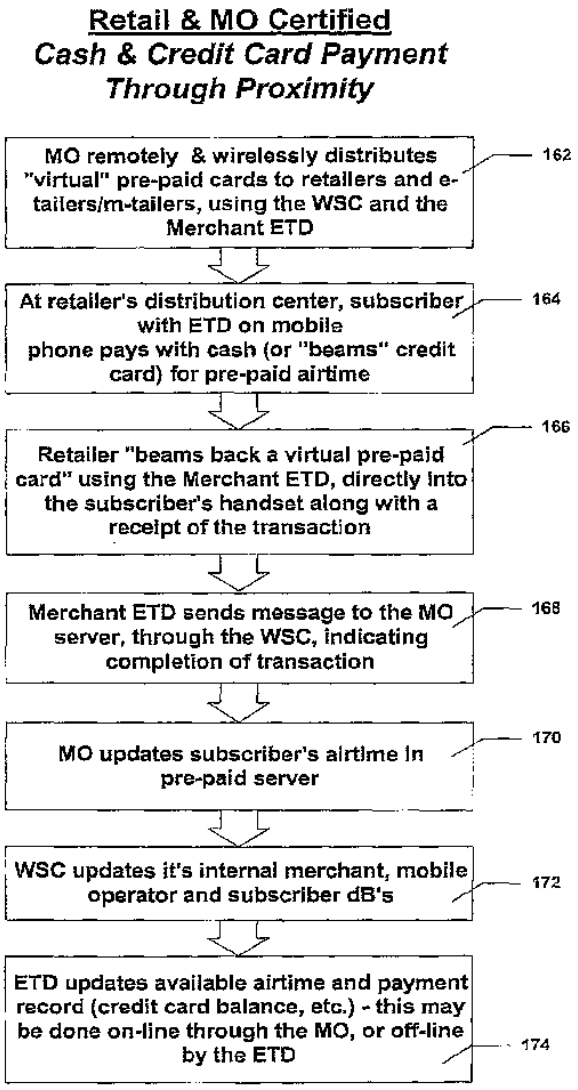

Retail & MO Certified
Cash & Credit Card Payment
Through Proximity
MO remotely & wirelessly distributes "virtual" pre-paid cards to retailers and e-tailers/m-tailers, using the WSC and the Merchant ETD
162
At retailer's distribution center, subscriber with ETD on mobile phone pays with cash (or "beams" credit card) for pre-paid airtime
164
Retailer "beams back a virtual pre-paid card" using the Merchant ETD, directly into the subscriber's handset along with a receipt of the transaction
166
Merchant ETD sends message to the MO server, through the WSC, indicating completion of transaction
168
MO updates subscriber's airtime in pre-paid server
170
WSC updates it's internal merchant, mobile operator and subscriber dB's
172
ETD updates available airtime and payment record (credit card balance, etc.) - this may be done on-line through the MO, or off-line by the ETD
174

Figure 6

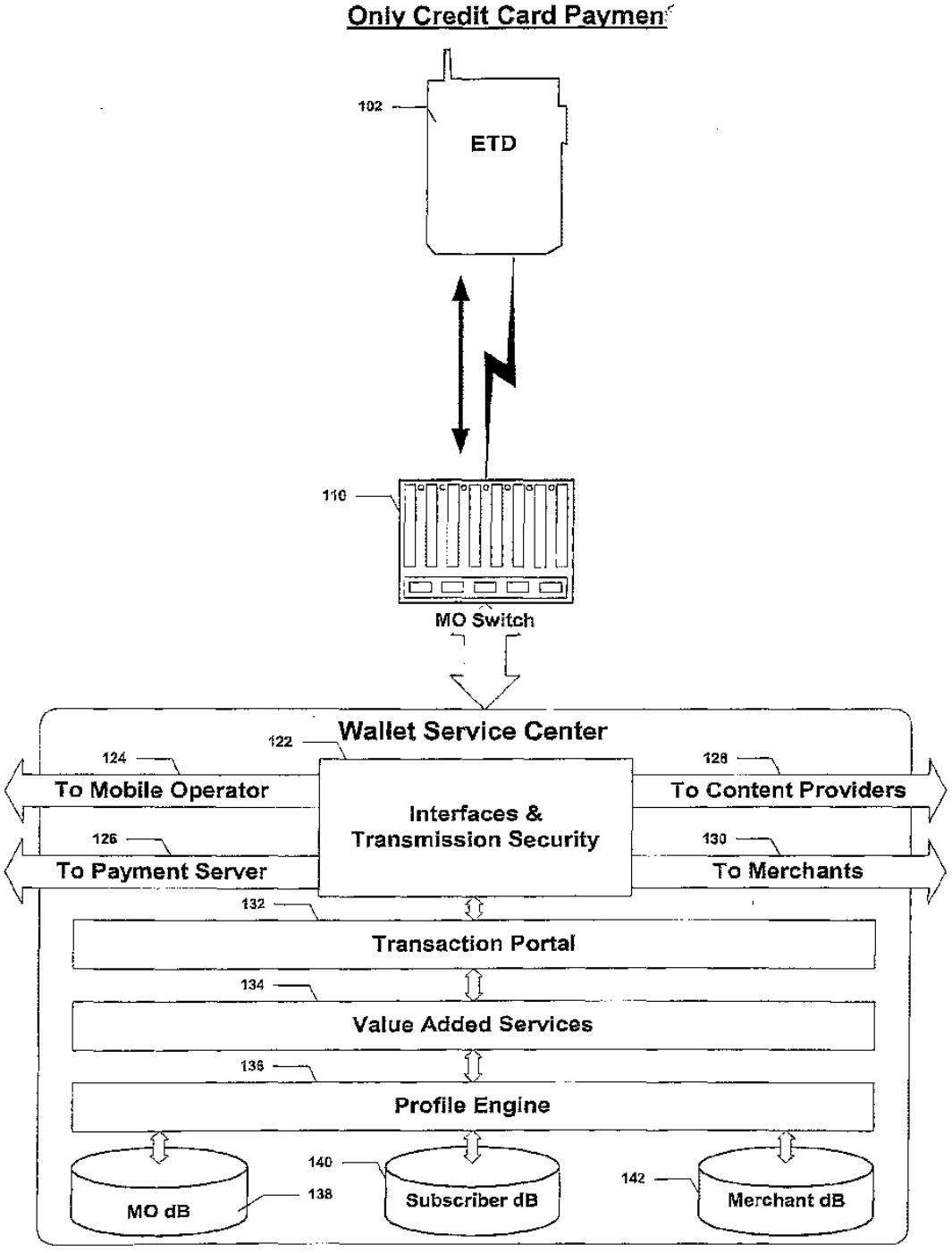

Only Credit Card Paymen
102
ETD
110
MO Switch
Wallet Service Center
122
124
To Mobile Operator
126
To Payment Server
128
To Content Providers
130
To Merchants
Interfaces &
Transmission Security
132
Transaction Portal
134
Value Added Services
136
Profile Engine
140
Subscriber dB
138
MO dB
142
Merchant dB

Figure 7

Only Credit Card Payment - Setup Sequence Flow Chart

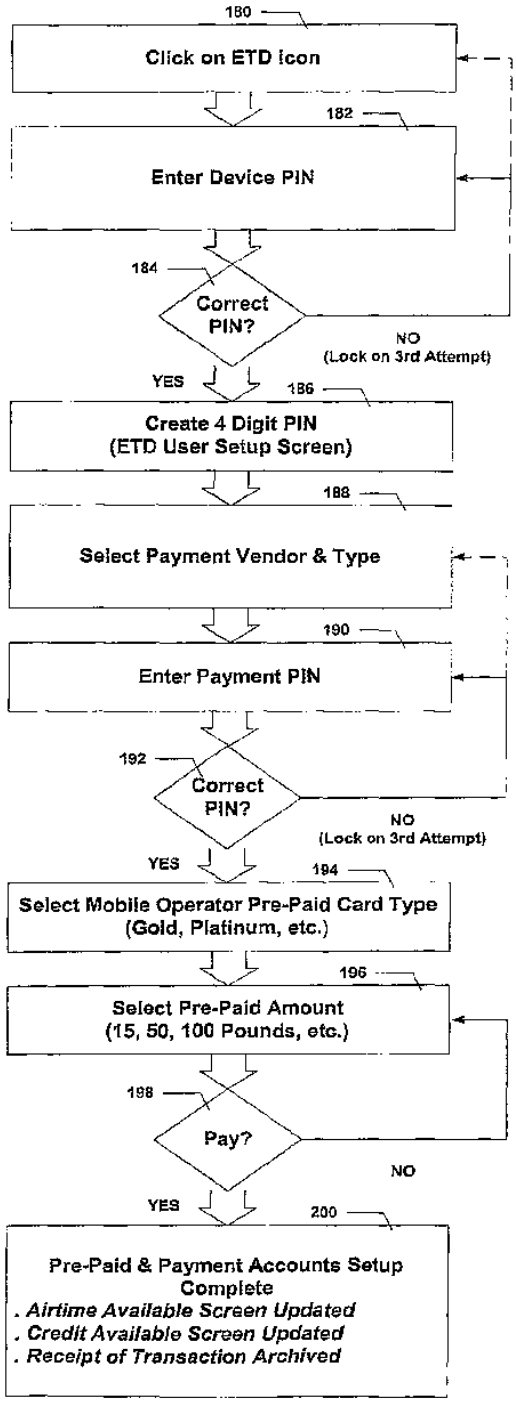


Figure 8

Only Credit Card Payment - "Top-Off" Sequence Flow Chart

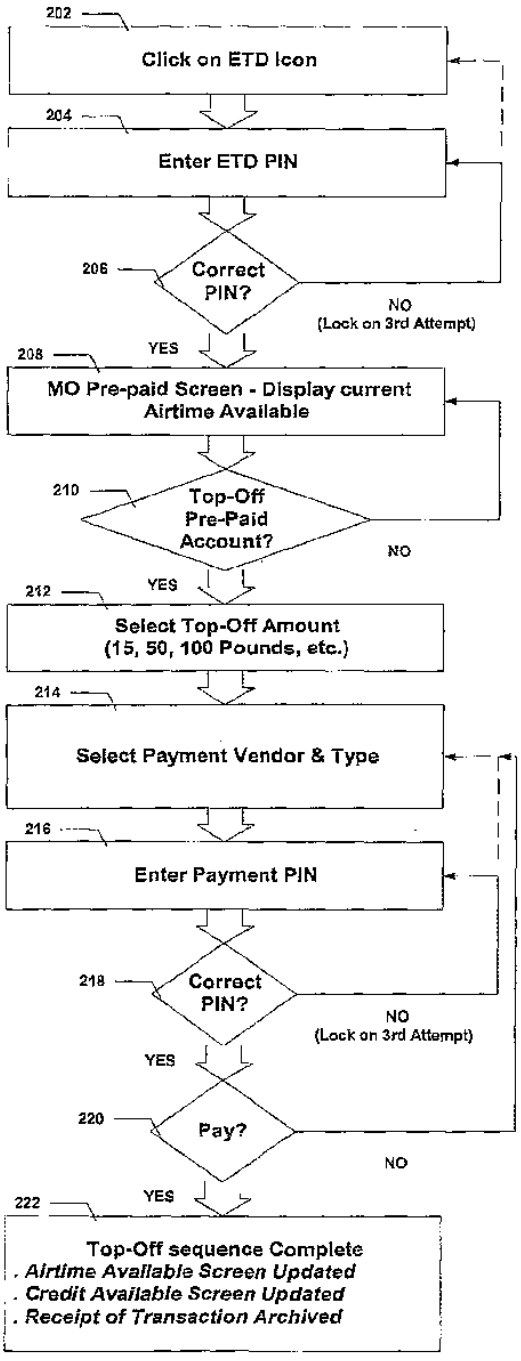


Figure 9

Only Credit Card Payment
Sample UIs

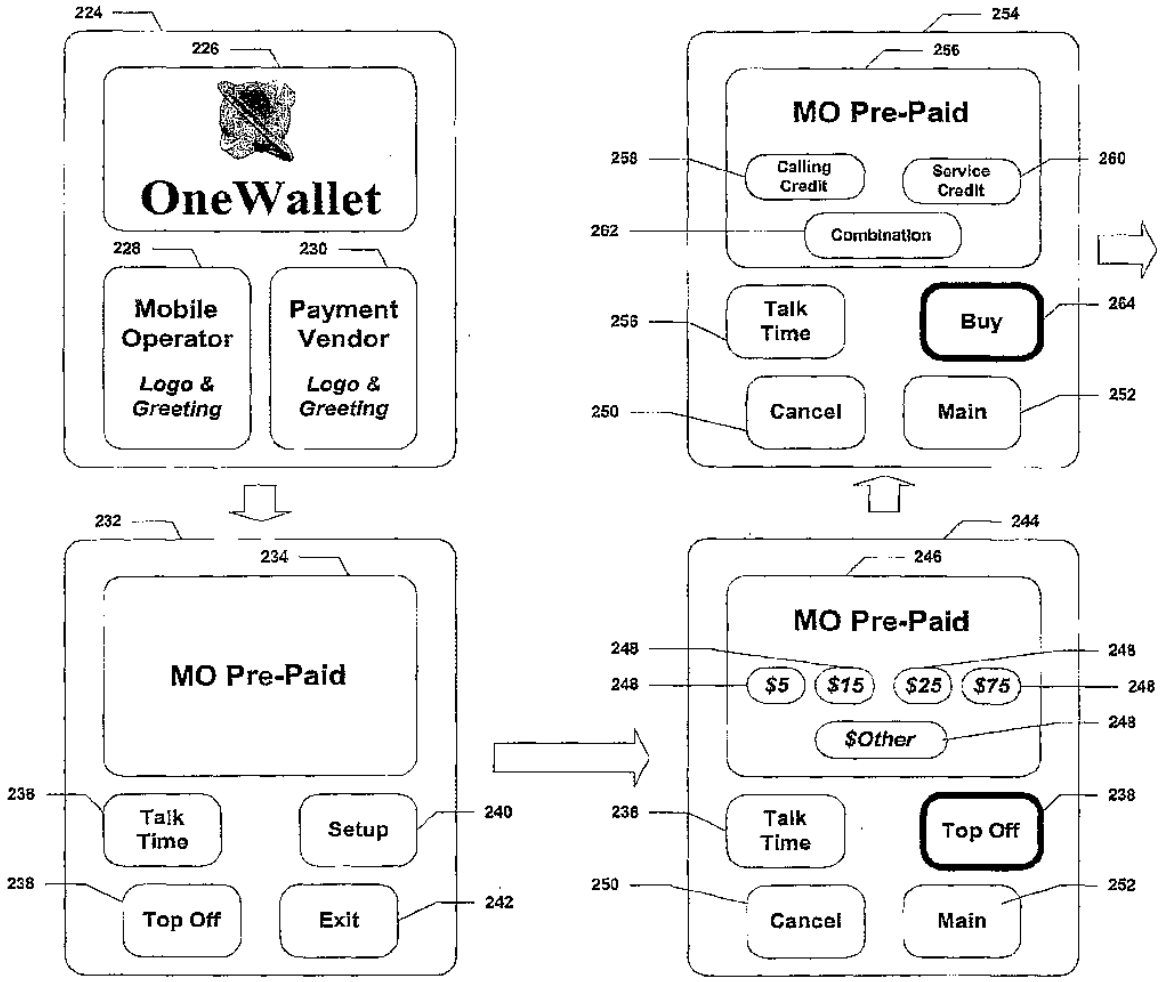


Figure 10

Only Credit Card Payment
Sample UIs

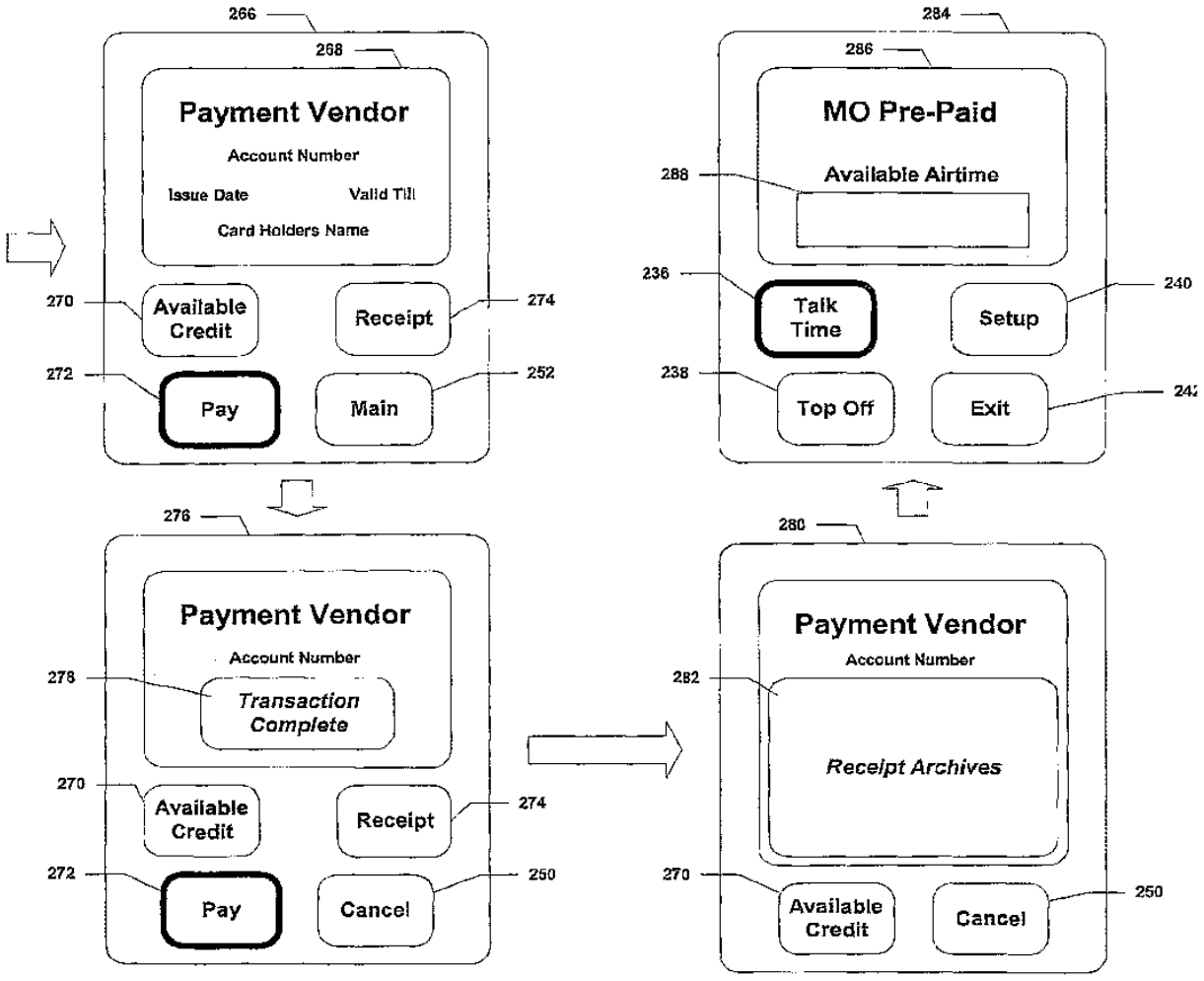


Figure 11

Merchant ETD Architecture

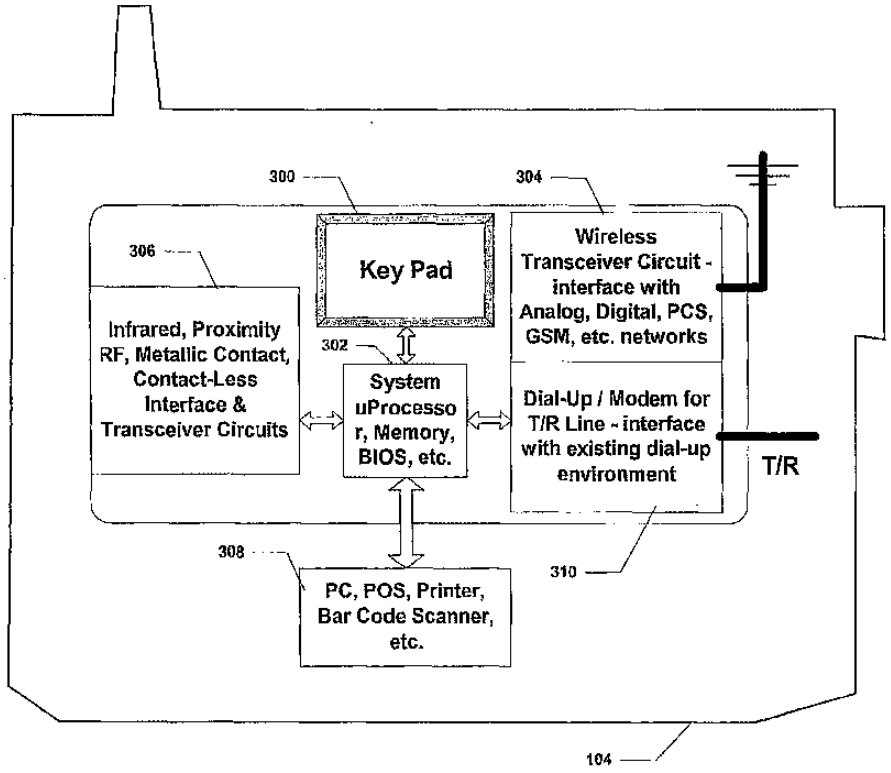


Figure 12

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 167 of 1360

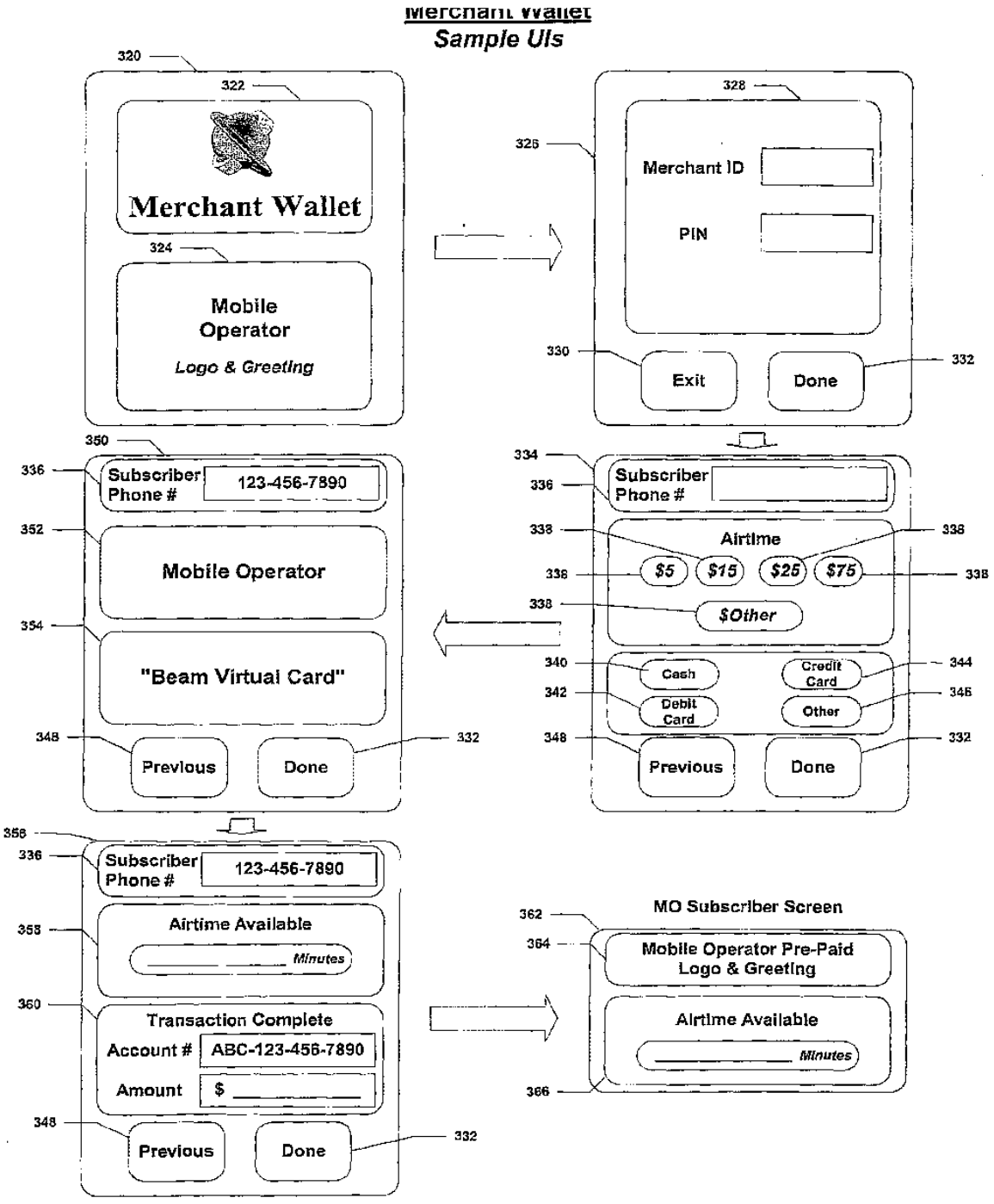

Merchant Wallet
Sample UIs
320
322
Merchant Wallet
324
Mobile Operator
Logo & Greeting
326
328
Merchant ID
PIN
330
Exit
Done
332
350
336
Subscriber Phone #
123-456-7890
352
Mobile Operator
354
"Beam Virtual Card"
348
Previous
Done
332
334
336
Subscriber Phone #
338
Airtime
$5
$15
$25
$75
$Other
340
Cash
Credit Card
342
Debit Card
Other
344
346
356
358
Airtime Available
Minutes
360
Transaction Complete
Account #
ABC-123-456-7890
Amount
$
MO Subscriber Screen
362
364
Mobile Operator Pre-Paid Logo & Greeting
Airtime Available
Minutes
366

Figure 13

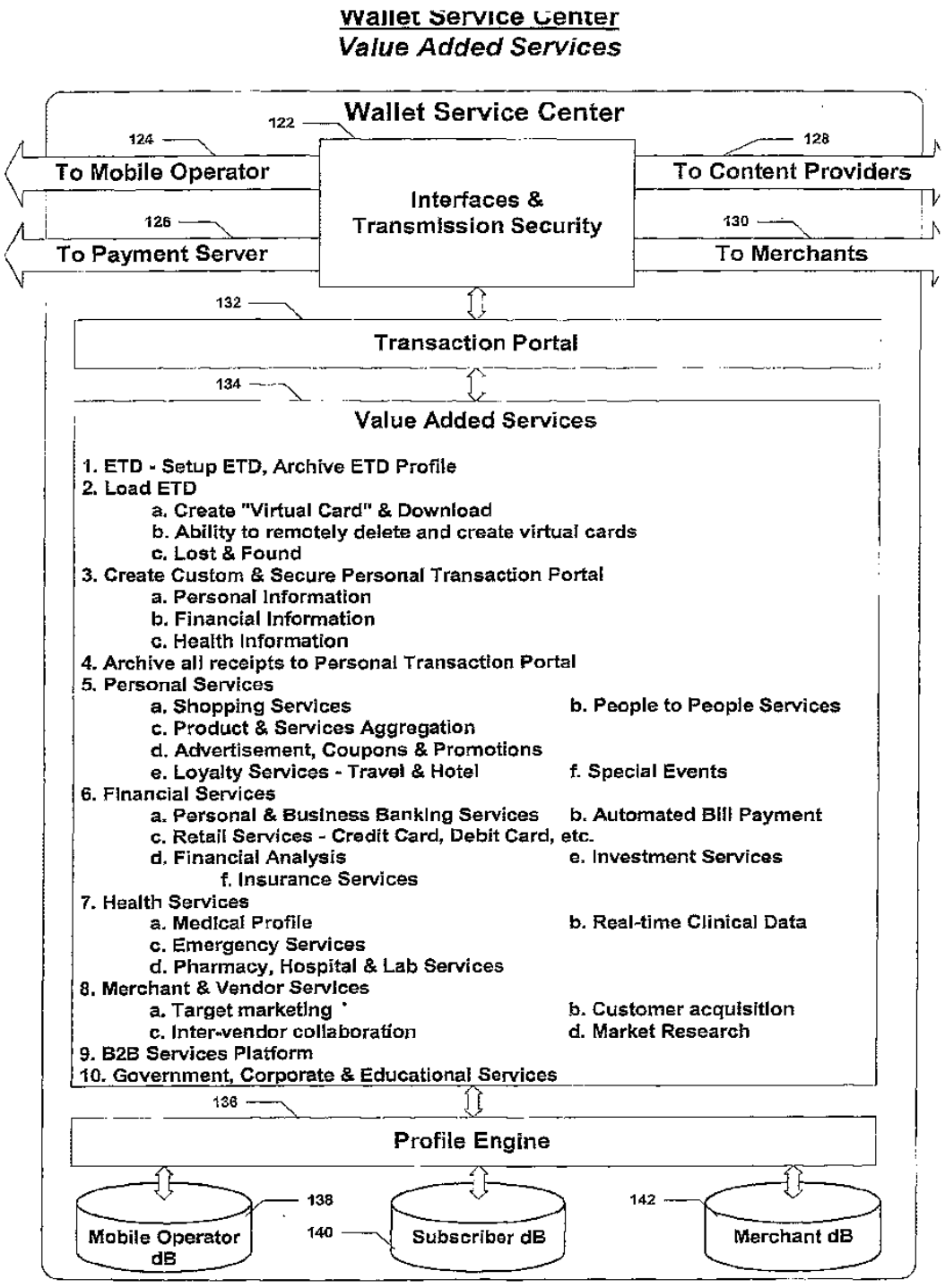
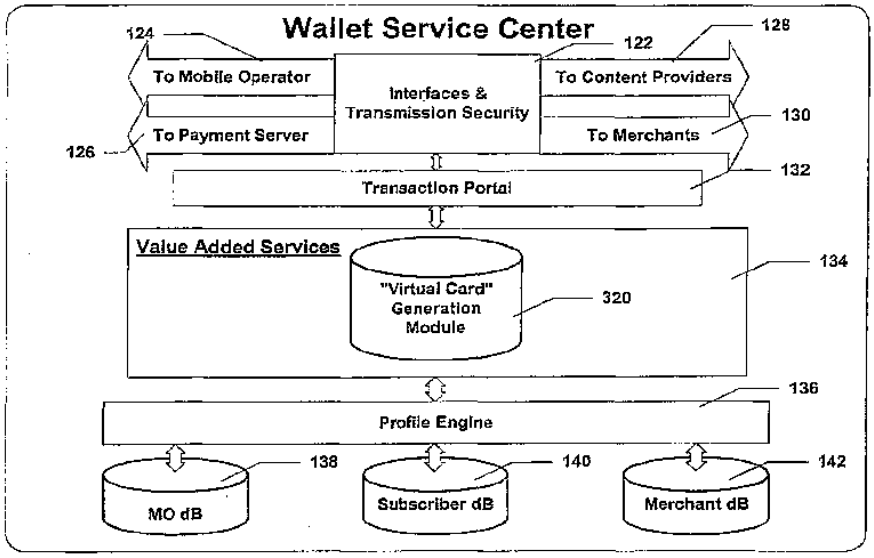
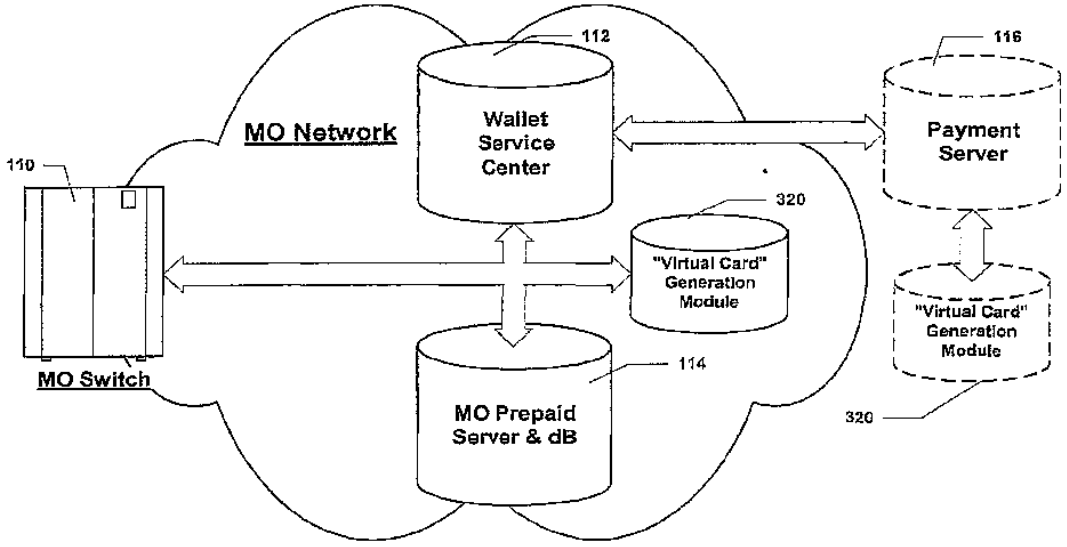

Wallet Service Center
Value Added Services
Wallet Service Center
122
124
128
To Mobile Operator
Interfaces &
Transmission Security
To Content Providers
126
130
To Payment Server
To Merchants
132
Transaction Portal
134
Value Added Services
1. ETD - Setup ETD, Archive ETD Profile
2. Load ETD
a. Create "Virtual Card" & Download
b. Ability to remotely delete and create virtual cards
c. Lost & Found
3. Create Custom & Secure Personal Transaction Portal
a. Personal Information
b. Financial Information
c. Health Information
4. Archive all receipts to Personal Transaction Portal
5. Personal Services
a. Shopping Services
b. People to People Services
c. Product & Services Aggregation
d. Advertisement, Coupons & Promotions
e. Loyalty Services - Travel & Hotel
f. Special Events
6. Financial Services
a. Personal & Business Banking Services
b. Automated Bill Payment
c. Retail Services - Credit Card, Debit Card, etc.
d. Financial Analysis
e. Investment Services
f. Insurance Services
7. Health Services
a. Medical Profile
b. Real-time Clinical Data
c. Emergency Services
d. Pharmacy, Hospital & Lab Services
8. Merchant & Vendor Services
a. Target marketing
b. Customer acquisition
c. Inter-vendor collaboration
d. Market Research
9. B2B Services Platform
10. Government, Corporate & Educational Services
136
Profile Engine
138
140
142
Mobile Operator dB
Subscriber dB
Merchant dB

Figure 14

"Virtual Card" Generation & Download



A



B

Figure 15

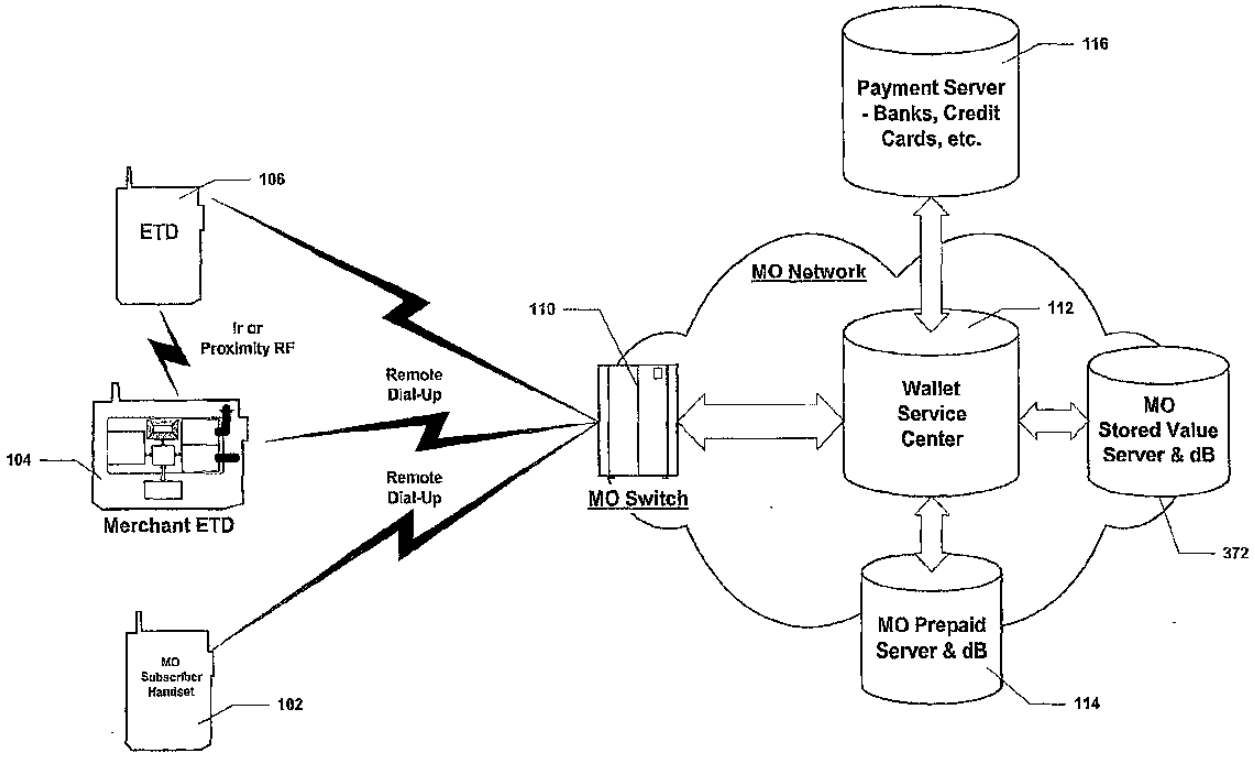


Figure 16

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 171 of 1360

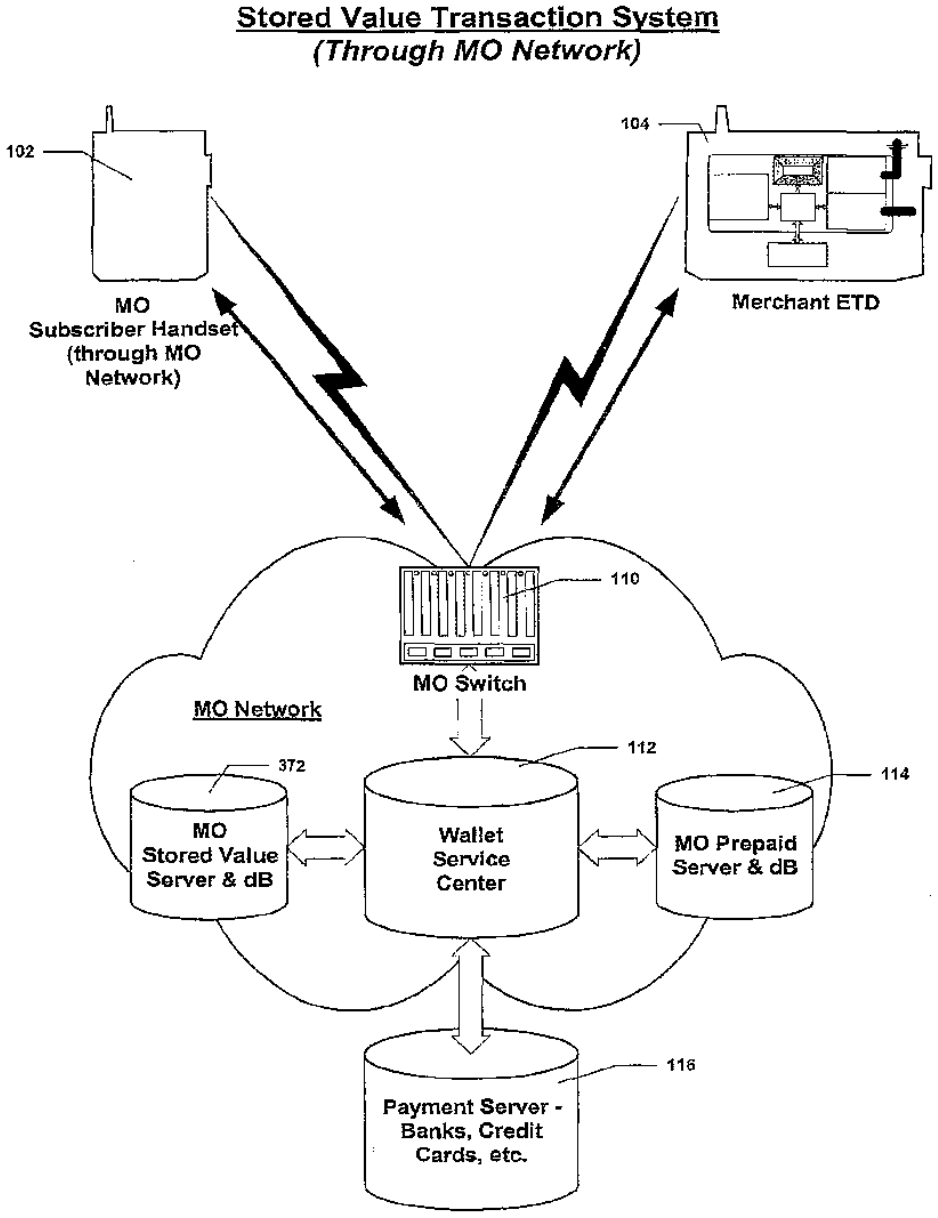

Stored Value Transaction System
(Through MO Network)
102
MO
Subscriber Handset
(through MO
Network)
104
Merchant ETD
110
MO Switch
MO Network
112
372
114
MO
Stored Value
Server & dB
Wallet
Service
Center
MO Prepaid
Server & dB
116
Payment Server -
Banks, Credit
Cards, etc.

Figure 17

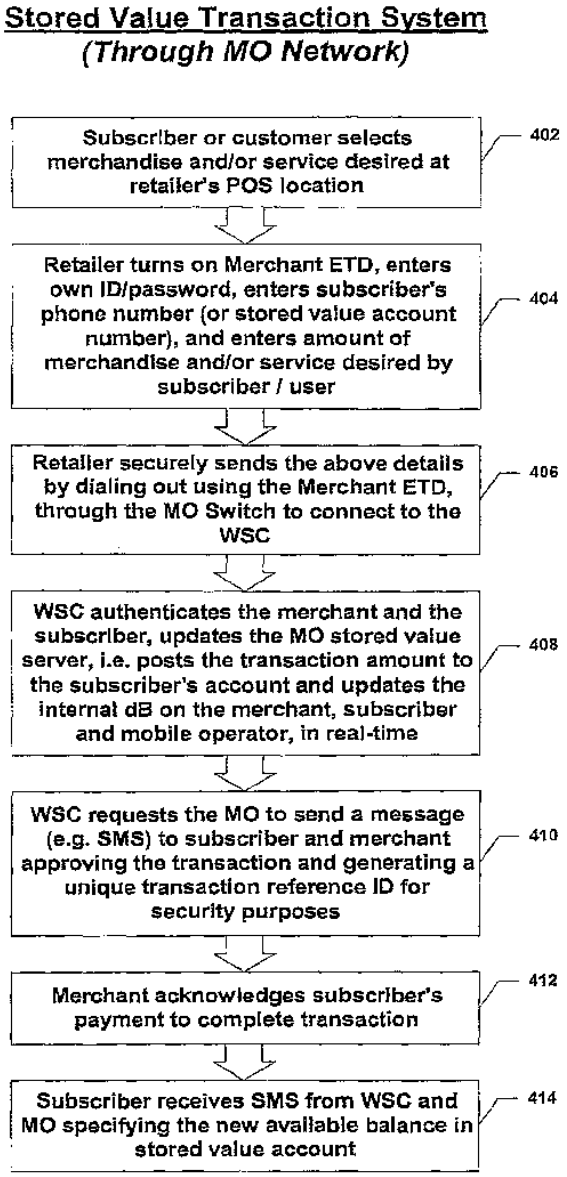


Figure 18

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 173 of 1360

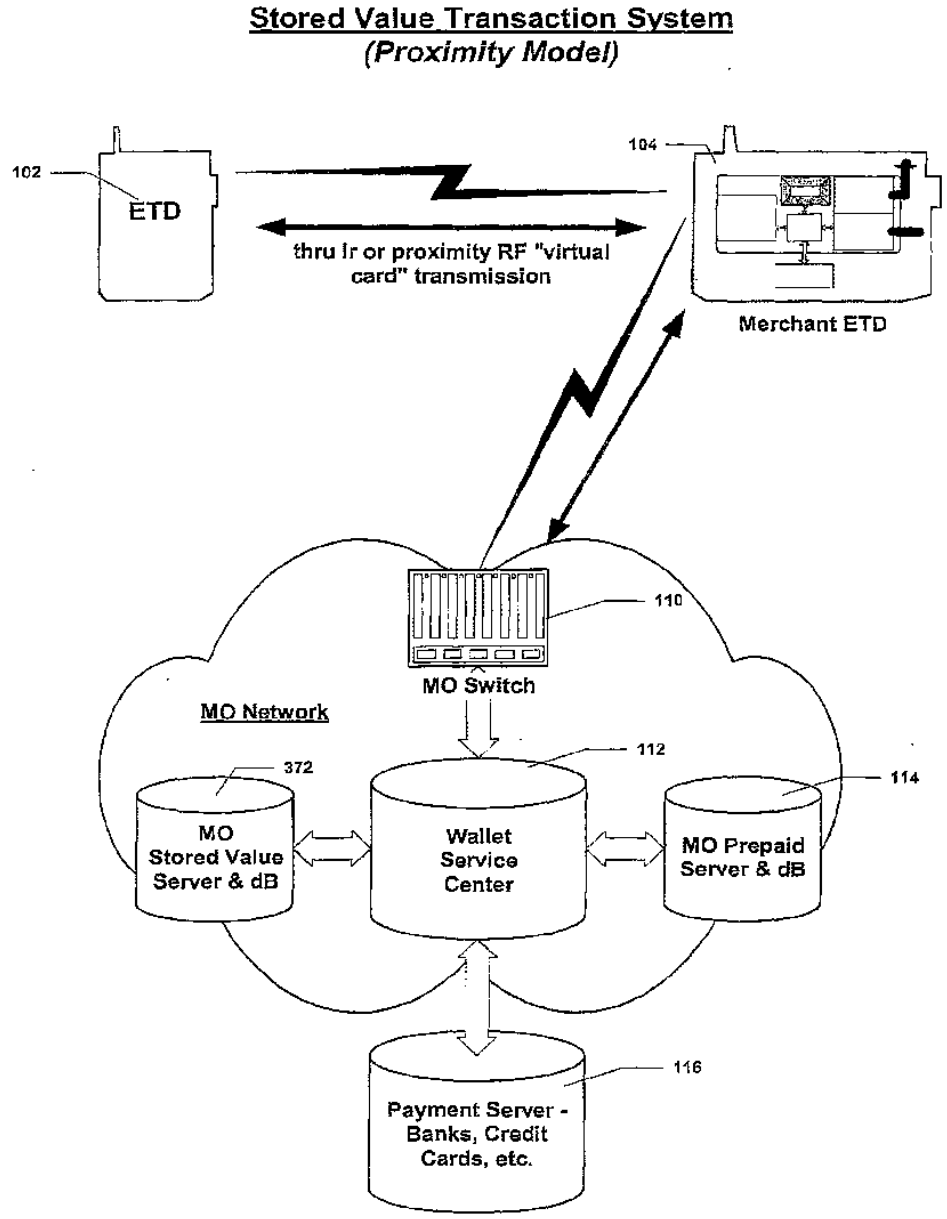

Stored Value Transaction System
(Proximity Model)
102
ETD
104
thru Ir or proximity RF "virtual card" transmission
Merchant ETD
110
MO Switch
MO Network
112
372
114
MO Stored Value Server & dB
Wallet Service Center
MO Prepaid Server & dB
116
Payment Server - Banks, Credit Cards, etc.

Figure 19

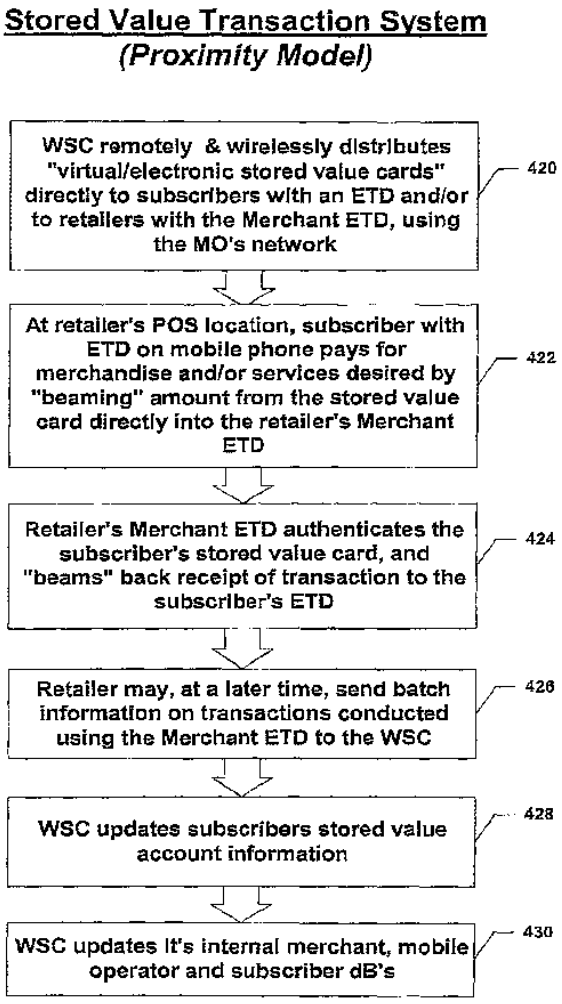

Stored Value Transaction System
(Proximity Model)
WSC remotely & wirelessly distributes "virtual/electronic stored value cards" directly to subscribers with an ETD and/or to retailers with the Merchant ETD, using the MO's network
420
At retailer's POS location, subscriber with ETD on mobile phone pays for merchandise and/or services desired by "beaming" amount from the stored value card directly into the retailer's Merchant ETD
422
Retailer's Merchant ETD authenticates the subscriber's stored value card, and "beams" back receipt of transaction to the subscriber's ETD
424
Retailer may, at a later time, send batch information on transactions conducted using the Merchant ETD to the WSC
426
WSC updates subscribers stored value account information
428
WSC updates it's internal merchant, mobile operator and subscriber dB's
430

Figure 20

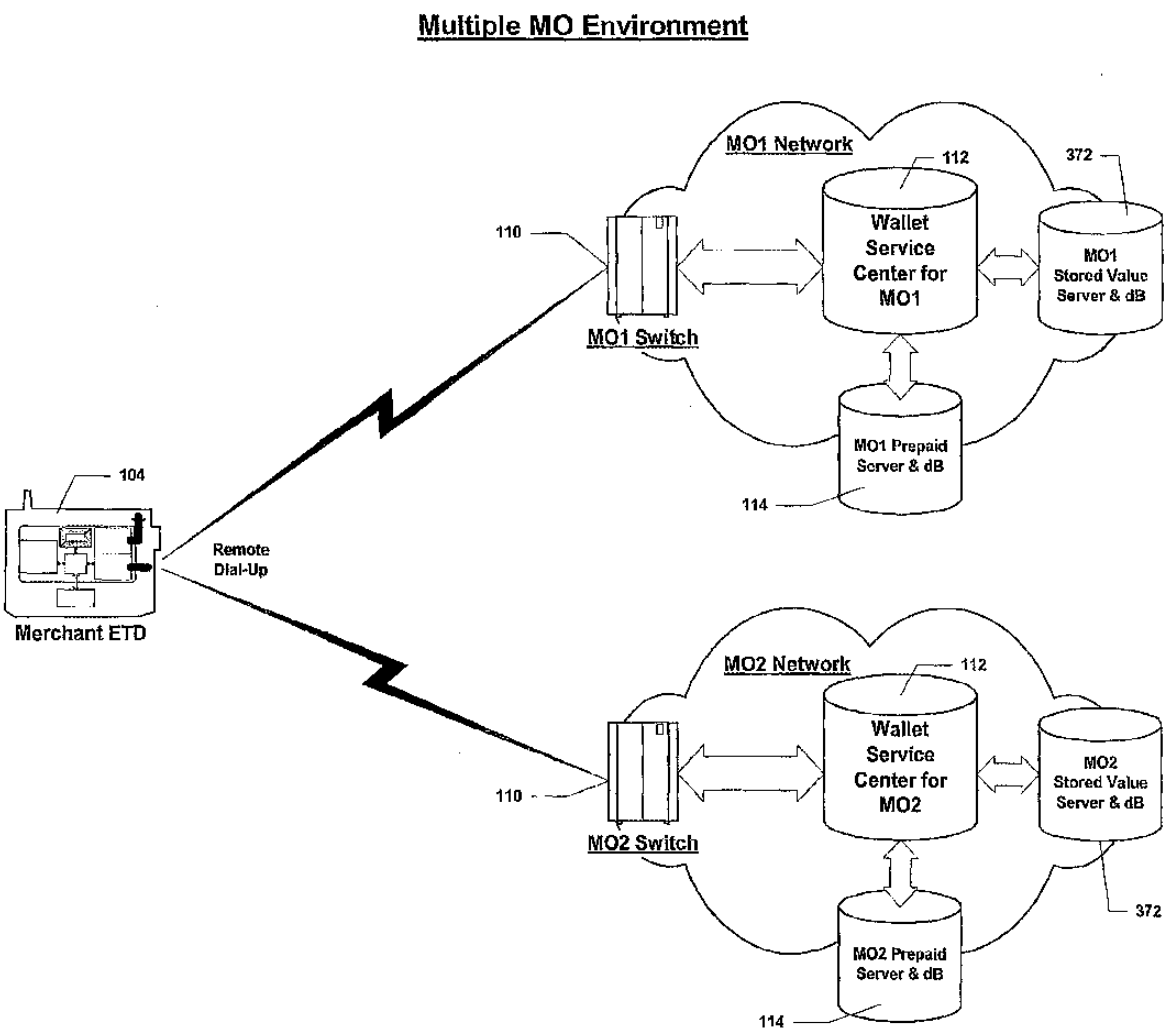

Multiple MO Environment
MO1 Network
112
372
110
Wallet Service Center for MO1
MO1 Stored Value Server & dB
MO1 Switch
MO1 Prepaid Server & dB
114
104
Remote Dial-Up
Merchant ETD
MO2 Network
112
Wallet Service Center for MO2
MO2 Stored Value Server & dB
110
MO2 Switch
372
MO2 Prepaid Server & dB
114

Figure 21

Multiple MO Environment
Sample UIs

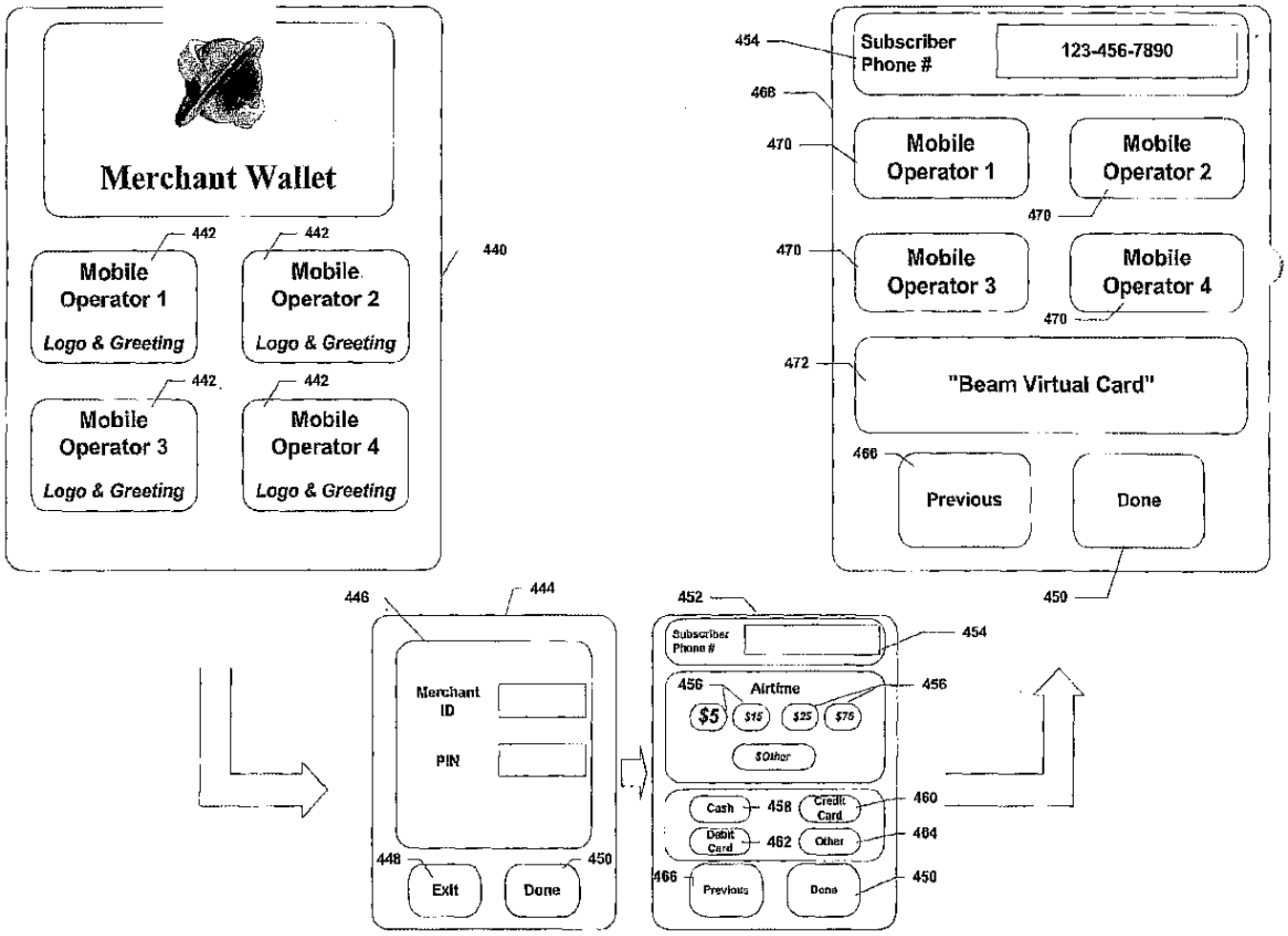


Figure 22

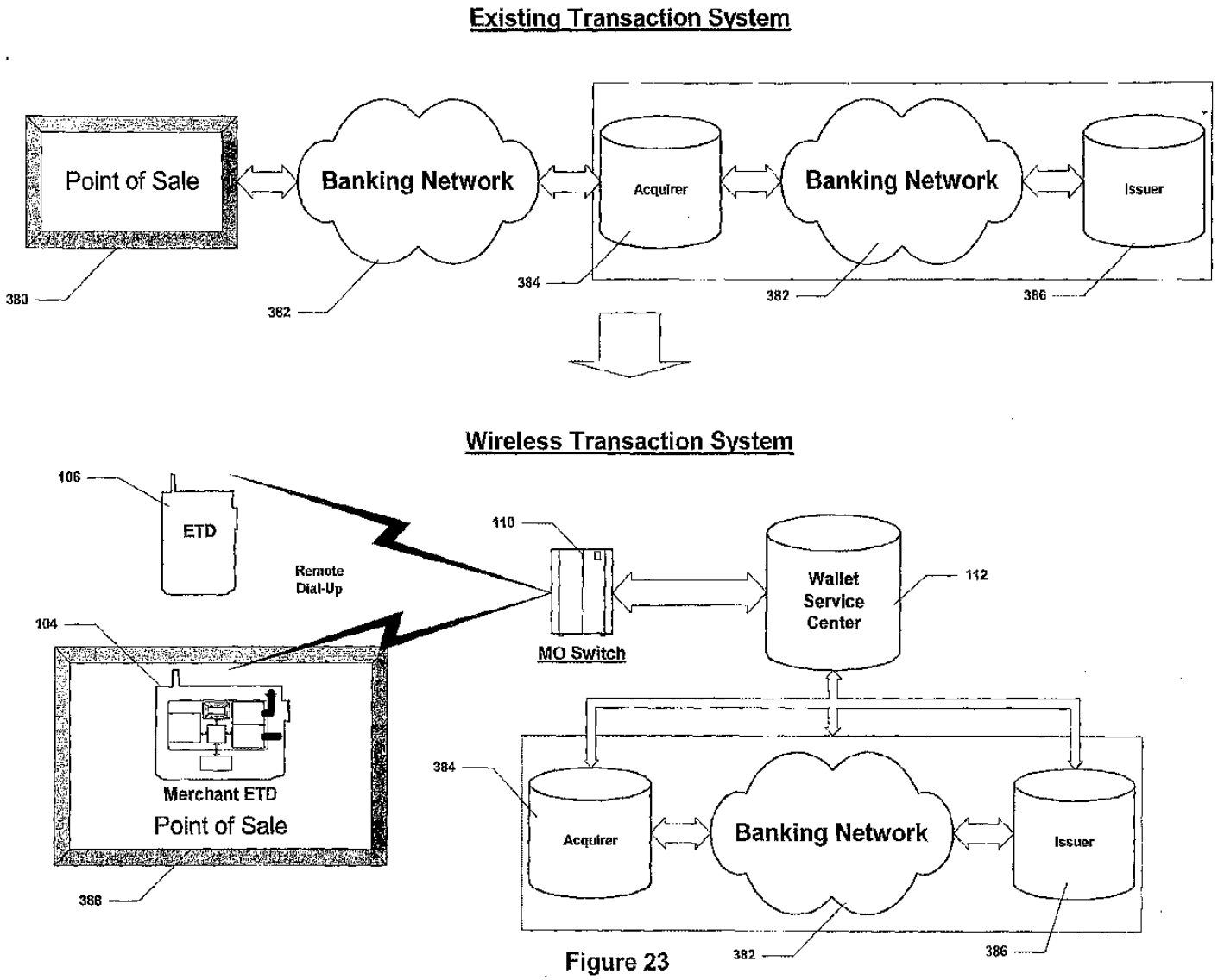

Existing Transaction System
Point of Sale
Banking Network
Acquirer
Banking Network
Issuer
380
382
384
382
386
Wireless Transaction System
106
ETD
Remote
Dial-Up
110
MO Switch
Wallet
Service
Center
112
104
Merchant ETD
Point of Sale
388
384
Acquirer
Banking Network
Issuer
382
386

Figure 23

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/23899

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G 06 F 17/60
US CL : 705/65

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/65, 1, 53

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)

EAST, search terms: pre-paid, virtual card

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ---- Y	US 5,828,740 A (KHUC et al.) 27 October 1998, col.1 lines 11-65, col. 2, lines 25-64, col. 3, lines 1-27, col. 4, lines 8-24.	1 and 5 ---------- 2-4 and 6-17
Y	US 6,105,008 A (DAVIS et al.) 15 August 2000, col. 7, lines 24-64 and col. 8, lines 11-32.	2-4 and 8-17
Y	US 6,185,545 B1 (RESNICK et al.) 6 February 2001, FIG. 2	6 and 7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 24 SEPTEMBER 2001	Date of mailing of the international search report 16 NOV 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Harvad HYUNG S. SOUGH Telephone No. (703) 308-0505

Form PCT/ISA/210 (second sheet) (July 1998) ★

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/010393 A1

(51) International Patent Classification[7]: G07F 19/00, H04M 17/00

(21) International Application Number: PCT/IL2002/000601

(22) International Filing Date: 21 July 2002 (21.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (*for all designated States except US*): **PARTNER COMMUNICATIONS COMPANY LTD.** [IL/IL]; 8 Ha'amal St., Afek Industrial Park, 48103 Rosh Ha'ayin (IL).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): **FELDMAN, Avi** [IL/IL]; 8 Ha'amal St., Afek Industrial Park, 48103 Rosh Ha'ayin (IL).

(74) Agent: **CALDERON, Hana**; Jacob & Hana Calderon, Advocates, Crystal Bldg., 12 Hilazon St., 52522 Ramat Gan (IL).

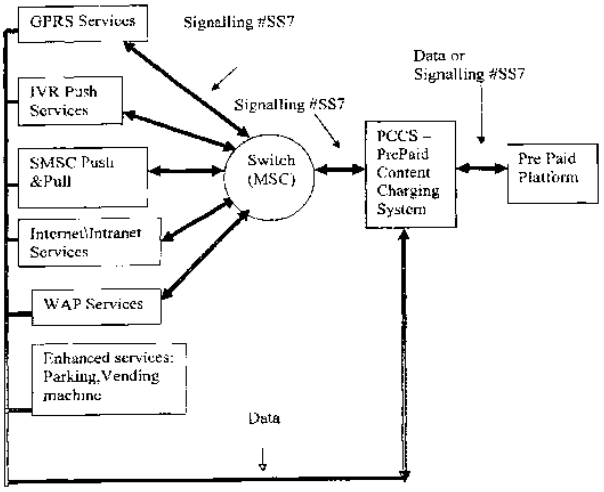
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) **Title:** PREPAID CHARGING SYSTEM AND METHOD



(57) **Abstract:** A complementary system for charging Prepaid subscribers implemented in a PLMN, PSTN or DATA communication network with a plurality of Service platforms using different #SS7 and Data communication protocols and a Prepaid platform with real time charging means that communicates through a limited number of communication protocols. The PCCS monitors the signaling and Data in the network and initiates a balance request or a charge request to the Prepaid platform when a balance or charge request is received by the PCCS following a session request from a Prepaid subscriber or the opening of a session by a push platform in the case of a push service. The prepaid platform routs an account status response or "adequate balance" or a "balance inadequate" response with or without an account status response to the PCCS which then issues a "supply service" or a "do not supply service" response to the Service Platform.

WO 2004/010393 A1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 180 of 1360

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 181 of 1360

PREPAID CHARGING SYSTEM AND METHOD

Background of the Invention:
The so called Pre Paid service was developed with a view to supply a limited range of voice telephony services to users with a tight budget or users whose budget is controlled by others such as children under age, employees using a business telephone, prisoners etc..

According to this prevailing concept of the Prepaid Service, content services such as Data services, SMS Services, Vending machine services,GPRS services, Internet services,WAP services, IVR Enhanced Services etc. are considered out of scope. Consequently methods of charging have been developed for the voice telephony market only, the various content services remaining unsupported or not fully supported by the PrePaid platforms for the reason that these platforms are only able to monitor a limited range of # SS7 protocols and most of them are unable to monitor Data.

This attitude of the prior art to the Pre Paid service resulted in a much larger variety of services being available for the Post Paid subscriber than those enjoyed by the Pre Paid subscriber, the reason being that the operator is unable to charge the Pre Paid subscribers for those services. Obviously the present state of the art leaves a large amount of consumer demand unattended. The more so as children and teenagers, naturally belonging to the Pre Paid customer group, tend to make an extensive use of innovative and sophisticated data services.

It is a main drawback of the prior art that Pre Paid vendor systems are designed to support their own Pre Paid services only, while any other platform services are left without precharging means. Thus an Operator implementing a Pre Paid platform will not be able to supply his full variety of services to the PrePaid subscribers.

The PrePaid market has therefore created a demand for a PrePaid system with a payment method that is not limited to a class of services. It is another demand of the market that a general operator with different platforms and services be capable of supplying the same advanced voice and data services for his PrePaid subscribers and Post Paid subscribers.

It is therefore desirable to provide a PrePaid Content Charging System that enables any PrePaid Operator, regardless of the Pre Paid Platform implemented by the said Pre Paid Operator, the PrePaid services to be supplied or the kind of #SS7 or Data protocols or technology operated in the said network, to charge and support the same Content services, including Data services such as: SMS, WAP, Internet (Push and Pull forms), GRPS and Enhanced Voice Services, that are supported for the post paid subscribers.

Further, it is desirable to provide a real time charging mechanism for a Content Service such that the PrePaid subscriber is charged in the course of ordering or immediately after getting the desired service, according to any marketing definitions.

Summary of the Invention

The invention concerns a charging system that is applicable in cellular telephony systems or wired systems (PSTN) or any other communication network systems using PLMN/PSTN/DATA technologies and that enables real time charging of PrePaid subscribers for various Data and Voice services including Content services and Advanced Voice services employing a variety of Data and # SS7 protocols, regardless of the type of the PrePaid platform, network platform or service platforms applied in the said communication sytem.

The inventive PrePaid Content Charging System (hereafter - PCCS) is designed to function as a charging request gateway or as a service junction which includes the PrePaid subscribers Database. The PCCS monitors the different kinds of # SS7 signalling or Data in the network and it enables real time charging of the Pre Paid subscriber by routing a balance request or a charge request to the PrePaid platform via #SS7 signaling that is compatible with the said PrePaid platform when a service request or a charging request has been routed to the PCCS by a service platform via any of the said different #SS7 or Data signalling as a result of a session initiated by a PrePaid subscriber. All PrePaid subscribers related service requests are balance analyzed and charged accordingly by the PrePaid Platform that sends a response of "balance adequate" or "balance inadequate" or account status to the PCCS whereupon the PCCS responds accordingly by putting out a "supply service" or "deny service" response to the relevant service platform, via #SS7 or Data signalling appropriate for that platform.

In the event of a "push" service, the balance request or charge request is routed to the PCCs by a relevant "push" platform when the time that has been set for the service by the prepaid user arrives. In case that there is a finding of "balance inadequate", the PCCS repeats the "balance request" or "charge request" a preset number of times until a balance adequate response is received.

In accordance with another aspect of the invention, the PCCS may also comprise means for managing and supplying one or more PrePaid related services such as Vending machine, Parking machine, etc.

The inventive PCCS enables charging a PrePaid subscriber for any services in the network such as Push and Pull SMS services, Internet, Intranet,WAP, push IVR services, enhanced services such as Parking,Vending machines etc.

Brief Description of the Drawings

Fig. 1 is a schematic representation of the PrePaid platform connections in an existing cellular network.
Fig. 2 is a schematic representation of the charging process in an existing network
Fig. 3 is a schematic representation of the PCCS network connections
Fig. 4 is a block diagram of a Network in which a PCCS system is implemented
Fig. 5 is a representation of the charging call flow for push or pull services in a network with a PCCS system
Fig. 6 is a schematic representation of the basic architecture of a PCCS system

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 183 of 1360

Detailed Description of the Invention in Respect of a Preferred Embodiment

Cellular telephony services providers cater to Post Paid as well as Pre Paid users. While the Post Paid user gets the desired service on the basis of future charging, the Pre Paid user may only use the service on the condition that his balance has been checked and found sufficient for the requested operation. It is therefore necessary to monitor the balance of the PrePaid user, to consider it before supplying the service, to make the decision of supplying or denying the service in real time, to charge the Customer for the service instantly and to continue monitoring the service during use such that it may be terminated when the customer reaches balance inadequate.

Current charging methods in the PrePaid World are of two kinds. The Real Time Charging method involves a PrePaid Data Base and charges Voice calls according to the PrePaid Calling Numbers, some PrePaid platforms also supporting Mobile Originated SMS and Terminated Called Numbers, whereas according to the Calling Detail Record (CDR) based Charging method – only PrePaid CDRs are analyzed and the PrePaid subscriber balance is charged accordingly.

A schematic representation of the PrePaid platform connections in an existing cellular network is shown in Fig. 1. As seen in Fig. 1, when a service is required by a Prepaid user, the Prepaid user's mobile handset initiates a request to a Mobile Switching Center (MSC) using # SS7 protocol which then sends a request to the Prepaid platform also via # SS7 protocol, the Prepaid platform response indicating via # SS7 protocol whether the subscriber's account allows him to receive the specific service. Where the response is positive, the Mobile Switching Center connects the subscriber to the requested service. In the network of Fig. 1, the PrePaid platform is only capable of performing the above described authorizing procedure in respect of Short Message Service Center (SMSC) and Mobile Originated (MO) services such as Voice Calls and Mobile Originated SMS while many other services such as SMS Push services, IVR Push Services, WAP, GPRS as well as Internet/intranet services remain out of scope for the PrePaid user for the reason that the PrePaid platform is incapable of monitoring the types of #SS7 or Data protocols employed for these services. Many PrePaid platforms fail to support even mobile originated SMS services, while other PrePaid platforms may be suited to support different types of services such as IVR only, WAP only etc., all according to PrePaid platform design. While in Fig. 1 a cellular network with a Mobile Switching Center is described, it will be understood that other Switching Center means may be used for different communication networks as known.

It will be understood that the considerably limited scope of current Prepaid Charging systems results in a large number of services being blocked for PrePaid subscribers in systems of the known type, the kind of services blocked depending on the kinds of #SS7 protocols compatible with the said PrePaid Charging system as a result of Designer choice.

While CDR based charging may be applied for services that are not supported by the PrePaid platform, this charging method has the drawback of not enabling any real time charging. This means that the operator may fail to charge the service, resulting in loss of valuable income.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 184 of 1360

The charging of Content Services in existing Prepaid Charging platforms is related to the capabilities of the PrePaid platform vendor and not to the services to be charged. In other words, the PrePaid platform is only capable of charging for a limited number of services according to its design while other platform services cannot be supplied to PrePaid users due to lack of charging means.

Fig. 2 shows the charging flow of a voice session in an existing network comprising a PrePaid Platform and a Switching Center such as the network of Fig. 1, the said charging flow comprising the following steps:

Step 1: The Prepaid subscriber initiates the session by calling a destination and/or requesting a service

Step 2: The Switching Center initiates a balance request or a charging request to the PrePaid platform

Step 3: The PrePaid platform responds according to the subscriber balance: in case that the balance is adequate, a "connect" response is routed to the Switching Center, otherwise the response routed to the Switching Center is "disconnect".

Step 4: in the event of an adequate balance the call will be routed by the Switching Center to the Called Party and it will be charged accordingly by the Prepaid platform .

In the event of an inadequate balance the call will not be routed. In some systems an announcement of "balance too low" is displayed or played to the PrePaid subscriber.

It will be understood that in some cases the PrePaid subscriber may also be the Called party, such as in the case where a third party requests a service that involves a call to the Prepaid subscriber.

In the case of a Service session, where the balance is adequate the call will be routed to the requested Service platform. However this operation is only feasible where the PrePaid platform is capable of using the type of $SS7 or Data protocol of the respective Service platform.

It is a main drawback of the prior art that due to the existing PrePaid platforms being incompatible with the protocols implemented in most services and technologies available on cellular and PSTN networks, the above described charging flow can only be realized with respect to a very limited number of services .

While the drawings of Figs. 1 and 2 refer to a cellular network, it will be understood that PrePaid subscribers in PSTN (wired) networks are subject to similar drawbacks and therefore it is also desirable to enable the charging of various additional services for the PrePaid PSTN subscriber.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 185 of 1360

The PrePaid market charging requirements demand that Content Services be charged regardless of the PrePaid platform vendor and PrePaid platform version. It is a further demand of the market that Content services be charged, regardless of the type of service or service platform (WAP, IVR, Internet or other) and regardless of the type of #SS7 or Data protocol used by a service or service platform and that Pre Paid subscribers be charged regardless of service technology, whether GSM, GPRS, CDMA, TDMA or other. The Pre Paid market demands a very fast introducing and charging of newly launched Content Services to the Pre Paid subscriber.

In accordance with the present invention a Pre Paid Content Charging System (PCCS) is proposed that enables the implementing of a real time method for the charging of PrePaid subscribers in respect of a large variety of services, platforms and technologies, including Content services and advanced Voice services.

The invention will be described hereinbelow by way of example in respect of a preferred embodiment. It will be understood however that many other variations and modifications of the invention may be made that still remain within the scope of the description and the claims.

In accordance with the invention the PCCS is implemented in a telephony network with a Prepaid Platform that may be a PSTN (Public Switching Telephony Network) or PLMN (Public Land mobile Network) or any other communication network type, and it monitors the signalling or the Data in the said network. The PCCS is provided with means for monitoring the network signalling according to a variety of # SS7 protocols such as Wireless Application Protocol (WAP), IN Application Protocol (INAP), or ISDN User Part Protocol (ISUP) or any other #SS7 protools applied in the network. The PCCS is further provided with means for monitoring the network Data using a variety of Data protocols such as HTTP/TCP/IP, HTTP/UCP, HTTP/MAP or any other Data Protocol applied in the network. The PCCS further has means for communicating with the PrePaid platform.

Signalling or Data in the Network that constitutes a PrePaid call or message is analyzed according to a PrePaid customer database such that all PrePaid subscribers related service requests are balance analyzed and charged accordingly.

The PCCS may be implemented as a charging request gateway or it may be implemented as a service junction that comprises the PrePaid subscribers Database.

Within the network the PCCS is connected to a BSCS (Business Support and Control System), BGW (Billing Gateway) and SOG (Service Order Gateway) or any similar subscriber management means in order to allow management of the PrePaid subscribers.

The PCCS enables the charging of a PrePaid subscriber for various services in the network supplied by platforms of various types such as Push and Pull SMS, Internet, Intranet,WAP, push IVR services, enhanced services such as Parking,Vending machines etc.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 186 of 1360

Fig. 3 is a schematic representation of a network in which the PCCS of the invention is applied, showing the PCCS connections in the network. As shown in Fig. 3, the PCCS connections may comprise a DWH (Data Warehouse) means for storing and processing subscriber CDRs, a BGW (Billing Gateway) means for processing raw CDRs from network platforms, a SOG (Service Order Gateway) means for storing subscriber characteristics, a BSCS (Business Support and Control System) means for storing a subscriber database, and a CSR (Customer Service Representative) such that managing and controlling customer service and data is facilitated. It will be understood by those versed in the art that the above listed systems communicate via Data protocols. Other PCCS connections comprise a variety of services and platforms that are available in the network such as IVR, GPRS,WAP, using various #SS7 protocols and SMSC, IN and Internet Gateway means using Data protocols of different kinds. In accordance with the invention, all of the above listed services may be supplied to a PrePaid user and charged accordingly due to the inventive PCCS having means for communicating via the said #SS7 and Data protocols.

It will be understood that a Gateway shown in Fig. 3 may also be a server and that many other services may be added in the said network to be charged by the inventive PCCS whether those existing today or any services to be developed in the future.

As seen in Fig. 3, the inventive Prepaid Charging Complementary System is connected to a PrePaid platform, the said connection enabling the PCCS to send a charging request or a balance request to the said PrePaid platform and to receive a response from the PrePaid platform. As shown in Fig. 3, the Prepaid Charging Complementary System communicates with the PrePaid Platform via #SS7 or Data protocols.

It will be understood to those versed in the art that the Prepaid Platform may be implemented as a PrePaid SCP or SDP or Prepaid Switch.

In Fig. 3 some of the different protocols that may be used for communication of the Prepaid Charging Complementary System of the invention with various systems within the network are indicated such as INAP, ISUP #SS7 protocols or TCP/IP Data protocols for communication with the PrePaid subscriber management means, TCP/IP or HTTP Data protocols for communication with the Data Warehouse means, INAP or HTTP Data protocols for communicating with IN means, HTTP or UCP Data protocols for communicating with SMSC means, HTTP or TCP/IP Data protocols for communicating with IVR service means, HTTP or MAP Data protocols for communicating with WAP gateway means and #SS7 Protocols for communicating with the Switching Center means and the GPRS Gateway means.

In accordance with a further advantage of the invention, the Prepaid Charging Complementary System may be adapted for communication via other protocols in case that such protocols are developed or applied in the future in communication networks.

It is one of the advantages of the inventive PCCS that it may be implemented in a preexisting network that comprises all or a part of the systems described in refence to Fig. 3 whereby the said network acquires the ability of supplying additional voice and data services that could not be supplied to the PrePaid subscriber prior to the installation of the said Prepaid Charging Complementary System.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 187 of 1360

Fig. 4 is a general diagram of the preferred embodiment showing a network with a PCCS, a PrePaid platform, an MSC (Mobile Switching Center) and a variety of service platforms. The MSC (Mobile Switching Center) receives the calls initiated by the subscribers via the different platforms by means of #SS7 signaling. In the event that the subscriber is a PrePaid subscriber, the Mobile Switching Center communicates with the Prepaid Charging Complementary System of the invention by initiating a service request. The Prepaid Charging Complementary System routs a balance request or a charge request to the PrePaid platform and the said PrePaid platform responds by data or signaling or both that indicates the PrePaid subscriber balance or new balance after charging of the PrePaid subscriber balance.

In the preferred embodiment, service requests may also be routed from the platforms to the PCCS directly, without passing the Switching Center means. As seen in Fig. 4, the GPRS, IVR, SMSC, Internet/Intranet and WAP service platforms communicate with the PCCS both directly and indirectly, via the MSC, while service requests from some enhanced service platforms such as Parking, Vending machines etc. are only directly routed from these platforms to the PCCS. The communication protocols used for routing the service requests include #SS7 signaling such as INAP, ISUP, MAP, UCP, CAMEL PH 2/3 and Data signaling such as HTTP, TCP/IP or any other protocol that is appropriate for the relevant service platform.

Having received a response from the PrePaid platform that indicates the said PrePaid subscriber balance, the Prepaid Charging Complementary System Signals to the relevant Service platform via INAP, ISUP, MAP, UCP, or CAMEL, PH2/3 HTTP, TCP/IP or any other #SS7 or Data protocol as appropriate depending on the relevant platform protocol and indicates a balance response according to which the service is allowed or denied.

In case of balance 0 or inadequate balance or any other predefined balance value, a "balance 0" or "balance inadequate" or any similar message is sent to the PrePaid Caller from the relevant platform, indicating that the requested service is unavailable. In accordance with the invention, the balance message may be sent by way of announcement or SMS.

In accordance with the invention, where the balance is sufficient, the charging procedure is executed by the Prepaid platform via an IN session, ISUP session or Data session in compliance with the network operational characteristics.

In accordance with another aspect of the inventive PCCS system in the event of a no acknowledge message from the PrePaid platform regarding the supply of the required service to the PrePaid subscriber, the request is repeatedly resent by the PCCS to the PrePaid platform at a later point of time until a "balance adequate" message is received by the PCCS. It will be understood that this feature of the invention has the advantage of considerably increasing the number of service events that, inter alia, by enabling Push services to Prepaid subscribers whereby the profitability of the network in which the PCCS is implemented becomes much higher.

In accordance with yet another aspect of the invention a resend service threshold is defined such that above the said threshold the service resend is ceased.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 188 of 1360

It will be understood that other service platforms, using other protocols, may be implemented in a network according to the invention and the supply of services to PrePaid users by these platforms may be managed by employing the inventive PCCS.

Fig. 5 is a more detailed presentation of the flow of various Push and Pull services in the network of Fig 4, wherein Push services are delayed services supplied at a predetermined point of time or at a point of time that is chosen by the user, the said point of time being subsequent to the call requesting the service.

As shown in Fig. 5, a balance or charge request, indicated by arrow 1', may be routed directly from the Push platform to the Prepaid Charging Complementary System. The Prepaid Charging Complementary System then initiates a balance or a charge request, indicated by arrow 3, to the Prepaid Platform. The Prepaid platform responds by sending a response designated by arrow 4 to the Prepaid Charging Complementary System, wherein the said response 4 may be an account status response or an "adequate balance" or a "balance inadequate" response with or without an account status response. The Prepaid Charging Complementary System then outputs a "supply service" or "do not supply service" signal, indicated by arrow 5', that is routed directly from the Prepaid Charging Complementary System to the relevant service platform.

In the preferred embodiment, such direct routing of a balance of charge request occurs in the case of Vending machine and similar services. It will be understood however that other modes of making the invention may be designed in which other services will be charged by routing balance or charge requests via a Switching Center means while all or some of the services that in the preferred embodiment are requested via the Switching Center means may be charged such that the respective balance or charge requests are routed directly to the Prepaid Charging Complementary System.

In accordance with another aspect of the invention, in the case of services such as IVR, WEB or SMSC, when the time chosen by the PrePaid subscriber for receiving the service arrives, the relevant Push platform initiates a request that is routed to the Prepaid Charging Complementary System via the Switching Center Means. This request is indicated by arrows 1 and 2. The Prepaid Charging Complementary System then initiates a balance or a charge request, indicated by arrow 3, to the Prepaid Platform. The Prepaid platform then sends a response indicated by arrow 4 to the Prepaid Charging Complementary System, wherein the said response 4 may be an account status response or an "adequate balance" or a "balance inadequate" response with or without an account status response. The PCCS outputs a signal to the Switching Center means designated by arrow 5 or it outputs a signal directly to the Push Platform, designated 5', the said signal being a "supply service" signal or a "do not supply service" signal according to the input 4 from the Prepaid Platform.

It will be understood that in the case of Push and Pull services that are routed through the Switching Center means, the services may be defined in a database that is comprised in the said Switching Center Means or in an external data base or they may be defined in the PCCS for the purpose of managing the said Push and Pull services.

In the case of Push and Pull services that are directly routed to the Prepaid Charging Complementary System, the said Push and Pull services are managed by an external data base or a Data base in the PCCS.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 189 of 1360

While the drawings of Figs. 4-5 refer to a cellular network, it will be understood that the inventive PCCS may also be applied in a PSTN (wired) network to enable the charging of various additional services for the PrePaid PSTN subscriber.

Fig. 6 shows the basic architecture of the PCCS of the invention. The PCCS comprises three structural levels, a Service Level, an Application level and an Interface level. The Service level comprises means for connecting to the Prepaid platform and communicating with the said Prepaid platform through an interface using #SS7 and Data protocols.
In accordance with a preferred embodiment the Service level further comprises means for managing and supplying one or more PrePaid related services such as Vending machine, Parking machine, etc.
The Application level comprises means for monitoring the incoming #SS7 signaling or Data transferred from the Interface level.
The Interface level comprises signaling and data stacks means for communication between the operator Network and the PCCS, the said signaling means using #SS7 protocols and the said data stacks means using DATA protocols that are compatible with the different services –Prepaid or Post paid – supplied in the network, whether of the PLMN or PSTN type, in which the PCCS is implemented.

It is a considerable advantage of the invention that due to the capability of the PCCS to communicate with the different elements of the network, including the PrePaid platform, the diverse service platforms and the MSC, via standard protocols, the charging operation is implemented through the most reliable and adequate method for the PrePaid platform and the services, regardless of the type of platforms applied for the various services in the network.

In accordance with another advantage of the invention, the inventive approach of the PCCS enables the merging of voice and data services with the PrePaid charging methods, allowing the operator (PSTN or PLMN) to charge a PrePaid subscriber regardless of the type of Network vendor, Content platform vendor, services or service platforms.

It is yet another advantage of the invention that the PCCS installation and activation is very simple and fast such that an old Prepaid platform may be upgraded with new Services from other vendors by installing the PCCS of the invention in a network with a Prepaid Platform of the prior art.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 190 of 1360

Claims:

1. A PrePaid subscriber charging system to be implemented in a communication network, the said communication network comprising a plurality of Service platforms using different communication protocols and a PrePaid platform with real time charging means, the said PrePaid platform being adapted to communicating with only a limited number of the said Service platforms, the said PrePaid subscriber charging system comprising a) a Service level with means for communicating with the said PrePaid platform, b) an Interface level comprising signaling and data stacks means for communication between the said communication network and the said PrePaid subscriber charging system and c) an Application level with means for monitoring signaling or data transferred from the said Interface level using the said different communication protocols, whereby the said PrePaid subscriber charging system enables real time charging of PrePaid subscribers in respect of the said plurality of Service platforms.

2. A PrePaid subscriber charging system according to claim 1 wherein the said Service level also comprises means for managing and supplying one or more Prepaid services.

3. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said communication system is a public switching telephony network.

4. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said communication system is a public land mobile network.

5. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said Prepaid platform is a Prepaid SCP or Prepaid switch.

6. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said communication system further comprises a switching center means and balance requests or charging requests from one or more of the said Service platforms are routed to the said PrePaid subscriber charging system through the said switching center means.

7. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said communication protocols are standard #SS7 or Data protocols.

8. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said communication protocols comprise a wireless application protocol (WAP) or IN application protocol (INAP) or ISDN user part protocol (ISUP) or HTTP or TCP/IP protocol or HTTP/UCP or HTTP/MAP protocol or any other suitable communication protocol.

9. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said service platforms comprise an IVR push service platform or SMSC push and pull platform or Internet platform or Intranet platform or WAP services platform or Parking or Vending machine or any other suitable service platform.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 191 of 1360

10. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said service platforms comprise a content service platform.

11. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said service platforms comprise an advanced voice service platform.

12. A PrePaid subscriber charging method to be implemented in a communication system according to any of the preceding claims, the said method comprising the following steps:

    a. A PrePaid subscriber initiates a session by routing a request to a Service Platform,

    b. The Service Platform routs a service request to the PrePaid subscriber charging system, using a communication protocol designed for the said Service Platform,

    c. The PrePaid subscriber charging system initiates a balance or a charge request to the said Prepaid Platform,

    d. The prepaid platform responds by sending an account status response or an "adequate balance" or a "balance inadequate" response with or without an account status response to the said PrePaid subscriber charging system,

    e. The said PrePaid subscriber charging system outputs a signal of supply service or do not supply service to the said service platform according to the said response from the said Prepaid Platform.

13. A Prepaid subscriber charging method according to claim 12 hereinabove wherein the said service request is routed to the said PrePaid subscriber charging system via the said switching center means.

14. A Prepaid subscriber charging method according to claim 12 hereinabove wherein the said Service platform is a Push platform and the said session is initiated by the said Push platform at a point of time that had been preset by the said Prepaid subscriber.

15. A Prepaid subscriber charging method according to claim 12 hereinabove wherein the said Service platform is a Push platform and the said session is initiated by the said Push platform at a point of time that had been preset by a third party.

16. A Prepaid subscriber charging method according to claim 2 hereinabove wherein in the event that a "balance inadequate" response is sent from the said Prepaid Platform to the said Prepaid subscriber charging system the said Prepaid subscriber charging system repeats the said balance or charge request at preset intervals until a "balance adequate" response is received or until a preset number of repeated balance or charge requests has been performed.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 192 of 1360

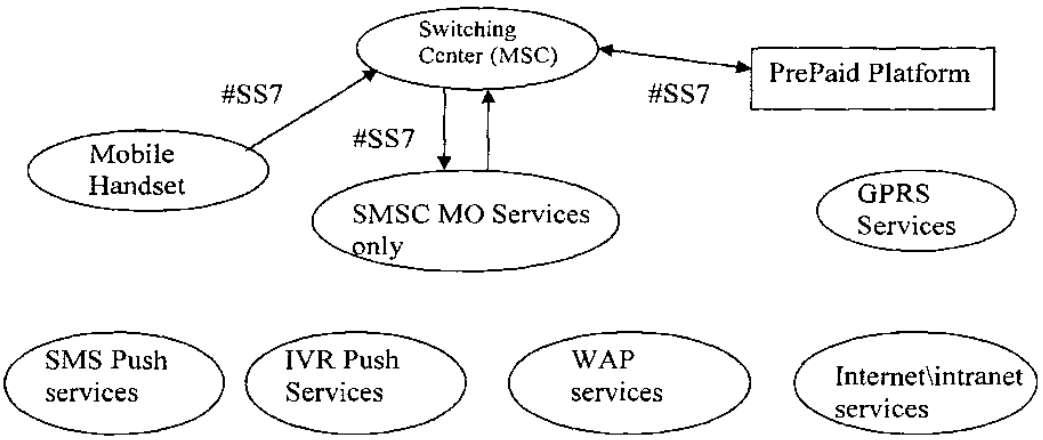

Switching Center (MSC)
PrePaid Platform
#SS7
#SS7
#SS7
Mobile Handset
SMSC MO Services only
GPRS Services
SMS Push services
IVR Push Services
WAP services
Internet\intranet services

Fig. 1

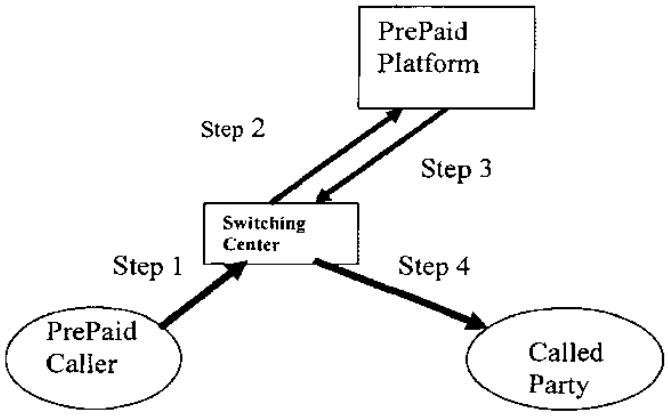

PrePaid
Platform
Step 2
Step 3
Switching
Center
Step 1
Step 4
PrePaid
Caller
Called
Party

Fig. 2

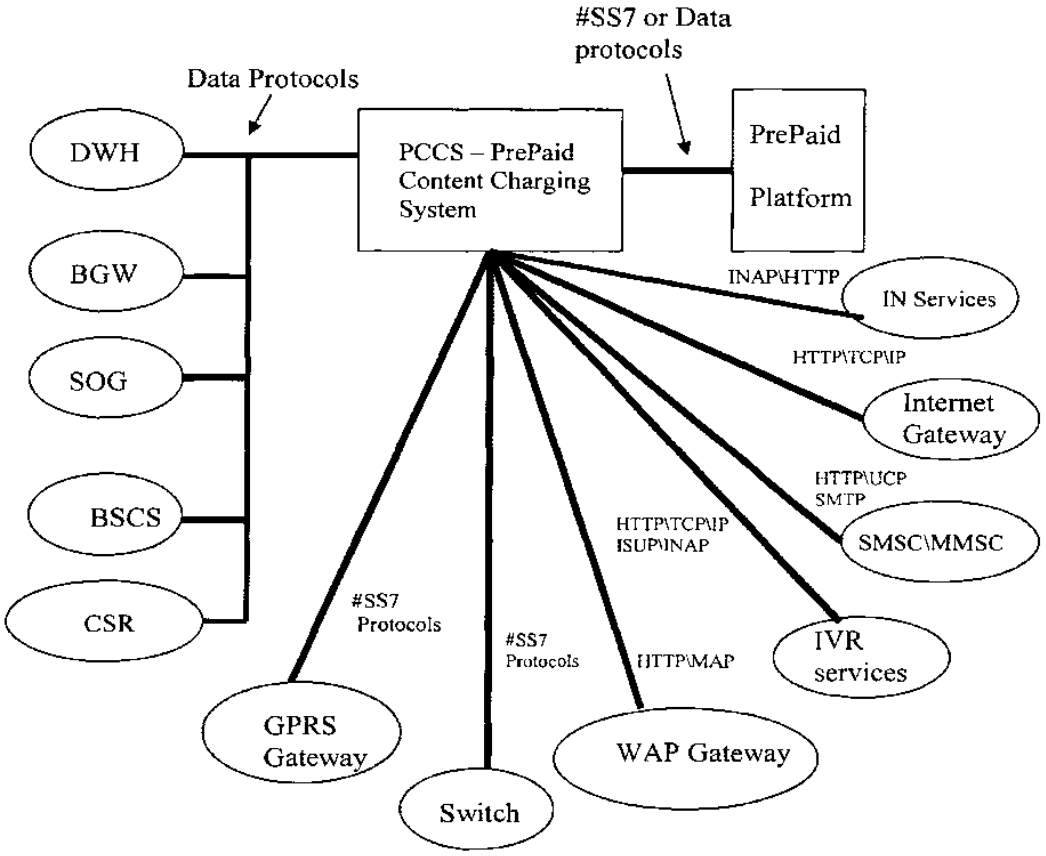

#SS7 or Data protocols
Data Protocols
DWH
BGW
SOG
BSCS
CSR
PCCS – PrePaid Content Charging System
PrePaid Platform
INAP\HTTP
IN Services
HTTP\TCP\IP
Internet Gateway
HTTP\UCP SMTP
SMSC\MMSC
HTTP\TCP\IP ISUP\INAP
IVR services
#SS7 Protocols
#SS7 Protocols
HTTP\MAP
GPRS Gateway
Switch
WAP Gateway

Fig. 3

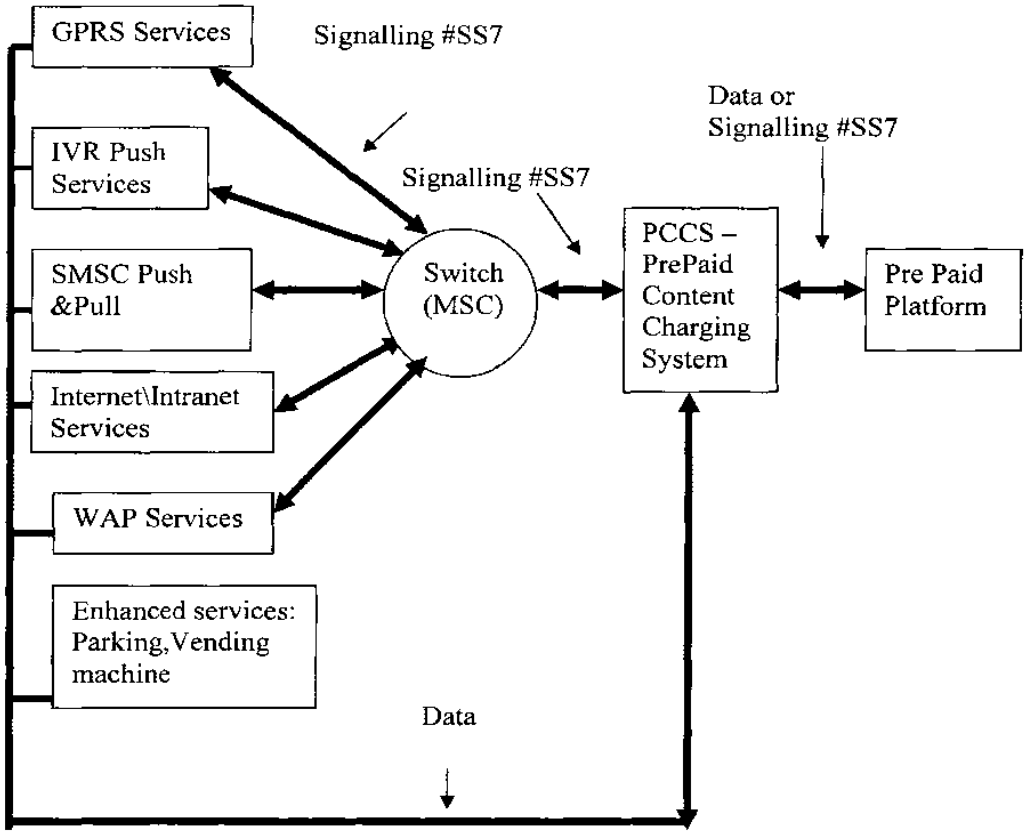

GPRS Services
Signalling #SS7
IVR Push Services
Signalling #SS7
Data or Signalling #SS7
SMSC Push &Pull
Switch (MSC)
PCCS – PrePaid Content Charging System
Pre Paid Platform
Internet\Intranet Services
WAP Services
Enhanced services: Parking,Vending machine
Data

Fig. 4

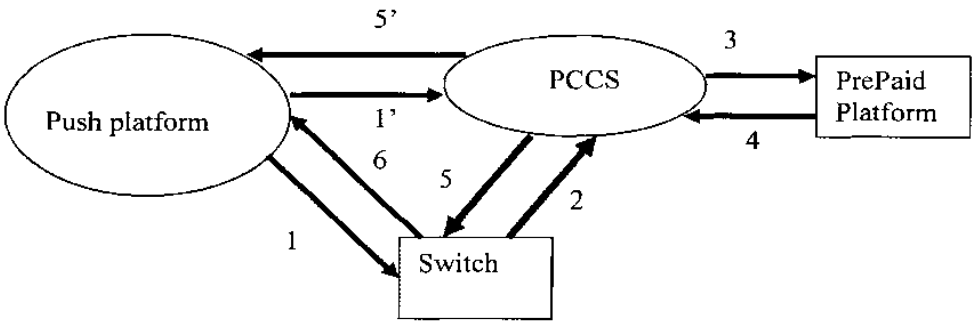


Fig. 5

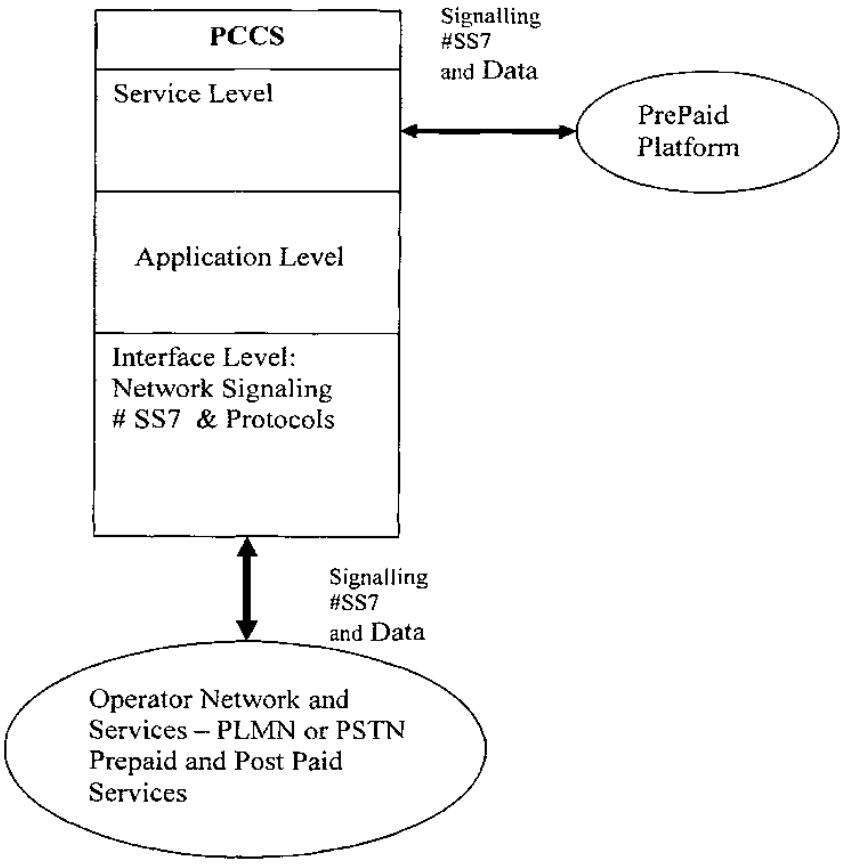

PCCS
Service Level
Application Level
Interface Level:
Network Signaling
SS7 & Protocols
Signalling
#SS7
and Data
PrePaid
Platform
Signalling
#SS7
and Data
Operator Network and
Services – PLMN or PSTN
Prepaid and Post Paid
Services

Fig. 6

INTERNATIONAL SEARCH REPORT

PCT/IL 02/00601

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 H04M17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04M G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 825 857 A (KHALIL ANIS ET AL) 20 October 1998 (1998-10-20) figures 3,4 column 3, line 17 - line 20 column 5, line 66 -column 6, line 14 column 6, line 38 - line 54 column 7, line 58 -column 10, line 30; figures 9A-J	1,3,4, 7-9,12, 13
X	US 5 640 446 A (KULT GEORGE MICHAEL ET AL) 17 June 1997 (1997-06-17) column 2, line 30 - line 56 column 4, line 56 - line 60 column 6, line 25 - line 47 column 17, line 23 - line 43	1-3,5,7, 8

-/--

[X] Further documents are listed in the continuation of box C

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 July 2003	16/07/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schofield, C

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01 93559 A (MURPHY ANNA M ;MOORE RICHARD B (US); VOGNSEN DAVID K (US); WORLDCO) 6 December 2001 (2001-12-06) page 6, line 13 -page 7, line 2 page 11, line 13 -page 12, line 3 figure 1 ---	9
A	WO 97 17678 A (NOKIA TELECOMMUNICATIONS OY ;HANNULA ANTTI (FI); KARI HANNU (FI)) 15 May 1997 (1997-05-15) page 3, line 18 - line 28 page 9, line 1 - line 29 -----	1-16

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 200 of 1360

INTERNATIONAL SEARCH REPORT

PCT/IL 02/00601

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5825857	A	20-10-1998	NONE		
US 5640446	A	17-06-1997	NONE		
WO 0193559	A	06-12-2001	AU	6530201 A	11-12-2001
			CA	2410161 A1	06-12-2001
			EP	1295461 A1	26-03-2003
			WO	0193559 A1	06-12-2001
			US	2002046255 A1	18-04-2002
WO 9717678	A	15-05-1997	FI	955354 A	08-05-1997
			AT	205002 T	15-09-2001
			AU	711112 B2	07-10-1999
			AU	7301496 A	29-05-1997
			CA	2236899 A1	15-05-1997
			CN	1203680 A ,B	30-12-1998
			DE	69614873 D1	04-10-2001
			DE	69614873 T2	11-04-2002
			EP	0865641 A1	23-09-1998
			ES	2160841 T3	16-11-2001
			WO	9717678 A1	15-05-1997
			HK	1016306 A1	12-04-2002
			JP	2000500256 T	11-01-2000
			US	2001011256 A1	02-08-2001

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 201 of 1360

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 March 2004 (18.03.2004)

PCT

(10) International Publication Number
WO 2004/023353 A1

(51) International Patent Classification[7]: G06F 17/60, 153/00

(21) International Application Number:
PCT/AU2003/001126

(22) International Filing Date:
3 September 2003 (03.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2002951198 3 September 2002 (03.09.2002) AU

(71) Applicant *(for all designated States except US)*: **TYNEVALE PTY LIMITED** [AU/AU]; PO Box 673, 19 Church Street, Maitland, New South Wales 2320 (AU).

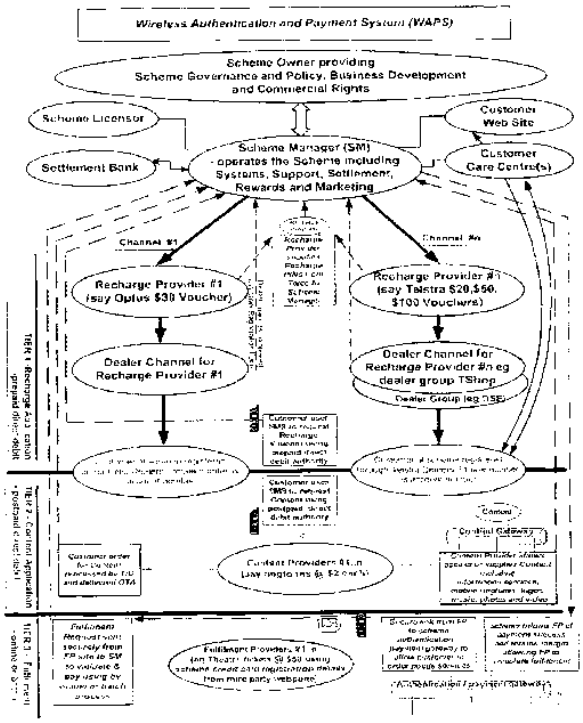
(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **REEVES, Peter, John** [AU/AU]; 21 Pollock Avenue, Wyong, New South Wales 2259 (AU). **SIMARD 3RD, Joseph, Arthur** [AU/AU]; "Lonou Park", 1524 Gresford Road, Torryburn, via Paterson, New South Wales 2421 (AU). **WANN, David, Paul** [AU/AU]; 7 Goonak Parade, Narara, New South Wales 2250 (AU). **PACKETT, Jayson, Geoffrey** [AU/AU]; Unit 2, 159 Denton Park Drive, Aberglasslyn, New South Wales 2320 (AU). **MORGAN-JONES, Mark** [AU/AU]; 95 Ridge Road, Kilaben Bay, New South Wales 2283 (AU).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR A WIRELESS PURCHASE REQUEST AND PAYMENT FOR GOODS OR SERVICES



(57) Abstract: Disclosed is a system and method that enables any subscriber to a wireless communications network to obtain wirelessly and instantly prepaid products and/or services by using their wireless device and by registering with a plan as a customer, and, allowing the plan to maintain the prepayment of the prepaid products and/or services from the customer's financial institution account or facility. Further, customers are able to purchase products and/or services on a non-recurring entitlement basis instantly and to pay for the products and/or services by a subsequent funds transfer to the plan. Furthermore, customers are able to purchase products and/or services from approved third parties through the third parties website, mail order service, phone order service, wireless service or other methods using a secure link to the plan's authentication and/or payment approvals methods.

WO 2004/023353 A1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 202 of 1360

SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designation US*

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR A WIRELESS PURCHASE REQUEST AND PAYMENT FOR GOODS OR SERVICES

Technical Field

The present invention relates to a new type of system for and method of the purchase of goods or services using the transmission of a purchase request via wireless means, and in particular to the purchase of goods or services whereby the purchase is requested by a mobile handset user via the mobile handset. Also in particular, the present invention relates to a computer program which facilitates a wireless request for the purchase, access or rental of goods or services by a mobile handset user making use of the mobile handset.

More particularly, the present invention relates to the wireless transmission by a mobile handset user of a purchase request for a prepaid mobile handset voucher, and a means for effecting payment for the prepaid voucher.

Background Art

Presently, it is known to provide a user of a mobile handset with access to a communications network by allowing the user to purchase prepaid mobile handset vouchers, the value of which can be applied to the user's prepaid mobile handset account, from organisations offering such prepaid vouchers. For example, in Australia a user can purchase preset values of prepaid vouchers (i.e. mobile handset recharge cards) from a telecommunications service provider, such as Telstra (an Australian company), or an authorised reseller. This allows the user to access a telecommunications network and associated services with a mobile handset, and also sets limits on the costs incurred by the user (i.e. the value of the prepaid voucher) for use of the telecommunications network or associated services.

To make use of this service a user is required to establish a "prepaid account" with a telecommunications service provider (i.e. telecommunications carrier), through an authorised retail outlet. A prepaid voucher can then be purchased by the user from a retailer. To use the prepaid voucher the user dials a number supplied by the telecommunications service provider and types in via the mobile handset keypad, the designated prepaid voucher number which appears, usually as a string of numeric and/or alpha digits, on the prepaid voucher. This acts to apply credit to the user's prepaid account which has previously been established with the telecommunications service provider.

Prepaid vouchers (i.e. mobile handset recharge cards or the like) can presently only be bought from certain retailers. A user, or someone else on behalf of the user, is required to attend the premises of such a retailer and purchase a prepaid voucher. This situation has disadvantages. For example, the user is required to physically attend the premises of the retailer. Furthermore, the user cannot access a telecommunication network if the credit in the user's prepaid account has been exhausted other than to access the toll free IVR system for recharging and the user cannot purchase a prepaid voucher, which may occur, for example, if retailers are closed.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 204 of 1360

This identifies a need to provide a user with a prepaid voucher via wireless means, for example by transmitting the prepaid voucher to the user's mobile handset. A further problem then also arises, concerning how to retrieve payment from the user for a wirelessly transmitted prepaid voucher. It would be possible to require the user to supply credit card details prior to sending a prepaid voucher to the user, and perform a funds transaction before delivering a prepaid voucher to the user. However, a problem with this approach is that generally most prepaid voucher users do not have credit cards. Furthermore, if direct debit accounts were to be used, funds cannot be deducted in real-time (due to technology and policy/regulatory restrictions). Organisations are reluctant to deliver goods or services to a user (i.e. customer) and then attempt to obtain funds afterwards through an overnight funds settlement process. This further identifies a need to provide a user with a prepaid voucher via wireless means and obtain payment for the prepaid voucher.

Also, at present, a user is limited in the types of payment systems with which the user can purchase various goods or services using a mobile handset. For example, it is known that at present a mobile handset user can purchase a mobile handset ring tone using a mobile handset by purchasing vouchers which entitle the customer to a number of ring tones. These tones are delivered to the mobile handset by dialling a number and entering in the code for the desired ring tone, or selecting the ring tone from a web site and entering the designated voucher number. This system has the same drawbacks of the current prepaid voucher system. Also, it is known that at present a mobile handset user can purchase cans of soft drink at specific locations by dialling a specified number on the delivery device (a vending machine). The funds are deducted from the user's account. {This system is at present limited to Telstra customers with a non-prepaid account and is currently not available for pre-paid accounts with any carrier.} Moreover, a user is limited in the types of goods or services which are able to be purchased or requested via a mobile handset. If the user does not have a credit card or an existing billing arrangement with an organisation, then the user is typically prevented from purchasing goods or services if the organisation requires payment before delivery of the goods or services to the user. Still furthermore, many users are reluctant to provide credit card details over the Internet or to an unknown organisation. This identifies a need for a new type of system for and/or method of the purchase of goods or services by using the transmission of a purchase request via wireless means, and associated payment means. This also identifies a need for a new type of computer program for facilitating the aforementioned systems or methods.

Definitions

As used herein the term mobile handset should be considered as equivalent to the term mobile phone, cellular phone, cell phone, car phone, satellite phone, module and the like. This includes all forms of mobile, transportable or portable telephones or handsets. The term mobile handset should also be taken to include any device which is able to connect to a wireless communications network and wirelessly transmit data, multimedia content or information to a remote device, for example a remote computer system, over the communications network. This could include, for example, mobile data terminals, personal digital assistants (PDAs), or pagers. The communications network infrastructure may include switches, base stations, bridges,

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 205 of 1360

routers, or any other such specialised components, which facilitate the connection between a mobile handset and a communications network.

Prepaid account: is a mobile handset user's service subscription with a telecommunications or other industry sector service provider (or telecommunications carrier) which can hold an amount of credit (prepaid) which allows a mobile handset to access and utilise a service provider's network and associated services.

Prepaid voucher (or recharge card, recharge voucher, prepaid card, or the like): is purchased by the user from a service provider, reseller, retailer, or the like, and when activated or used applies credit to the user's prepaid account which has previously been established with the telecommunications or other industry sector service provider.

User account (or customer account): is the account held on a management computer system which holds information on the user's entitlement to be issued with a pre-purchased prepaid voucher.

Financial institution account (or bank account): is a monetary account or facility held by the user's financial institution or card issuer. The financial institution account can be debited after obtaining user authority.

Disclosure of Invention

In its various embodiments the present invention seeks to provide a system, method or computer readable medium of instructions which overcomes, or at least ameliorates, the aforementioned and other problems inherit in the prior art.

In a broad form, the present invention addresses existing problems by allowing a user to register with a payment system which pre-purchases a prepaid voucher. Preferably, the pre-purchase is via an overnight settlement process. After the transfer of funds is completed the user is registered with the payment system and a user account is appropriately credited. This could be thought of as pre-allocating a prepaid voucher to the user account, or an entitlement to a prepaid voucher, which the user can request when required. Hence, the user account holds an entitlement to a prepaid voucher which the user has already purchased and may request at any time. The process of requesting the prepaid voucher also triggers a process of deducting further funds from the user's financial institution account, which results in a new prepaid voucher being allocated to the user account for when next required by the user.

Preferably, the prepaid voucher is delivered to the user's mobile handset via the Short Messaging Service (SMS). In another form of the invention, the prepaid voucher could be delivered to the user via Enhanced Messaging Service (EMS) or Multimedia Messaging Service (MMS). The prepaid voucher could be delivered to the user by any other means over a communications or telecommunications network. It should be appreciated that any form of 'messaging' involving transmissions over a wireless network could be utilised to transmit the prepaid voucher.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 206 of 1360

When received the user then applies this prepaid voucher to the user's prepaid account with a telecommunications service provider. In another embodiment, the prepaid voucher can be directly applied to the user's prepaid account with the telecommunications service provider without the user being required to receive and then apply the prepaid voucher.

In another broad form, the present invention provides a payment system which allows a user to request, via a mobile handset, the purchase of goods or services which are paid for by management software debiting the user's financial institution account according to a pre-existing debit authority.

In a further broad form, the present invention provides a system which allocates an entitlement to a prepaid voucher to a user of a mobile handset, the entitlement to the prepaid voucher being recorded in a user account in a management computer system, and whereby the user can request the prepaid voucher be delivered via a mobile handset. Preferably, after the prepaid voucher is delivered the user's financial institution account is debited and an entitlement to a new prepaid voucher is recorded in the management computer system.

In still a further broad form, the present invention provides a system for allowing a user of a mobile handset, with the user having a prepaid account with a telecommunications service provider, to add credit to the prepaid account, the system including:

- the mobile handset operated by the user;
- a management computer system which is able to communicate with the mobile handset;
- management software resident in the management computer system, the management software including a user account, the user account recording any entitlement of the user to a prepaid voucher;
- a financial institution computer system which is accessible via some electronic means, whether in real-time or by a message sent to the institution, by the management computer system, the financial institution computer system holding a financial institution account for the user; and

whereby, in response to a request by the user, the request being wirelessly transmitted from the mobile handset to the management computer system, for a prepaid voucher, the management software transmits the prepaid voucher to the mobile handset and subsequently requests a transfer of funds from the user's financial institution account to a nominated bank account, which when confirmed, results in an entitlement to a new prepaid voucher being recorded in the user account.

In accordance with yet another broad form, the present invention provides a payment system for allowing a user of a mobile handset, the user having executed a debit authority enabling funds to be transferred from a financial institution account to a nominated bank account, to purchase goods or services from a third party using the mobile handset, the system including:

- the mobile handset operated by the user;
- a management computer system;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 207 of 1360

- management software resident in the management computer system;
- a financial institution computer system which is able to communicate with the management computer system, the financial institution computer system holding the financial institution account for the user;
- a third party computer system which is able to communicate with the mobile handset, the third party computer system used by the third party to receive requests for goods or services; and

whereby, in response to a request by the user for the purchase of selected goods or services, the request being wirelessly transmitted from the mobile handset to the third party computer system, the third party requests funds from the management computer system which results in a request for a transfer of funds from the financial institution account to a nominated bank account, which when confirmed, results in the management software transferring the required funds and a purchase request to the third party for the goods or services.

In another embodiment of the present invention, there is provided a method of providing a user with a prepaid voucher which can be used to credit a prepaid account with a telecommunications service provider, the method allowing the user to request and receive the prepaid voucher via a mobile handset, the method including the steps of:

- the user being registered in a management computer system;
- the user wirelessly transmitting a request for a prepaid voucher to the management computer system which hosts management software;
- the management software checking the status of a user account for user entitlement to the prepaid voucher;
- the prepaid voucher being transmitted to the mobile handset; and
- the management software causing funds to be transferred from a financial institution account in a financial institution computer system to a nominated bank account, which when confirmed, results in an entitlement to a new prepaid voucher to be recorded in the user account.

In yet another embodiment of the present invention, there is provided a computer readable medium of instructions residing on a management computer system, the computer readable medium of instructions forming part of a system for facilitating a user of a mobile handset to add credit to a prepaid account with a telecommunications service provider, the computer readable medium of instructions including procedures for:

- receiving a request for a prepaid voucher, the request having been wirelessly transmitted from the mobile handset to the management computer system;
- checking the status of a user account for user entitlement to the prepaid voucher;
- transmitting the prepaid voucher to the mobile handset;
- requesting a transfer of funds from a financial institution account to a nominated bank account; and when the funds transfer is confirmed,
- adding an entitlement to a new prepaid voucher to the user account.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 208 of 1360

In still yet another embodiment of the present invention, there is provided a computer readable medium of instructions residing on an management computer system, the computer readable medium of instructions forming part of a system which facilitates a user of a mobile handset to purchase goods or services from a third party using the mobile handset, the computer readable medium of instructions including means for:

- receiving a funds transfer request from the third party computer system;
- requesting a transfer of funds from the user's financial institution account in a financial institution computer system to a nominated bank account;
- sending a purchase request to the third party
- confirming the transfer of funds; and
- sending the funds to the third party for the goods or services.

According to one aspect the request by the user is an SMS request. In a broad sense the goods or services may be "content" which can be wirelessly delivered to the user's mobile handset. In a particular embodiment, the content is delivered directly to the user's mobile handset from a third party, or to the user's mobile handset via the management computer system. In a particular form of the present invention, the content is prepaid Internet recharge vouchers, mobile handset ring tones, logos, graphics, video, music, subscription services, or the like. In a further form of the invention the goods or services requested by the user may be delivered by physically delivering or picking-up the goods or services.

In one embodiment, the prepaid voucher is an SMS message as representative of a wirless message. In a particular form of the invention the management computer system sends a SMS confirmation of the user's request or purchase confirmation to the user's mobile handset or other nominated mobile handset. In accordance with another specific embodiment of the present invention the mobile handset is not the user's mobile handset. In a further embodiment of the present invention, the nominated bank account is nominated by a Manager of the management computer system. In a further particular embodiment of the present invention, the third party computer system is integrated with the management computer system. In still a further embodiment of the present invention, the nominated bank account and the user's financial institution account are not in the same banking computer system.

The present invention according to yet another aspect provides that the funds transfer is by direct debit from the user's financial institution account. In other forms, the funds transfer can occur using any other form of electronic payment, for example, credit card. In a further broad form of the present invention, the management software provides for the registration of user's, account processing and payment, and receiving user requests.

According to one embodiment of the present invention, the distribution channels (eg. dealers) receive an on-going revenue stream from pre-paid 'connections', similar to post-paid mobile connections.

In a particular form of the present invention the management software is based on the JAVA programming

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 209 of 1360

language. In a particular form of the present invention, a Personal Identification Number (PIN) or password is required to be supplied by the user via the mobile handset before the user's request is processed.

In a further embodiment of the invention, the authentication is provided by an image of the users face captured by a camera contained or connected to the mobile handset and delivered to the biometric authentication component of the system. The face recognition process involves software within the system to generate a small file of approximately 2000 bytes known as a biometric template that represents the salient features of the user's face that can be understood by software in an authentication process to validate an image captured on the user's mobile handset and compared to/with or against the biometric template generated by the system. The face recognition process is triggered which verifies (within high bounds of statistical probability) that the user of the mobile handset is the same person enrolled in the system by comparing the user's biometric template created during the enrolment process and compared with the processed image either generated on the mobile handset or transmitted to a biometric authentication system allowing the system to authenticate the user. Further, content purchased or delivered by the system can be digitally signed (and encrypted if required) with the user's biometric template incorporated into the content to enhance the content owners rights to control and or monitor how the content is distributed including options such as authentication processes involving the user having to present their captured image to the system whenever the content is required to be accessed or played. In addition to purchasing and accessing content used in the system, this 'use of content transaction' could be used as a service to ensure secure delivery of emails and documents over the Internet requiring the user to authenticate themselves with the system's biometric authentication server whenever highly confidential emails, content or documents are required to be accessed either directly on the user's mobile handset or delivered to an Internet service or the user's email service. This embodiment of the invention provides a low cost method of biometric authentication without the user having to purchase personal authentication devices such as tokens or smartcards that must be carried by the user and readers (such as personal smartcard readers) to enquire and /or authenticate the physical token. The enrolment process which could be performed at the retail outlet would incorporate additional steps whereby the retailer would complete a new enrolment or update an existing users biographical enrolment data by confirming the enrolment systems pairing of the biographical enrolment data with the user's biometric template created when the user is directed by the retailer to connect to the system's biometric authentication system. The pairing occurs when the biometric authentication system captures a suitably framed image of the user's face using the user's camera on the mobile handset and creating the user's biometric template, displaying the user's image captured within the retailers online enrolment screen and requesting the retailer validate that the image displayed on their enrolment screen is of the person being enrolled by them. When the retailer confirms this to be the case, the system pairs the biographical enrolment data (including the user's financial institution account details and associated payment authority agreed during the enrolment process) with the user's biometric template created during enrolment. The user's biometric template can be stored on the system's biometric authentication server requiring to be paired with the user's biographical enrolment data whenever a financial transaction or use of content transaction is required to be performed. Alternatively, and subject to the technology embodied within the user's mobile handset, the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 210 of 1360

user's biometric template could be securely stored on either the smartcard that serves as the user's subscription identity module or in a secure 'electronic wallet' or similar concept incorporated into the user's handset. Alternatively, the further embodiment of the invention could provide for a biometric validation engine to be licensed by mobile handset manufacturers and incorporated into future mobile handset models that allow for the local authentication of the user's biometric template without having to connect to the system's biometric authentication system to provide authentication services. In this embodiment, the face recognition process would occur on embedded software within the handset and the software would send an authorisation token, rather than the captured image of the user, to the system during the purchase request.

Brief Description of Figures

The present invention should become apparent from the following description, which is given by way of example only, of a preferred but non-limiting embodiment thereof, described in connection with the accompanying figures, wherein:

Figure 1 illustrates a broad schematic of an embodiment of the payment system;

Figure 2 illustrates a broad schematic of a specific embodiment of the method of the present invention;

Figure 3 illustrates the main use cases according to an embodiment of the present invention; and

Figure 4 illustrates a logical view of the main entities of a particular embodiment of the present invention.

Modes for Carrying Out the Invention

I Overview

Referring to figure 1, a general schematic of the payment system 10 is illustrated. The user 15 has access to a mobile handset 20. The user 15 also has a user account 25 which is recorded in the management computer system 30. The management computer system 30 is administered or managed by a Manager (or Management organisation). The user 15 is additionally required to have a financial institution account 35 held in the financial institution computer system 40. Resident in the management computer system 30 is management software 45. The management software 45 can provide functions for processes such as user registration, account processing and payment, and receiving user wireless requests for a purchase, which could be for a prepaid voucher.

In use, the user 15 desires to purchase user selected goods or services from a third party or the Manager. The third party operates a third party computer system 50 which can at least receive requests for goods or services. Goods or services may include prepaid vouchers or prepaid starter kits for access to a telecommunications network and associated services, "content" such as mobile handset ring tones, logos, graphics, video, music, subscription services, etc, or any other goods or services which are required to be physically delivered to, or picked-up by, the user 15. Prepaid vouchers need not be physically delivered to the user 15, and "content" can be wirelessly delivered to the mobile handset 20, or any other nominated

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 211 of 1360

mobile handset. A prepaid starter kit allows dealers to activate in-store a SIMcard with a new prepaid mobile service. Previously, the dealer received a package that contained the SIMcard and associated mobile handset number. This may be performed on-line from a retail store.

Prior to requesting goods or services, the user needs to be registered with the management computer system 30. This involves the user authorising the Manager to debit the user's financial institution account 35 when required. After registering, funds are transferred from the user's financial institution account 35 to a nominated bank account, the funds being used to purchase a prepaid voucher on behalf of the user. The user's entitlement to receive the prepaid voucher is recorded in the user account 25.

To request goods or services the user 15 operates the mobile handset 20 causing a wireless request 55a to be transmitted to the management computer system 30, or, an SMS request 55b to be transmitted to the third party computer system 50, depending on the goods or services requested. For example, if the purchase request is for a prepaid voucher, then the wireless request 55a is sent to the management computer system 30. If the purchase request is for "content" such as a mobile handset ring tone, then the wireless request 55b is sent directly to the third party computer system 50 offering the ring tone.

When the management computer system 30 receives the wireless request 55a, data or information in the wireless request 55a is passed to the management software 45. If the request is valid, the management software 45 causes a prepaid voucher in the wireless format 60 to be transmitted from the management computer system 30 to the mobile handset 20. If the wireless request 55a is for a prepaid voucher, then the management software 45 checks the user entitlement to a prepaid voucher by checking the user account 25. If the user is entitled to be delivered a prepaid voucher then the management software 45 effects the delivery of the prepaid voucher 60 as a wireless message to the mobile handset 20. The user 15 can then apply or activate the prepaid voucher by dialling a telehandset number indicated in the message. This applies credit, embodied as the prepaid voucher, to the user's prepaid account with the telecommunications service provider, thus enabling the user to access the telecommunications network and associated services.

Furthermore, once the prepaid voucher 60 has been delivered to the mobile handset 20 the management software 45 initiates a request for a further transfer of funds from the financial institution computer system 40, via the computer network 65. The management software 45 requests a transfer of funds from the user's financial institution account 35 in the financial institution computing system 40 to a nominated bank account. This request can be made immediately or at some later time. When the transfer of funds to the nominated bank account is confirmed by the financial institution computer system 40, an entitlement to a new prepaid voucher is recorded in the user account 25 within the management computer system 30. The user can then obtain this pre-purchased prepaid voucher when required in the future without waiting for funds to clear.

Hence, the user 15 is purchasing an entitlement to be sent a prepaid voucher (which may be referred to as a "prepaid prepaid voucher") for access to a telecommunications network and associated services offered by a

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 212 of 1360

telecommunications network provider and the Manager is acting as a reseller.

When the user 15 requests "content", or other goods or services not being a prepaid voucher, an SMS request 55b is sent to the third party computer system 50. Depending on the nature of the goods or services, delivery, that is wirelessly or physically, and the third party itself, goods or services may be delivered prior to or after the transfer of funds associated with payment for the goods or services from the user's financial institution account 35.

Whether pre- or post- delivery payment is required, the third party computer system 50 can receive the user's purchase request. The third party bills the Manager according to its usual practice. When a request for a transfer of funds is received from the third party operating the third party computer system 50 the management software 45 causes the user's financial institution account 35 to be debited accordingly. The funds can then be transferred to the third party, for example to the third party computer system 50, and the Manager can retain a payment processing fee.

Alternatively, the SMS request 55a received by the management software 45 could be a request for content or physical delivery-type goods or services provided by the third party. The Manager could have an arrangement with the third party to offer selected goods or services. In this situation, the management software 45 can relay the user's purchase request to the third party computer system 50 via the computer network 70. Either before or after the goods or services have been delivered to the user 15 or the mobile handset 20, the user's financial institution account 35 can be debited and funds transferred to the third party (which could be confirmed by communication between the management computer system 30 and the third party computer system 50). It may be a condition in the arrangement between the Manager and the third party that funds must be transferred to the third party prior to delivery of goods or services.

II Modules

The following modules provide a more detailed outline of a particular embodiment of the present invention. The modules are intended to be merely illustrative and not limiting to the scope of the present invention.

System and Processes

This section contains various system and process definitions describing the various participants in the method or system and how the participants inter-relate with each other when conducting business within the method or system.

The method or system allows registered users (referred to as Customers in this section) of the method or system to purchase goods and services using a mobile handset. Registration involves a Customer providing an authority to the Manager to pay for goods or services ordered by the Customer.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 213 of 1360

Goods and Services

Goods and services that can be purchased by the Customer in the method or system can broadly be described as:

1) prepaid vouchers: (recharge vouchers) supplied 'over the air' to the Customer's mobile handset. Examples may include Optus' currently existing $30 mobile handset recharge cards, Telstra's currently existing $25, $60 and $100 mobile handset recharge cards;
2) content: that can be ordered and delivered 'over the air' to the Customer's mobile handset. Examples are mobile handset ring tones, logos, video, music, subscription services and other content;
3) fulfilment: of other goods or services ordered by the Customer through endorsed fulfilment methods using sales points provided by other parties such as websites, Wireless Application Protocol (WAP) sites, IVR and other emerging eCommerce technologies. Fulfilment goods and services are not delivered 'over the air'. Delivery is through traditional fulfilment methods such as by courier, mail, email or by Customer pickup. Examples are venue reservations, ordering goods from infomercials or anything that can be sold over the Internet.

Applications

Each of these three types of goods or services are generally distinct within the method or system and involve distinct 'Applications'. Applications are distinct business models, methods or systems involving different payment and delivery processes. The Applications supported by the method or system can include:

1) recharge vouchers: may be purchased using a prepaid direct debit method. This could also referred to as 'prepaid prepaid';
2) content: may be purchased using post-paid direct debit referring to the concept that the payment request is made after the goods or services are delivered; and
3) fulfilment: may be purchased using online authorisation of credit card authority.

In one embodiment of the invention, a Wireless Authentication Payment System (WAPS) is provided which caters for each of the Applications identified above.

System/Method Participants

Referring to figure 2, in a particular, but non-limiting, form of the present invention, the participants within the method or system can include:

(1) The Customer: is a prepaid mobile handset user who registers with the management computer system by providing financial institution account details authorising the Manager to purchase goods or services ordered by the Customer. The Customer might be required to pay the full retail price of a recharge voucher as if the Customer purchased the recharge voucher from a store.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 214 of 1360

(2) The Dealer Channel(s): functions to register the Customer to the method or system. The Dealer Channel comprises Dealer Groups identified and branded with the recharge products available through the Dealer Channel. Each Dealer Group includes:

- a Dealer Franchiser; and
- Dealer Franchisee(s) operating under the governance of the Dealer Franchiser.

When Customers are registered through the Dealer Channel, the Dealer Franchiser and the Dealer Franchisee registering the Customer receive a percentage of every recharge voucher purchased by the Customer as an ongoing commission;

(3) The Recharge Provider: performs two functions within the method or system:

- introduces one or more Dealer Groups to form the Dealer Channel to participate in the method or system; and
- provides (acquires and sells) recharge vouchers to the Manager as a supplier for the recharge products ordered by Customers signing up through the Dealer Channel.

The Recharge Provider bills the Manager for the supply of recharge vouchers making a margin on their cost price. The Recharge Provider does not receive a commission from the Manager.

(4) The Booking Provider: provides content for the method or system that can be ordered and delivered 'over the air' to the Customer's mobile handset. The Booking Provider establishes a retail price for their products; the Manager retains a margin of the transaction value.

(5) The Fulfilment Provider: provides goods or services that are not delivered 'over the air' to the Customer's mobile handset. Instead of paying by VISA, AMEX or Mastercard, etc., a Customer chooses to pay using the prepaid mobile handset account held in the system. The Fulfilment Provider should be authorised by the System Owner to cobrand their sales point (eg. website, WAPsite, IVR, infomercial, etc). The Fulfilment Provider establishes a retail price and the Manager retains a commission from the Fulfilment Provider when processing the Customer payment for goods or services ordered using the system or method.

(6) The Manager: provides the operations management functions of the system or method including hosting the system and registration databases, providing dealer support, settlement and reporting services to the various participants, marketing and assumes responsibility for any reward programmes that may be established. In addition, the Manager can also provide oversight and/or outsources a Customer Care Centre and a Customer website service provision. The Manager may make a profit on the difference between the retail price charged to the Customer less the commissions paid to the Dealer Channel, to system support, to clearing payments through the bank, payment of merchant fees, bad debts and the cost to maintain the Customer Care Centre and the Customer website.

(7) The System Licensor: is regarded as the provider of the management software to the system. The System Licensor may provide an exclusive licence to the System Owner and/or Manager to use the management software The System Licensor may be paid a transaction fee as a percentage of each Customer

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 215 of 1360

purchase made in the system. The System Licensor may also be responsible for the maintenance and upgrading of the management software.

(8) The System Owner; is regarded as the owner of the system. The System Owner provides the System Governance and Policy, Business Development and determines Commercial Rights. The System Owner may provide an exclusive or non-exclusive licence to the Manager to use the system.

System Definition and Processes – The Customer

The system or method enables prepaid mobile handset Customers the ability to buy vouchers (prepaid recharge cards) using a mobile handset 'over-the-air' anywhere and at any time effectively using a bank account. This allows the Customer the 'best of both worlds', that is all the convenience of a post-paid account handset with all the advantages of a prepaid account including lower call costs, superior cost control and no minimum spending requirement.

The system requires the customer to register with the system using a password so that the account is secure. Registering with the system can be performed at an authorised dealer or can be performed using a website.

Part of the registration process involves signing a Direct Debit Authority authorising the Manager to purchase vouchers using the Customer's bank account. Whenever a voucher is ordered by using the mobile handset to send an SMS request, the voucher is sent almost immediately by being previously purchased using the bank account. This also allows a parent to control the use of a prepaid account that can be set up for use by a child or teenager. The parent is identified as the Account Holder and the child/teenager as the Account User, with the parent safe in the knowledge that the account can be used when required, and that the parent knows when vouchers are bought, and also that the prepaid account is secured by a password that only the parent (as the Account Holder) knows.

Furthermore, the system or method can include many advanced features such as 'Any Mobile' which allows credit to be bought, even if a Customer does not have any credit left in the prepaid account, by using another mobile handset, for example a friend's mobile handset.

A Customer can also:

purchase low value content that can be delivered 'over the air' to a mobile handset or like device. Current examples of such content are mobile handset ring tones, logos, video, music, information services and other content. A bank account or similar can be direct debited to the value of content ordered from the mobile handset or through an authorised website;order or book higher value goods or services over authorised Handset, websites or WAPsites using credit card registration details as the payment method. Using the system as a payment method provides confidence because a Customer does not need to supply credit card details over the handset or over the Internet.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 216 of 1360

System Definition and Processes - The Recharge Application

The Recharge Application is the business architecture of the system which allows Customers to register with the system through authorised storefront dealers or approved association organisations. Customers are required to 'register' with the system. Registration occurs when a customer signs up at an Authorised Dealer or other location.

A Dealer Channel includes one or more Dealer Groups associated with a Recharge Provider. A Dealer Group includes a Dealer Franchiser and Dealer Franchisees operating under the governance of the Dealer Franchiser. The system allows for multiple Dealer Groups associated with the introducing Recharge Provider and allows for multiple Recharge Providers within the system architecture. Collectively, this arrangement forms the participants of the Recharge Application, specifically, the collection of Recharge Providers each having contributed Dealer Channels, each of which is represented by Dealer Groups, each of which is identified as the Dealer Group Franchiser and the collection of Dealer Group Franchisees.

A Dealer Channel is typically identified as the collection of Dealers selling one or more brands of recharge card or voucher. As a non-limiting example, at present the Australian market would allow the system to have the following Dealer Channels marketing the following prepaid recharge voucher values:

Optus - $30 mobile vouchers, Optus - $14.95/7hr, $19.95/15hr, $34.95/30hr and $44.95/60hr internet vouchers; Telstra - $25, $60 and $100 vouchers; Virgin - $15; Vodafone - $20, $30, $50, $100 mobile vouchers; AAPT etc.

The system is flexible and allows for any combination of the following types of Recharge Application models which are provided as illustrative examples.

Example 1 – Dealer Group becomes the Recharge Provider.

A Dealer Group (say Network Communications – an Optus Premium Dealer) may negotiate the role of the Recharge Provider and introduce its dealerships to form a Dealer Channel. Network Communications dealerships could all be branded with Optus and the Manager brand.

Example 2 – Telco Introduces balance of Dealers

As an extension of example 1, Optus Communications may negotiate the role of the Recharge Provider and introduce the balance of its Dealer Groups (say Optus World, C21, Tandy and Strathfield Car Radios) to form a Dealer Channel. In this instance, there would be two Dealer Channels providing Optus recharge vouchers. The balance of Optus Dealer Groups would all be branded with Optus and the same Manager brands for both Dealer Channels. The Customer would not be able to discern that there are two Dealer Channels.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 217 of 1360

Example 3 – Telco introduces all its Dealers.

A telecommunications company (say Telstra) may negotiate the role of the Recharge Provider for the Telstra Dealer Channel with Franchisors for Tshops, DSE, Strathfield Car Radio, etc., introducing their Dealer Franchisees within their respective Dealer Groups to form the Dealer Channel.

Further, Telstra may decide to brand the system as its own product. Subsequent to negotiations with the System Owner, Telstra are licensed as a Manager of their own system and brand the system distinctly from the system described in Example 2.

Example 4 – Dealer Group participates in two different Dealer Channels

If examples 2 and 3 were to occur at the same time, the Dealer Group Strathfield Car Radio which holds dealerships with Telstra and Optus, could participate in two different Dealer Channels of the system at the same time. Customers registering through this Dealer Group would register with the Dealer Channel associated with the Customer's recharge voucher.

Dealer Groups receive ongoing commissions subject to commercial rights negotiated with the respective Recharge Provider and the currency of their dealership arrangement with the Dealer Channel to which their Customers are signed. In example 2, if Tandy were to lose their status as dealers in the Optus Dealer Channel, the Tandy Dealer Group would not receive any additional commission payments subsequent to the date of disassociation for Customers registered through that Dealer Channel. If Tandy participated in another Dealer Channel, Tandy would not be required to remove branding with the system and would continue to receive commissions generated through the other Dealer Channel.

When Customers are registered through the Dealer Group, the Dealer Franchiser and the Dealer Franchisee registering the Customer may receive a percentage of every recharge voucher purchased by the Customer as an ongoing commission with the Recharge Provider supplying Recharge Vouchers as appropriate. Unless commercial arrangements are made between the System Owner and the Recharge Provider, participants in the Content Application generally do not receive commissions from Customer purchases made within either the Content Application or the Fulfilment Application.

The system automatically generates settlements and settlement reports for commissions earnt by the members of the Dealer Groups within the Dealer Channel. Settlement may occur overnight, weekly or monthly subject to the terms of settlement negotiated by the Manager with the Recharge Provider on behalf of the Dealer Group. The Manager can provide support to the Dealer Group.

System Definition and Processes – The Content Application

The Content Application is the business architecture of the system that allows registered Customers within the system to purchase Content to be delivered to their mobile handset using either existing or future 'over the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 218 of 1360

air' or wireless technologies. Examples of Content that can be purchased are mobile handset ring tones, logos, screen savers, video, music, subscription and information services and other content.

There may be multiple Content Providers to the system. Content Providers can be authorised by the System Owner to participate in the system. Content Providers can provide access to the Manager for the Content through a Content Provider's 'Content System'. This may be through a technical interface to the Manager or directly supplied by the Content Provider and managed by the system. Collectively, this arrangement forms the participants and mechanisms of the Content Application, specifically, the collection of Collection Providers, and Content Systems and interfaces.

Each Content Provider provides a number branded to the Content Provider and distinct to the Request Number for the Customer to send SMS requests to order Content. The Content Provider is responsible for their own point of sale material, branding, content and content selection menus / content item numbers. When a Customer orders Content, the Customer send an SMS request to the Content Provider's Request Number, thus ordering an item. The message format could be agreed with the Manager to ensure consistency throughout all Content Providers.

If the order is accepted, (i.e. the Customer's account status is 'active'), then the ordered Content is delivered over the air to the Customer's mobile handset. This may be via SMS or another wireless delivery mechanism. The Customer's debit authority is used to draw funds to the value of the content ordered independent of any recharge process.

System Definition and Processes – The Fulfilment Application

The Fulfilment Application is the business architecture of the system that allows registered Customers within the system who have registered credit card details to purchase goods or services from Fulfilment Providers.

Fulfilment Providers sell goods or services through sales points that in addition to providing payment methods such as VISA, AMEX or Mastercard are authorised by the System Owner to offer payment using the system as a payment method. The sales point may be a website, WAPsite, IVR or infomercial, which is cobranded with the System Owner brand or other indicative indicia.

The Fulfilment Provider establishes a secure connection to the system to transmit online payment requests and to accept or decline the payment request. The Fulfilment Provider establishes a retail price and the Manager retains a commission from the Fulfilment Provider when processing the Customer payment for goods or services ordered using the system.

System Definition and Processes – System Management

The system uses software and operating processes designed and developed according to industry and security best practice guidelines and compliant with relevant legislation. The system is managed by the Manager. The

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 219 of 1360

Manager implements aspects of system management including system processes and support including the backend systems, databases, technical architecture, interfaces to a settlement bank, Call Centre and websites.

The following concepts are backend processes or procedures that enable the system to functionally operate.

Processing States

The system handles the processing of Accounts using logical states known as Processing States. The Processing States include:

- PreRegistered, PreRegistered_BadDebt and PreRegistered_BadBank which describe Accounts before they can be used by the customer:
  - *'PreRegistered'* means the Account has been created and the initial payment request has been made but not cleared;
  - *'PreRegistered_BadDebt'* means the Account has been created and the initial payment has been declined by the Customer's bank. No further processing occurs until the Customer advises sufficient funds are available. When notified, the state is reset to PreRegistered which restarts the payment request process;
  - *'PreRegistered_BadBank'* means that the Account has been created and the initial payment request has been rejected as the Customer Bank Account Details are incorrect. No further processing occurs until the Customer supplies their correct Bank Account Details. When corrected, the state is reset to Pending which restarts the payment request process;

- Active, Pending , Bad Debt and Bad Bank are normal processing states once customers start using the system:
  - *'Active'* means the Account has an entitlement to a Voucher which can be immediately sent to a Customer who Requests a Voucher;
  - *'Pending'* means that the Account does not have an entitlement to a Voucher, the system has requested a payment on the Customer's bank to initially allocate or replace a voucher and that the system has not received notification that funds have cleared;
  - *'Bad Debt'* means that the Account does not have an entitlement to a Voucher, the system has requested a payment on the Customer's bank to initially allocate or replace a voucher which has been declined by the Customer's bank. No further processing will occur until the Customer advises sufficient funds are available. When notified, the state is reset to Pending which restarts the payment request process;
  - *'Bad Bank'* means that the Account does not have an entitlement to a Voucher, the system has requested a payment on the Customer's bank to initially allocate or replace a Voucher and has been rejected by the Customer's bank as the bank account details are not recognised. No further processing occurs until the Customer supplies correct Bank Account Details. When corrected, the state is reset to Pending which restarts the payment request process;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 220 of 1360

- *'Cancelled'* is a state when the Account has been closed and the Customer can no longer use the system without Re-Registering.

Staff Roles

The system is administered and operated by the following staff categories performing roles that provide appropriate security access and controls to perform their operational responsibilities.:-

- Scheme Operators (SOs) – perform all the back office registration functions for the system including:
  - data entry of new applications and re-registering Customers;
  - the completeness and accuracy of information received and entered is correct;
  - the scanning and filing of registration information;
  - the initial 'Draw Down' of funds is completed correctly;
  - Bad Debts and Bad Bank processing of PreRegistered accounts is handled correctly and ;
  - that Accounts are Activated correctly.
- Scheme Administrators (SAs) – have full access to all of the operational management functions of the System and perform
  - Customer complaint resolution;
  - operational fraud management of the system;
  - cancelling customer accounts that are not initiated by the Account Holder;
  - acquirer bank settlement functions including
    - preparing and uploading Bank Bulk Funds Movement Files;
    - downloading and preparing Bank Settlement Files;
    - Process Account Statements;
    - manual oversight of closing open settlement batches within 2 business day window as required.
- Financial Administrator (FA) - is responsible for the financial management of the system or method including the financial management of the company with specific system responsibilities for
  - replenishment of PINs to the Unallocated Voucher Pool from the voucher supplier;
  - for internal audits of the system including manual and automatic processing;
  - processing dealer invoices and making settlement to Dealers;
  - oversight of settlement functions.
- Customer Care Operator (CCOs) – performs all Call Centre functions for calls received by the system including cancelling of accounts at Account Holder request. Complaints are deferred to an Administrator. CCOs also provide information on how to register for the system including mailing or emailing application forms upon request.
- Dealer Manager – overall responsibility for dealer management including
  - dealer appointments;
  - dealer training;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 221 of 1360

- dealer support;
- generating and providing dealer reports;
- dealer complaints resolution; and
- dealer collateral.

- Technical Support (TS) – overall responsibility for IT Systems, support, archiving, compliance with privacy and security policies, disaster recovery and system security.
- Operations Manager – responsible for the overall operation of the system.

Activate an Account

'Activate an Account' is an automatic process that changes the processing state of a PreRegistered Account to an Active Account. This process will occur whenever the Initial Draw Down results in the funds being cleared by the Customer's bank account. The Customer is notified the Account is Activated when the system sends the Customer a 'Welcome Message' by SMS. The Account can now be used by the customer to 'Request a voucher' from the system.

Request a Voucher

'Request a voucher' refers to a process that occurs whenever a Customer sends their password via SMS to the system's SMS server which upon receipt will validate the identity of the SIM in the mobile handset sending the SMS, authenticate the identity of the SIM against the Customer registration database and verify that the password is valid.

Deliver a Voucher

'Deliver a voucher' refers to a process where the system has received a 'Request a voucher', has verified the Customer's password, confirms that the Customer's Account is Active and then sends and validates an SMS that is delivered to the Customer's mobile handset which contains a Voucher number that the Customer can subsequently use to credit their prepaid handset credit.

Bad Attempts

'Bad Attempts' occur when either a Customer does not send a valid 'Request a voucher' or an attempt is made to defraud the system.

Account is Blocked

The system does not ignore 'Bad Attempts' and writes attempts to a 'Potential Fraud Log File'. When threshold levels are reached, the system restricts the operation of an Account by flagging the Account as Blocked. Blocking an Account will allow normal processing of States to occur, such as 'Draw Downs' and clearing of payments, however when an account is Blocked, the system will not allow a Voucher to be delivered nor respond by continuing to send error messages via SMS to the requesting mobile handset.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 222 of 1360

Draw Down

'Draw Down' refers to a process where the system attempts to receive a payment from a Customer's bank account prior to the system providing either the initial Voucher (Initial Draw Down) or to purchase a replacement Voucher to replace a Voucher after a recent 'Voucher Delivery' to the Customer using SMS.

Batching of Customer Payment Requests – Bulk Funds Movement File

The system uses an acquirer bank and software created by the bank to upload Customer payment requests in a Bulk Funds Movement File (BFMF). The BFMF is manually created by an Administrator using the system, generally before a 5 pm settlement deadline each business day. When the BFMF option is run, the system processes all Customer payment requests to the acquiring bank in batches of nominally 100 transactions. The system creates a batch identifier that is associated with transactions within the batch to allow for cross referencing. The transactions uploaded are settled overnight by the acquirer with each of the Customer bank accounts associated with the payment request transactions.

Bank Settlement file

'Bank Settlement File' refers to the file that is downloaded each morning using the acquirer bank's online banking facility. The Bank Settlement file shows all batches that were settled in whole or in part the previous evening. For each batch in the file the system can interpret:-

- the batch identifier for that batch;
- A= the batch total of the customer payments requested in that batch;
- B= the batch total cleared to date in that batch;
- C= details and value of individual rejected transactions in that batch and;
- D= details and value of individual rejections of a bad debt type in that batch.

Consequently E (the value of transactions that have not cleared, not rejected or not declined for payment) can be represented in the equation $E = A - (B + C + D)$

Process Account Statements

'Process Account Statements' refers to a clearing process which processes the content of all Bank Settlement files that have Open batches. If a batch is Open, the system knows that some Customer transaction in the batch have not been accounted for by the acquirer bank. Consequently, the batch is still open if $E > 0$. If all Voucher values are equal, then the value of E is a multiple of the Voucher value and the multiple represents the number of payment requests that are still to be settled by the acquirer bank.

If a batch is Closed, the system knows that every Customer transaction in the batch has been accounted for as either cleared (payment received), not cleared (a bad debt) or not processed (a bad bank) by the acquirer bank. Consequently, the batch can be closed when $E = 0$.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 223 of 1360

When the Process Account Statement option is run :

- transactions that have been declared as Bad Debts in the Bank Settlement File will result in the state of Customer's Account being changed to either PreRegistered_BadDebt or Bad Debt; and
- transactions that have been declared as Bad Bank in the Bank Settlement File will result in the state of Customer's Account being changed to either PreRegistered_BadBank or Bad Bank.

When the Process Account Statement option is run and results in the batch being Closed, transactions that have not been declared as Bad Debts or rejected as Bad Bank have been settled in full by the acquirer bank. Every one of these transactions can automatically cause the state of the Account associated with these transactions to be set as Active and the system can move a Voucher from the Unallocated Voucher Pool to the Allocated Voucher Pool and create an entitlement to the voucher to the Account.

Manually Closed Batch

'Manually Closed Batch' refers to a manual process that is performed to Close a batch that has not been closed automatically by the system within the prescribed two business day window allowed for a Draw Down to be completed. Adjustments in respect of the unaccounted transaction(s) are followed up with the relevant customer and bank as soon as practicable. This should be an irregular event. Batch size is configurable. By limiting batch size, the system can realise a higher closure rate on Day 1 processing.

Business Day 1 - Friday

Assume a batch of Customer Payment Request is created on Friday afternoon. Settlement is performed over night with a 4pm cutoff (business nights only). If the Batch is closed the morning following the first settlement (Saturday), all transactions that have cleared can be processed on Saturday or within one business day.

Business Day 2 - Monday

Assuming the batch is not closed on Saturday. The batch can be reprocessed over night on Monday, being the next business day. If the Batch is closed the next morning (Tuesday), all transactions have cleared on Tuesday or within two business days.

Under the Service Level agreements operating with Direct Debit Authorities, it is not expected that any batches should survive as Open beyond two business days.

It is recommended that if a batch is still Open after Business Day 2 that

- calls are made to the acquirer bank to determine why the batch has not closed
- and that by 4pm, that a 'Manually Closed Batch' option is performed

This means that all batches should be closed within two business days.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 224 of 1360

III Software Architecture

The following description describes a preferred, but non-limiting, embodiment of the software architecture which can be used to provide the system or method. Various other types of software architecture could equally be used and should be considered to be within the scope of the present invention.

Introduction

This section describes the software architecture for the Wireless Application Payment System. The system is a system to allow product purchase and/or delivery and/or confirmation using SMS or other wireless communication methods-initiated transactions.

The first application of the software is to allow delivery of a prepaid mobile handset voucher to a Customer via SMS, at the request of the Customer from an SMS message, and the Customer's account to be credited with another prepaid voucher after a successful transfer of funds from the Customer's bank account to the Scheme Manager's bank account. Other applications which can extend the system include delivery of ring tones and other products capable of being delivered to a Customer's mobile handset, and purchasing of products by registered users of the system using the funds transfer mechanisms of the system. The system does not preclude purchasing of a product via other means (such as through web-based interfaces), where the confirmation of purchase is performed using the wireless technology.

Overall Description

The system contains a service that accepts SMS messages and forwards the message to the J2EE processing and settlement engine via JMS. This service also receives messages from the JMS bus and sends the message via the SMS device/gateway. The J2EE processing and settlement engine receives messages from the JMS bus and processes these messages, which are normally requests for products. The engine is implemented as a collection of EJB session and message-driven beans.

The system also contains a Java, wing-based GUI for maintaining the application reference data, Customer registrations, system participants, and financial information. Referring to figure 3 and figure 4 the following use cases represent the architecturally significant use cases in the system.

Register Customer

- Customer details are entered into a screen from a paper registration form.
- The Customer details are checked against the current database for consistency: specifically, is this Customer already registered (duplicate mobile number), or is

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 225 of 1360

someone else registered using this mobile number. Also, BSB and account number is checked against the database and a warning is flagged to the operator.

- Customer Password is preferably 4-6 alphanumeric characters but is configurable to any system requirements.
- If the Customer registration is successful, a NewVoucherRequest record is created to allow the initial voucher credit against the Customer's account. The Customer record is in a state of "Pre-processed" until the request is processed.

Process Account Statement File

- User selects the file
- File is opened
- For each record in the file:
    - Extract the account or batch reference
    - If it's a WAPS entry:
        - If the amount is –ve and there is a WAPS account reference,
            - Check for duplicates
            - create a bad debt
            - set Customers account to "BAD_DEBT"
            - find the outstanding NewVoucherRequest record and set its status to "FAILED"
        - If the amount is +ve and there is a batch reference
            - Check for duplicates
            - Find the DirectDebitBatch and set the "ActualAmount"
- Perfom the Settle Outstanding Accounts use case.

Settle Outstanding Accounts

- Find all DirectDebitBatch records which are not "CLEARED"
- For each batch:
    - If the Amount and ActualAmount are different, and the sum of the bad debts for this batch is not equal to the difference, do not clear the batch

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 226 of 1360

- To clear the batch, execute the "Clear Funds for NewVoucherRequest" for each item in the batch for which there is no bad debt.

Clear Funds for New Voucher Request

When a debit was successful, the new voucher request was successful and the Customers voucher account is credited and funds from the payment are settled.

- Set status to cleared
- Apportion funds to participant accounts using the margins contained in the RechargePlan. Credit these amounts as new AccountLineItem records for each ParticipantAccount.
- Update the Customer's account by setting a voucher credit to the account and setting the state to "ACTIVE".

Process Prepaid Voucher File

- User selects File
- Create a voucher file record
- For each record in the file, add the record to the database

Process Recharge Request

Main Flow

- System receives an SMS
- The sender is validated against the account database
- The PIN in the message is validated against the database
- If the account status is in credit then send an SMS using the next voucher from the pool
- Update the account status (set to "PENDING") & creates NewVoucherRequest transaction (used by the Create Direct Debit use case) and sends the SMS

No credit:

- Check the time of the last successful NewVoucherRequest. If it is within the last hour,
- If there have been 3 or more resends in the last hour, ignore it, otherwise:
- resend the PIN and remember the resend.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 227 of 1360

- Otherwise , if there has been less than 3 errors in the last 24 hours, send a "No voucher credit" message

Invalid Password:

- For the first three occurrences, send a message "Invalid password (n/3)"

Alternatives

- The number of invalid password attempts or no credit attempts is configurable
- The messages sent in the SMS is configurable

Create Payment File

- User selects participant type and participant.
- If the participant type is Dealer, then the user selects a Dealer Group and the "Create Dealer Payment File" use case is executed for the whole group. Otherwise:
- Create a FundsTransferFile and a physical batch file with a line item that is a credit to the participant's bank account.
- The amount is the sum of all uncleared line items in ParticipantAccount for that participant.
- All line items are set to "cleared"

Create Dealer Payment File

- Create a FundsTransferFile and a physical batch file
- For each dealer:
  - Add up all the Amounts for the Dealers account that have not been cleared and add the total to a line item in the file. The line item will be a credit to the dealers bank account.
  - All line item amounts are set to "CLEARED".

Maintain Users

- Users have 1 or more roles corresponding to the actors in the specification
- Each function is associated with one or more roles
- The system will validate that the user has the appropriate rights to perform each use case by checking the role(s) of the user

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 228 of 1360

Create Direct Debit File

- Create a new direct debit file (using date for filename)
- For each unprocessed CustomerAccountDebit transaction:
  - Add it to the DD file
  - Mark it as processed (link it to the debit file db record)

Supplementary Requirements

- The number of unsent vouchers, minus the number of outstanding requests, must appear on a main menu.

IV Appendix A

Attached in Appendix A is a narrative of example scenarios of the present invention in actual use. These scenarios are intended to provide an understanding of the various embodiments of the present invention and are not intended to limit the invention in any way. The scenarios are illustrative examples. Reference to "TopItUp" in Appendix A should be read as a reference to the system or the method, the Manager or the System Owner as appropriate.

Thus, there has been provided in accordance with the present invention a system or method, or a computer program, which satisfies the advantages set forth above.

The invention may also be said broadly to consist in the parts, elements and features referred to or indicated in the specification of the application, individually or collectively, in any or all combinations of two or more of said parts, elements or features, and where specific integers are mentioned herein which have known equivalents in the art to which the invention relates, such known equivalents are deemed to be incorporated herein as if individually set forth.

Although the preferred embodiment has been described in detail, it should be understood that various changes, substitutions, and alterations can be made herein by one of ordinary skill in the art without departing from the spirit or scope of the present invention.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 229 of 1360

APPENDIX A

Scenarios

Scenarios are a method of telling a narrative which provides insight and understanding into the workings of a system or scheme.

Instore Registration Scenarios

Customer Types

John Evans lives at Port Kembla and travels to work at Hornsby each day by train. His wife Kristy works in the local pharmacy three days per week and walks to work They are blessed with two sons Mark aged 15 and Matt aged 10. Mark and Matt both travel to school by bus. As a typical family with both parents working, being together as much as possible, keeping in touch and personal safety issues are key values in family decisions.

John has an office job and has a company supplied handset as he is often required to be contactable out of hours. John will occasionally ring Kristy on her mobile or the home handset when travelling home from work to arrange important family matters such as 'do you want me to bring anything home', 'what's on for dinner' or 'can you pick me up'.

Kristy bought a mobile handset three years ago on a $20 a month access fee plus calls plan with Telstra. The handset has worked great but is now considered bulky by modern standards. Until recently, she used the handset to be contactable, to make emergency calls at work and for personal safety reasons walking to work. Recently, Joanne, a friend in her Wednesday bridge club showed her how to use SMS and Kristy now regularly sends SMS to John to pick up groceries etc on his way home. Joanne has a Nokia 3310 prepaid mobile that she bought from Network Communications at Wollongong and has been encouraging Kristy to get a new prepaid handset from them since they really helped her when she was getting started.

When Matt gets home from primary school each day, Mum asks him to ring her on her mobile to let her know that he got home safely. Sometimes the school bus is not that reliable getting to school, particularly as the timetable has changed twice in the past three months. On two occasions recently, Matt has waited with other primary school kids at the bus stop for twenty minutes after the bus is due. He had been told that if ever missed the bus to go back home and ring Kristy at work.

Mark's 16th birthday is next Thursday. Half of the kids in Mark's class already have mobiles (mostly prepaid). Mark has had a keycard for four months. His allowance is paid into his account each month by Dad using internet banking. During the winter months, Mark stays back after school for soccer training. Mark gets home twenty minutes later than Matt. Mark doesn't have to ring Kristy unless his plans change at school. He has used a friend's mobile in the past.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 230 of 1360

Matt's bus incidents have caused great concern for his parents. They decide to get a new prepaid mobile for both Kristy and Mark. Mark's handset is to be his birthday present. Kristy is going to pass on her old handset to Matt.

On Saturday , they go to the Network store Joanne recommended to Kristy. After talking to Lee, the salesperson, they choose to port Kristy's number from Telstra to her new Nokia 3310 Optus prepaid handset using a port pack. Mark gets a new Optus prepaid Nokia 3310 and faceplate. Matt gets an Optus prepaid starter kit and a new faceplate for the Nokia 5110. Lee demonstrates the handsets and explains to the Evans's the various options for topping up their handsets. .

Customer InStore Registration

Lee knows that Prepaid is becoming a very significant proportion of his business while at the same time postpaid connections have dropped alarmingly. He's all too aware that despite the increased prepaid handset bundles and starter kit sales since prepaid was launched some four years ago, the number of customers topping up each month at his store is dramatically less than the number of prepaid connections he has done, even allowing for customers churning or cancelling their service. Lee knows these customers of his are topping up somewhere else and this loss of revenue coupled with the reduction in contract customers is adversely affecting his business. He's convinced that TopItUp is the way to increase his income by signing up prepaid customers to the TopItUp system simply because it ensures that he receives every TopUp his customer purchases no matter where and when the customer decides to TopUp. He also is pretty happy about the fact that he doesn't have to worry about receiving anymore prepaid TopUp invoices from Optus or, in relation to these invoices, not having enough money to pay his hardware account as TopItUp administer all that. Lee also knows that eventually TopItUp can, in the future, be used by him to sell other products and services thereby providing even more income for the store and the Network vision.

He therefore pulls out a TopItUp User Guide brochure and explains the advantages of topping up their handsets using TopItup over existing methods. Lee explains further that TopItUp gives them the 'Best of Both Worlds' being 'Prepaid Prepaid'. TopItUp allows them the convenience of an account handset in that they can TopUp over the air whenever and wherever they want to. At the same time, TopItUp provides all of the advantages of a prepaid account including lower call costs, superior cost control and no minimum spends.

After having spent some time with the Evans's, Lee knows that the primary reason they have decided to come into the store today is for Matt's situation concerning the erratic bus service. Lee is quick to point out how TopItUp can provide even greater peace of mind and convenience than other TopUp methods through the parental control feature via SMS. At the same time he points out to Mark that should he find himself in a similar situation with little or no credits, he can top it up via the 'Any Mobile' feature using a mate's handset. Mark is impressed and thinks that when the time comes he will try it from a friend's handset just to 'show off'.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 231 of 1360

John and Kristy are impressed with the benefits of the TopItUp service and are pretty much convinced that, coupled with their particular circumstances, topping up via SMS is the way to go, but want to know how to pay for the TopUps and what 'prepaid prepaid' means exactly.

Lee advises that John or Kristy (or possibly both) will need to sign a Direct Debit Authority (DDA) against their nominated cheque or savings account to pay for TopUps as well as completing the Registration Form as part of the registration process. Mark of course has his own bank account and can sign both forms for himself.

Customer Terms and Conditions

Lee takes them through the terms and conditions for using TopItUp. They understand:-

- that (like a contract handset) they are paying an upfront payment for the prepaid prepaid (initial) voucher (the TopUp Voucher value which is currently $30) to gain these benefits, however, the payment of this amount is a pre-purchase entitlement to something they own (being an entitlement to a TopUp Voucher for prepaid handset credits) and not a fee (unlike a contract);
- that by completing the Direct Debit Authority they authorise TopItUp to deduct the value of a TopUp Voucher from the nominated bank account to Register and whenever they Request a TopUp and that this authority applies if they were to order other products (such as ring tones) using TopItUp;
- that they agree to notify TopItUp promptly by phoning Customer Care if there are any changes to their financial institution account details;
- that there are sufficient funds in their account to cover the cost of the TopUp Voucher whenever they 'Request a TopUp' using TopItUp and that they are aware that their bank will charge them hefty fees if they don't have sufficient available funds;
- that an account will require up to three business days to pass between Requesting a TopUp to allow time for their funds to clear;
- that the personal information (including their bank account information) they provide to TopItUp when they register is secure and will remain private being used to allow TopItUp and any of its support agencies to conduct their account. The personal information will not be provided to or be used by any other organisation for marketing or any other purposes not specifically relating to the conduct of their account;
- that if they tick the 'Send Info Box', that they are giving their permission to TopItUp to send them SMSs from time to time to advise them of new services available with TopItUp;
- that they agree to keep their Password private. They should understand that giving someone their Password is akin to giving someone the PIN to their keycard account.
- that they pay for the cost of the SMS when they order a TopUp Voucher and that if they ring the Customer Care number on their mobile they will pay the standard mobile fee for a local call to an Optus 1300 number for each call;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 232 of 1360

- that TopItUp, at their discretion, may elect to close the Account.
- that should they decide to close their Account that TopItUp will SMS a final TopUp Voucher to their handset as long as
    - they have a pre-paid entitlement to a TopUp Voucher and;
    - their account does not have any bad debt provisions associated with the final TopUp Voucher.

Completing the Registration Form

Mark is going to signup with TopItUp on his own behalf. Lee provides a TopItUp Registration Form and a Direct Debit Authority form for Mark to complete. Mark's mobile handset number will be his account number. The T&Cs include a requirement that Mark agrees to have more than $30 (being the current TopUp value) available in his account whenever he Requests a TopUp. Mark understands that when he does Register, TopItUp is going to deduct $30 from his bank account that night and set this amount aside as a TopUp Voucher the next time he Requests a TopUp using TopItUp. Mark knows he has sufficient funds to cover the initial $30 Draw Down. Mark also thinks of a great password to protect his account. Since Mark is managing his own account, the Account Holder Name is entered as Mark Evans and the User Name is entered as Mark Evans. He writes this on the form for registration purposes with the knowledge that once it is entered into the system, he is the only person who can access his TopItUp account. Mark also wants to get ringtones for his handset, so he ticks the 'Send Info Box' that gives TopItUp permission to send information using SMSs when new services or specials are available to him.

Completing the Direct Debit Authority

Mark doesn't know his Direct Debit bank details. He does have his keycard with him. Lee has a current list of bank information handset numbers that allows him to quickly rings the bank's information number associated with the Mark's keycard and hands the handset over to Mark to get the details from his bank. Lee knows that recording this information is a very important step to get right so that the TopItUp registration process is not delayed. Mark selects 'Savings or Cheque' account option. Mark signs the Registration Form and the Direct Debit Authority Form thereby completing the instore registration process.

Kristy checks the credit balance on Matt's handset and finds that he has been more frugal than either Mark or herself. Matt has an available credit of $23.70. Lee explains that Kristy can manage Matt's account under her control. The Account Holder Name is entered as Kristy Evans and the User Name is entered as Matt Evans. She registers Matt's TopItUp account using all her other details including the direct debit authority with the debit card details of her own combined credit/debit card account details. Unlike Mark, Kristy does know her bank details as she makes payments to the electricity account using bPay. She does not want Mark getting ring tones or other promotion, so the 'Send Info Box' on the registration form is not ticked. She also picks a password that Matt or Mark cannot easily guess and signs the Registration Form and the Direct Debit Authority Form.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 233 of 1360

Kristy registers her own handset with the TopItUp Service. She enters her own name as the Account Holder and the User Name. She ticks the 'Send Info Box' keen to know about how to get the Bridge Over Troubled Waters ringtone that rings on Joanne's handset.

TopItUp User Guide

Lee also gives all three users a 'TopItUp User Guide' and explains each of the basic steps.

He programs the 'TOPUPS' number (0412 876877 or 0412 TOPUPS) into each of their handsets and makes sure Mark and Kristy know how to send an SMS with their Password to the 'TOPUPS' number as shown in the User Guide. He also tells them if they get into trouble to ring the 1300 TopItUp Customer Care number (**1300 300 482**) and also enters this number into the address book of their handsets.

Wait for Welcome Message SMS

Lee explains that they have to wait to get a notification by SMS from TopItUp before they can access their first TopUp Voucher. This is usually sent by TopItUp within 2 full business days. Business days do not include National Public Holidays. It is already well past the 4pm processing cutoff, which means that the Accounts may not be registered until Tuesday afternoon at the latest. If they had been in before 4pm, they would have made the daily cutoff and be registered before Monday afternoon.

The last thing Lee always does is to remind the customer that they will receive a Welcoming Message by SMS when they are registered which lets them know they can start to use TopItUp. He asks them not to send any Requests for a TopUp until they get the Welcome Message.

The Evans go home wrapped thanking Lee for all his help and knowing that they now have both control and the anywhere convenience that TopItUp provides.

John asks whether he could use his Master Card instead. Lee says 'no' as the service has been built around the overwhelming majority of prepaid users who are not credit card holders, and is the only way a prepaid user can avail themselves of the service. Besides, the merchant fees at the moment are too expensive. But he reassures John that in the future this payment method would most likely be available.

So what about the 'prepaid prepaid' part asks Kristy? Lee says that the TopItUp service is just like many other services people have where they pay in advance for the use of or access to that service. He puts it in terms of 'rental' fees as this is what most people understand about account services. Lee cites examples such as Telstra's monthly fixed-line access fees, electricity accounts, and Kristy's current Telstra mobile account which is just like Optus' contract mobile handset users who pay in advance and use up the access fee in included calls. Lee explains that TopItUp is different and better as the prepayment is actually for calls you can use and not a rental or access fee. In fact, he says, TopItUp charges no joining, ongoing or rental/access fees whatsoever.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 234 of 1360

Lee explains further that direct debits can take upto three business days to transfer the funds from their account to TopItUp. Once the funds are cleared, a TopUp can be ordered immediately requesting it by SMS. This starts the order process for the replacement TopUp which in turn will take upto three business days to transfer clear funds during which time another TopUp can not be ordered. John asks if they can get $50 vouchers. Lee explains the only vouchers that are issued are the $30 ones as there is no benefit to the customer to pay more if they can order when they need them.

Lee also explains the section in the User Guide that warns about having sufficient funds in the nominated bank account to cover the cost of the TopUp and points out that the banks will charge hefty funds if the account is overdrawn which will in turn delay delivery of the replacement TopUp. He puts forward the case that by prepaying now all subsequent payments can naturally be budgeted as spending with only monies you currently have available in your account.

This makes sense to Kristy and John, and, as they weren't sure how much they were going to spend on prepaid handsets today. They are happy to sign up.

Lee pulls out the Direct Debit Authority and Registration Form while asking for a copy of a driver's licence or best available ID. He photocopies the ID and commences to fill out the Registration Form first using that information to fulfil Optus' requirement for new customers connecting new or additional prepaid services. Lee is sure to complete every field in the Registration Form accurately and legibly knowing that the process demands the same attention to detail and integrity as do postpaid connections. He doesn't want to lose any revenue possibilities due to sloppy work .

Lee explains Kristy and Mark the importance of not providing your password to any other person. Kristy chooses a 4 to 6 character password for her own account and a separate one for Matt's account. Passwords should be letters and numbers and should not be whole words, such as FIDO, which are easy to guess. They can be typed in upper or lower case. The relevant password is written onto each of the Registration Form.

Once finished with the Registration Form, Lee now turns his attention to the Direct Debit Authority. John and Kristy have a joint bank account which they decided to provide the authority against. They state it's a savings account. Lee asks them first whether they have the BSB and account number for this bank account leaving the account name details to later. He's prudent enough to ask whether they have a cheque book just in case, as it would have all the necessary details.

They indicate that they don't have a cheque book for this account and don't know such details. Lee is not phased and simply asks for their financial institution's name and branch. They indicate that they are members of the Hornsby Teachers Credit Union as John has his wages paid into this account. As this is not one of the major financial institutions such as Westpac, CBA, ANZ or NAB and is not in the Wollongong telehandset directory area, Lee quickly goes to the web to access the contact handset number for the Credit Union. He

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 235 of 1360

keeps a couple of browser applications open on his desktop, one of which is the WhitePages online website www.whitepages.com.au . He quickly types in the information he has into the appropriate fields and clicks 'search'. He checks with John that he has the correct institution and address and rings the number indicated. He hears the recorded message and realises that it is Saturday and that the credit union is closed until Monday.

Lee is not phased as he has secured John and Kristy's trust and they agree to sign the paperwork now and on Monday, Lee will ring John or Kristy for the BSB and Account Number details. Before the Evan's leave, he programs the TopItUp SMS Request Number (0417 866877) into each handset and stores it on their HandsetBook directories under the name TopItUp and makes sure they now how to send an SMS with their password to order a TopUp. He also programs the TopItUp Customer Care Number into their handsets.

Lee explains to them that once he has the bank account details and a successful debit of their account has occurred a Welcome Message with their password will appear on their handsets. Then, when they're ready to TopUp, use the TopItUp number stored in their handset to send the SMS containing their Password. He points out that the User Guide details all this but nevertheless if they have any problems to contact the Customer Care number.

After registering their handsets with Optus prepaid services, the boys are sending SMSs to each other that afternoon and to their friends. On Wednesday afternoon, Mark finds out that he can't make calls as he has run out of credit. As soon as he gets home, he rings Kristy at work and explains his problem.

Problem alright .... Kristy is not impressed. It's Mark's birthday tomorrow and he's spent $30 in four days. He needs to be taught a lesson but it is his birthday tomorrow. Kristy rings '555' to find out that she has $8 credit (after all, she did have to ring all her friends to tell them about her new mobile.) She didn't think she'd used so much. She's afraid to check Matt's handset. She rings John at work. John is not impressed either. John leaves for work early and gets home late. He doesn't know where to get TopUpand even if he did, he'd have to leave work 10 minutes early to get them and might miss his train. The milk bar near the railway station isn't open when he gets home. Disaster - Mark is without credit Wednesday night. He can receive calls so it's not a total disaster. Mark gets up early on his birthday to plead with his parents. They remember that Lee said you could get them just about anywhere and they remember what he said about TopItUp. Back to the store on Thursday night.

John buys Mark another birthday present being a $50 TopUp card over the counter with cash. Mark rings '555' and enters the voucher number purchased into his handset to restore his credit so that he can use his handset immediately.

Lee explains the best way to manage their handsets using TopItUp. The Evan's decide to signup.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 236 of 1360

TopItUp Dealer

Forwarding Registration Forms to TopItUp

Once the Evans family leaves the store, Lee faxes the completed registration and authority forms to TopItUp. Lee then stores the completed forms in a locked cabinet until they are mailed to TopItUp.

Once a week (on Monday), Lee mails last week's originals to TopItUp as required by the TopItUp Dealership Agreement.

Dealer Perspective

Lee is pleased to be able to help the Evan's and at the same time help his own store financially. By taking the extra trouble to mention TopItUp to them when they bought the handsets, they returned to his store when they needed the convenience that TopItUp provides.

Lee signed up his Network Communications dealership to become a TopItUp Dealer to stem the 'leakage' from his store of Prepaid customers. Lee knows leakage is occurring because a large number of the people who buy Starter Kits and Prepaid Handsets from him predominately buy TopUp cards from other outlets for customer convenience reasons.

The Evans were in store for 35 minutes to buy the handsets and 40 minutes to register all three accounts with TopItUp. Taking this extra trouble has made the Evans family valuable prepaid customers providing ongoing revenues of 12.0% to the store. Every time they order a TopUp using TopItUp, Lee gets this commission. Lee knows that the Evans have travelled from Port Kembla and even though he has provided exceptional after sales service, it is highly unlikely that he will see them unless they have a warranty problem or need a new handset. Assuming they are average prepaid users, signing each of them up will bring $43 in ongoing revenues every year which is better than the $6 he receives he would receive without TopItUp if he never sees them again.

True, this commission is not the full margin of an instore voucher but each commission is a payment that would not have occurred if the Evan's had bought elsewhere. Now, even if the Evan's go on holidays, move interstate or go to Australia Post, a service station or newsagent that sells TopUp vouchers, there is no reason they would buy a TopUp voucher from anyone else (unless they wanted a spare voucher).

The store opened just over twelve months ago and the number of vouchers and starter kits sold each month grew for 9 months and is now starting to level off. Whilst Lee knows that his store is capturing a significant

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 237 of 1360

number of sales of prepaid handsets and starter kits sold in Wollongong, he is selling approximately four times this number of TopUps month after month. This means his potential for revenue is 'leaking'.

Lee had been shown figures that if he started selling TopItUp from day one registering just 25% of prepaid customers coming in store he would be able to stop the 'leaking of his prepaid customer base'. Lee knows it is in the best interest of his store to aggressively push TopItUp to every prepaid customer entering his store convinced that the 'Best of Both Worlds' applies not only to customers but to dealers as well.

Other Dealer Opportunities

Lee wonders if he can't use the store promotion code to sign up Marks' local football club after Mark makes a comment about how many of his mates at footy think TopItUp is brilliant.. A lot of the members are juniors, about half of which own prepaid mobiles. Lee thinks, I could approach the Club Committee and offer them a fund raising opportunity. For every person signing up to TopItUp, I could donate $1 of my commission on every TopUp voucher ordered through the club. Lee understands that he is giving away some commission, but he is gaining revenue from an audience that might never enter his store. Better still, some of the people signing up may be Telstra or Vodahandset users.

Mark gets the Secretary of the Club to ring Lee. Andrew had just been working out whether 'its chocolates or cookies' this month as the club fundraiser. When Lee explains that Andrew only needs to have one fundraiser that is ongoing and doesn't take up any of his time, he is enthusiastic. He asks Lee to give him some brochures to present at the next Club meeting and asks 'Would you be prepared to come to the following meeting? Can people go to your store to sign up?'

Lee knows he can produce the payment information from the reports he gets from TopItUp to write ongoing monthly cheques to the Club as the best money raiser they've ever had.

Best of Both Worlds all right thinks Lee for churches and clubs as well..

Dealer Obligations to TopItUp

Lee completed a Dealer Registration Application for a TopItUp Dealer Agreement which includes obligations on the Dealer to honestly represent TopItUp to potential prepaid customers and act with integrity in dealing with TopItUp customers and TopItUp. The Dealer Agreement is renewed annually.

The Dealer Agreement applies obligations on the Dealer to ensure

- that the Dealer prominently displays TopItUp's Privacy Statement and understands his role in the privacy obligations as an agent of TopItUp;
- that the customer's Personal Information is subject to TopItUp's Privacy Statement;
- that the customer understands TopItUps Terms and Conditions;
- that the customer has been adequately walked through the TopItUp User Guide;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 238 of 1360

- that the bank account details provided by the customer are complete and accurate either by witnessing documented evidence provided by the customer or by information provided when the customer handsetd their bank's information line in store;
- that customer Registration and Direct Debit forms are completed accurately, signed and forwarded to TopItUp as required;
- that the customer's handset has been programmed with the TOPUPS number and the TopItUp 'Customer Care Number'.
- that the Dealer has an ABN and invoices TopItUp using this ABN for commissions paid including GST.

TopItUp Obligations to Dealer

The Dealer Agreement applies obligations on TopItP to support the Dealer in the following manner:-

- Dealer Support for Lee is provided by TopItUp. TopItUp provides a Dealer Manager who also performs the role of TopItUp's Privacy Officer. Dealers would handset the Dealer Manager in the first instance for all support issues;
- Dealer is required to display TopItUp branding for the period of the Dealer Agreement;
- Provide up todate collateral and point of sale material to the Dealer ;
- As a dealer, Lee receives commission advises by email daily showing month to date commission and commissions pais in the previous 24 hour period.
- Once a month, TopItUp will provide a Monthly Commissions Report to the Dealer showing all the ongoing transactions processed within that month for that Dealer;
- The Dealer is to invoice this amount (inclusive of GST) and fax/email this invoice to ensure prompt payment and followup with the original invoice in the mail.
- Upon receipt of fax/email, TopItUp will make a monthly commission payment direct to the Dealers bank account.

TopItUp also provides useful management reports to the dealer on a month by month basis in a format that can be imported into an Excel spreadsheet and used for in store sales analysis.

Dealer End of Term

The Dealer Agreement is renewed annually by TopItUp. The Dealer Agreement provides for ongoing commissions to a Dealer from the TopItUp customers signed up by the Dealer for the currency of the agreement.

There are four sets of circumstances under which the Dealer Agreement would or could be cancelled or terminated being:-

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 239 of 1360

- Initiated by Dealer – under these circumstances would normally cease and the customers signed up from the dealer may be reallocated. At the sole discretion of TopItUp, commissions may be continued to be paid to a bank account nominated by the departing dealer;
- Dealer sells dealership – under these circumstances, the new dealer would be allocated a new dealership account (consistent with Optus Dealership code) and the customers associated with the old dealership will be paid to the new dealership. This is achieved by the bank account details of the old dealership being changed to reflect the new dealership bank account details and the new dealership would receive two commission payments (one for the old account number and one for the new account number). The customer base is effectively split over both the old and the new account code. TopItUP will not allow customers to be registered to the old dealer account;
- Initiated by Optus or Network Communications – if the dealer is no longed authorised by Optus Communications or Network Communication to be a dealer, the TopItUp dealership will be automatically terminated;
- Initiated by TopItUp – if the dealership has acted inappropriately in the interests of TopItUp, the dealership will be terminated and ongoing commissions to the dealership will not be recognised.

Back Office Staff Roles

TopItUp is administered and operated by the following staff categories performing roles that provide appropriate security access controls to perform their operational responsibilities:-

- Scheme Operators – perform all the back office registration functions for TopItUp ensuring the completeness and accuracy of information is correctly entered, that the initial 'Draw Down' of funds is completed correctly, that Bad Debts and Bad Bank processing of preRegistered accounts is handled correctly and that Accounts are Activated correctly.
- Scheme Administrators –have full access to all of the operational management functions of the System and perform financial and settlement administration, customer complaint resolution and fraud management of the system.
- Financial Administrator - is responsible for the Financial Management of TopItUp including the financial management of the company with specific responsibilities for internal audits of the System and oversight of payment and settlement functions.
- Customer Care Operator – perform all Call Centre functions for calls received by TopItUp through the 1300 Customer Care number. **(1300 300 482)**
- Dealer Manager – overall responsibility for dealer management including dealer appointments, dealer training, dealer support, complaints resolution and dealer collateral.
- System Administrator – overall responsibility for IT Systems, support, disaster recovery and security.
- Software Support – provided by Fieldware Pty Limited.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 240 of 1360

Staff Type – Scheme Operator

On Friday morning at 9am, Ann makes her first coffee of the day. She is one of TopItUp's Scheme Operators and is responsible for the back office registration functions for TopItUp. Ann knows it is important that she ensures the completeness and accuracy of information is correctly 'Registered' and that the initial 'Draw Down' of funds is completed before Activating the TopItUp Account.

Stopping near the fax machine, Ann draws off the faxes received for the Evans family (amongst others). Ann logs into TopItUp's Backoffice system with access rights to create and update account registration details and to Activate Accounts. Ann creates Accounts for Mark, Matt and Kristy entering their details into the TopItUp backend system. She checks all the paper work carefully. If there any problems, such as a customer not completing all required information or signing either form, she will handset the customer directly. She double enters the Password field and the bank account fields to ensure a system accuracy check of this information.

When Ann has completed the data entry for each Account, she saves the registration details which sets the state of the Account to PreRegistered and will commence the Initial Draw Down process.

Three things will now occur. Either

- The applicant's Initial Draw Down fails because of a declined payment by their bank
- The applicant's Initial Draw Down fails because of a incorrect BSB or account details
- The applicant's Initial Draw Down is settled and the Account is Activated.

SO - Follows up Initial Bad Debt

Ann does the follow up of any Bad Debts associated with new users registering to TopItUp. Ann prints a PreRegistered Payment Exception Report which shows her all accounts that have failed the Initial Draw Down of funds for the reasons of Bad Debts (payment declined) or Bad Bank account details (rejected account details).

The Report is sorted in reverse date order so Ann can start at the top of the Report and find the Accounts that have failed activation most recently. Ann knows it is important to keep the customers confidence and that this hiccup, if overcome, will ensure the highest rate of ongoing customer satisfaction with minimal cost impact to the customer and TopItUp.

Ann will handset the Account Holder directly advising them of the payment decline or bad bank details. Ann informs them that their account cannot be activated until the payment can be cleared or the bank account details made accurate.

If there has been a payment decline (indicated by TopItUp declaring the state of the Account as PreRegistered_BadDebt), Ann will also inform them that their bank will charge them a dishonour fee. Ann

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 241 of 1360

asks them to handset the TopItUp Customer Care number when sufficient funds haven been deposited to cover the TopUp Voucher and the dishonour fee from the account holder's bank. Summary notes are entered against the Account. No other action is taken until the Account Holder handsets back. The payment process is then repeated. If the payment is declined a second time, in most circumstances, the Account would be cancelled by an Scheme Administrator. TopItUp absorbs the merchant dishonour fee of $2.50.

SO - Follows up Initial Bad Bank

If their BSB or bank details have not registered (usually notified on the first overnight settlement and indicated by TopItUp declaring the state of the Account as PreRegistered_BadBank), Ann will handset the Account Holder explaining what has happened and ask for them to fax details of their bank account details (eg a current statement) to TopItUp to allow their correct bank details to be entered. Summary notes are entered against the account. No other action is taken until the Account Holder faxes the details.

When the fax is received, Ann will file the proof of account faxed by the account holder with their registration forms and update the Account with the correct bank accoiunt details and set the state of the account to PreRegistered which will restart the Initial Draw Down..

SO - Initial Draw Down is Settled

TopItUp performs automatic settlement (with provision of manual override) of settlement of Draw Downs after a maximum of two business days.

If an Account has not failed the Initial Draw Down by either of the above reason, TopItUp will automatically Activate their Account which will automatically generates a Welcome Message to the Account handset, allocate an entitlement to a TopUp Voucher (known as a PIN by transferring an unallocated PINs to the Allocated PIN Pool associated with the Account Holder's Account. As part of the end of day settlement process, a commission notification email is sent to the dealer known as a Daily Dealer Commission Notification associated with the Account notifying them the Account has been Activated and notifying them of their commission entitlement. The Notification also details the settlement transaction details including the name, account number and the commission amount and customer activity (registration activation or top up).

Staff Type - Scheme Administrator

Joe is a Scheme Administrator for TopItUp. He has full access to all of the operational management functions of the System and performs

- customer complaint resolution
- operational fraud management of the system
- cancelling customer accounts associated that are not initiated by the Account Holder
- acquirer bank settlement functions including
    - preparing Bank Bulk Funds Movement files
    - receives Bank Settlement Files

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 242 of 1360

- manual oversight of closing open settlement batches as required

SA - Morning Settlement

Each morning, Joe accesses the TopItUp's online bank account from its acquiring bank and exports this information to a Bank Settlement File. The Bank Settlement File shows all batches that were Closed and those that remain Open from the previous evening's settlement by the acquiring bank

TopItUp performs a sophisticated clearing process whenever an Scheme Administrator runs the Process Account Statement option. Batches are either Open or Closed.

When a batch is Closed, TopItUp knows that every customer transaction in the batch has been accounted for as either cleared (payment received), not cleared (a bad debt) or not processed (a bad bank) by the acquiring bank.

Settlement Batches processed by TopItUp's acquiring bank Joe then imports the Bank Settlement file into TopItUp and runs the 'Process Account Statements' option. This option processes all reports and updates the Account as a result of the Settlement process.

SA - Afternoon Preparation

TopItUp's acquiring bank has a 5pm close off. Joe runs the Prepare Bulk Funds Movement File option which prepares a file to be uploaded to the acquirer bank. This option will include all Draw Downs that have been generated since the option was last run. The file breaks the Draw Downs into settlement batches of 100 (configurable) entries per batch.

Joe uses application software provided by the acquirer bank to upload the Bulk Funds Movement File.

Staff Type – Financial Administrator

Morgan is the Financial Administrator for TopItUp. He is responsible for the Financial Management of TopItUp including the financial management of the company with specific responsibilities for internal audits of TopItUp and oversight of payment and settlement functions. He is also responsible for authorising and purchase order approval for TopItUp to order additional PINs to replenish the Unallocated Pool with replacement TopUp vouchers from the voucher supplier when the Unallocated Pool quantities fall below the just in time re-order point.

Staff Type - Customer Care

Craig is a Customer Care Agent and works in TopItUp's call centre. Craig is trained in handling most customer scenarios and will only pass a call onto an Scheme Administrator in the event of a Customer Compliant.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 243 of 1360

Craig knows the importance of identifying the Account Holder or the Account User as appropriate.

Craig normally accesses and Account by the Account Number being the mobile handset number associated with the Account. Craig can access also an Account Holders details by a surname search against the Registration Database and further qualification of the Account Holder.

Whenever Craig takes a call from a customer, he is aware of TopItUp's obligation for confidentiality of the Account Holder's private information.

Craig will type a record of the conversation which is attached to the Account and is known as a 'File Note'. File Notes are date and time stamped and identify the Customer Care Agent and record an outcome for the interaction with the caller.

Back Office Scenarios

Applicant Fails Registration

Mark is not having much luck. On the following Monday, Mark's name appears as declined on the PreRegistered Payment Exception Report as a declined payment. Ann rings him and requests that he checks why his payment is declined. Ann asks him to ring back on the TopItUp Customer Care 1300 Number when he has deposited sufficient funds to clear the bank decline fee and the amount of the TopUp Voucher. Ann gives him a call log number to quote that is generated from her system and types in details of their conversation.

Mark is embarrassed and thanks Ann for letting him know. He has not decided whether to tell his mum or forget about TopItUp. Mark eventually tells Kristy.

If Ann hadn't been able to contact him, she would have sent an SMS to Mark asking him to call Customer Care and quote the call log number. TopItUp has already changed the processing state of Mark's account from 'PreRegistered' to 'PreRegistered_BadDebt'. Changing the processing state to PreRegistered_BadDebt means that whenever an Scheme Adminstrator (such as Joe) or an Scheme Operator (such as Ann) runs the PreRegistered Payment Exception Report, Mark's name will appear. At some point in time, Joe would assess this account is not likely ever to be registered and Cancel the account by changing the state of the account to 'Cancelled'. Ann (being an Scheme Operator) does not have access to perform this function.

Applicant is Activated

On the Tuesday morning, Kristy and Matt's accounts are Activated. This means that $60 was drawn down from Kristy's bank account on Friday night has cleared and that A 'TopUp Voucher entitlement has been automatically allocated to both accounts.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 244 of 1360

Customer gets a Welcoming Message to TopItUp

When TopItUp Activates Kristy and Matt's accounts, TopItUp sends a Welcoming Message to both handsets stating "Welcome to TopItUp. You can now Request a TopUp. Thank you for using TopItUp"

Dealer Commission Advise

The commission advise for Kristy and Matt's initial TopUp is automatically processed at the end of day settlement run on Tuesday and a settlement advise is generated and emailed to Lee showing details of the commission and the activities that generated the income.

Lee rings Kristy after seeing that Kritsy and Matt have been Activated on his report. He asks if she has any questions. Kristy thanks Lee and says she will recommend TopItUp to her friends.

Need Sufficient Funds to Re Register

When Kristy gets her SMS notifying her that her account has been activated, she remembers about Mark's decline. She was going to let Mark stew until he could fix his bank account balance. She rings John and they agree to cover Mark's funds and John deposits the required funds into Mark's bank account using internet banking.

When Matt gets his Welcome SMS, he rings '555' to check his account balance to see if he needs to use TopItUp. He then remembers that he can't use the service as he doesn't know the Password. He thinks 'maybe I can get mum to tell me'.

Kristy then rings Matt to see if he received a Welcome SMS as well. Matt asks for the Password but Kristy tells him to wait at least 6 months until he proves that he can be trusted. Matt straight away blames Mark for creating problems himself without understanding that if Kristy gives him the Password, he has open slather on Kristy's bank account.

John rings Mark to tell him that he deposited the required funds into his account to try to reactivate his account with TopItUp. Mark thinks this is brilliant news, he has almost run out of credit. John also tells Mark that once he is registered, that he cannot request a TopUp Voucher until Mark has deposited sufficient funds to cover the bank fee and the TopUp Voucher into his bank account. This is not good news for Mark.

Mark Calls Customer Care

When Mark gets home from school, he rings the TopItUp Customer Care number using the home handset. Craig is a Customer Care Agent and works in TopItUp's call centre. Craig is trained in handling most customer scenarios and will only pass a call onto an Scheme Administrator in the event of a Customer Compliant.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 245 of 1360

Craig takes Mark's call asking for Marks handset number. Craig accesses Mark's account. Craig then asks for his name, current address and date of birth. Craig verifies that Mark is the Account Holder. Craig also sees from the file note that Mark's account is 'PreRegistered_BadDebt'.

Craig asks how he can help. Mark says that he has put money into his bank account as requested and can you try to activate my account please? Craig explains that this is the second attempt at registration and that since it is Wednesday, expect a Welcome SMS on Friday saying that the account has been activated. Mark agrees and Craig enters a File Note and changes the state of the account from PreRegistered_BadDebt to PreRegistered.

Craig asks if there is anything else he can do to help. Mark says no and rings off.

Mark's Account is Ready for Second Registration Attempt

When Joe runs the Create Bulk Funds Movement File option at 4:30 pm that day, Mark's second attempt at registering with TopItUp is included in one of the settlement batches uploaded to the acquirer bank. On Friday morning, the batch that contains Mark's settlement is Closed, TopItUp determines that Mark's funds have cleared and Mark's Account is Activated by TopItUp. Like Kristy and Matt one week before, Mark now receives an SMS welcoming him to TopItUp and his entitlement to a PIN is made.

Other Registration Problems – Account Number is Not Accurate

In this scenario, the Customer's handset number (their account number) is not registered accurately. This could be caused by the number not being recorded accurately on the registration form or incorrectly entered into the Schemes database when registering. The chance of the second reason is minimised as the SO is required to re-enter the account number to verify the entry.

In either case, the fact that the account number is not recorded correctly is a problem as the Customer will not receive a 'Welcome Message' to the scheme as the SMS will be sent to another prepaid mobile number.

The following scenarios may occur:-

- If the incorrect mobile number is not registered on the carrier's network, the System will know something has gone wrong and the System will generate an exception report to be investigated by an SO. A letter may need to be sent to the Account Holder requesting the Account Holder to ring an SO direct and not Customer Care.
- If the number is registered on the carrier's network, the Welcoming Message will be sent to another mobile handset. This certainly presents a problem. TopItUp believes the account is registered and the Account User is still awaiting their Welcome Message. This registration will remain in an error state until the customer eventually rings Customer Care who do not have a record of the account number being quoted by the customer. Customer Care will need to locate the account using search features and referring the matter to an SA.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 246 of 1360

Other Registration Problems – Account Number is Reissued by Carrier

In this scenario, the Customer's handset number (their account number) has been reissued by the carrier after the number has been cancelled and quarantined by the carrier. This presents a problem if the previous user was also registered with the Scheme as an account associated with that number exists in the System.

When the SO attempts to register the new account, the SO will be aware the old account exists and will alloacate a two digit suffix (starting with '00') to the old account number. This action will identify the old account as superceded yet still tied to the old account number and then allow the new account to be established.

TopUp Scenarios

Kristy Requests a TopUp for Her Account

Later that month, Kristy decides to Request a TopUp. She goes to the SMS messaging area on her handset and writes an SMS containing her Password only. She finds the number for TopItUp that Lee saved on her handset and sends the SMS. *She remembers that Lee had asked her to delete the sent SMS from her handset for security reasons and does so.*

The TopItUp system receives her request and processes the request within a minute of the SMS being received. Processing the request will select the oldest PIN activation date from the $30 Optus TopUp Pool and sends that PIN as the TopUp Voucher using an SMS to Kristy's mobile handset. If the Reward System is running, Kristy would also get an acknowledgement of the Reward Points due.

Kristy gets her TopUp Voucher from TopItUp

Kristy remembers that Lee had told her that the TopUp process in most instances is pretty much immediate. He pointed out to her in the User Guide that if there were problems with the SMS network, such as network congestion or coverage for her handset, delivery will be delayed. If she hasn't received the TopUp Voucher within the hour, she should send another SMS to re-request the voucher.

Kristy receives an SMS with her TopUp Voucher within two minutes. When she reads the SMS, the message is "Your TopUp Voucher is 1234567890. You have 25 TopUp Points. Thank you for using TopItUp". She reads the SMS and writes down the TopUp Voucher number. She rings '555' and enters her TopUp Voucher as if she had purchased it from a store.

TopItUp starts a Draw Down on Kristys' Bank

TopItUp will then start the Draw Down process on Kristy's bank account for a replacement voucher. TopItUp automatically changes Kristy's account state from Active to Pending. Overnight, TopItUp requests the Draw Down from Kristy's bank. At the completion of At the same time that TopItUp will automatically

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 247 of 1360

change the state of Kristy's account from Active to Pending, meaning that TopItUp has started a Draw Down process of additional funds from Kristy's bank account.

Clearing is performed by exception. Unless the account is declared a Bad Debt, after two business days, it is assumed the payment has been cleared which will change the state of the account to Active and a PIN is transferred from the unallocated PIN pool to the $30 Optus allocated PIN pool. This completes the Draw Down.

Kristy Knows Not to Send Multiple Requests

The User Guide also points out to Kristy that if she was to resend the Request a TopUp within 24 hours of her first request, TopItUp will send back the same PIN that was sent on the first request plus a message saying this is the second notification.

This allows the user to get the TopUp Voucher again if they didn't receive it, were too impatient or lost the number before entering it into the handset.

A third request will likewise resend the TopUp Voucher. The SMS to the customer indicating this is the third and final transmission of the same PIN.

TopItUp will not send any further SMSs and will effectively ignore any further SMS received from the account until the funds have been drawn down and a new TopUp Voucher is available to be requested. If the customer handsets Customer Care, the system will provide sufficient information to allow the Customer Care Operator to explain the state of their account.

User Problems - Bad Attempts

'Bad Attempts' are attempts to Request a TopUp that cannot be processed by TopItUp for whatever reason. They can occur by accident or could be the result of a fraud attempt.

In the following scenarios that generate Bad Attempts, TopItUp always writes the full contents of any SMS received that generates a 'Bad Attempt' to the 'Potential Fraud Log File' in the event that fraud is being attempted on the system.

In some of the scenarios listed, the account will be flagged as 'Blocked' which means that TopItUp will not issue TopUp Vouchers to a Request a TopUp from the account, nor will TopItUp send other SMSs to the account. Blocking an account does not stop TopItUp's automatic processing of account states. performed by TopItUp in Accounts can only be 'Unblocked' by an Scheme Adminstrator.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 248 of 1360

Matt attempts to guess the Password

Matt attempts to Request a TopUp guessing the Password that Kristy created for his handset. He types in their dog's name as the password and sends the SMS to TopItUp using his handset.

When TopItUp receives the SMS, the system verifies Matt's account is is registered with TopItUp but the Password sent does not match the entry in the TopItUp database. TopItUp sends an SMS to Matt's handset which informs the user "Bad attempt, your Password is not correct. If you get it wrong again, call 1300 TOPUPS". *The state of the account is 'Active'.*

Matt panics. He calls 1300 TOPUPS on his mobile. He speaks to George from the TopItUp Customer Care Centre. George asks how he can help. Matt says that he has forgotten his Password, can you help. George asks for the Caller's name. Matt gives his name. Other questions would normally follow but George notices that Matt is the Account User and not the Account Holder. George informs Matt that the Account Holder (without identifying the Account Holders name) must contact TopItUp in person. A record of conversation is made.

Matt is not one to give up easy, maybe the Password is Kristy's favourite colour. He's not sure what to do. If he gives up and Kristy performs the next TopUp Voucher on Matt's behalf and gets the Password correct, the Bad Attempt logic is broken and the account will operate as normal.

Matt decides to risk it two days later. Even though two days has passed, TopItUp remembers his first bad attempt. He enters the Password as 'blue' and sends his second SMS attempt to crack the Kristy's Password to TopItUp. When TopItUp cannot validate the password on the second attempt, TopItUp assumes fraud and flags this account as 'Blocked'.

Two Bad Attempts are allowed before the account is automatically Blocked. One SMS is sent in response to the first Bad Attempt. This must be dealt with by an Scheme Adminstrator.

The Result is Matt's Account is Blocked

When an account is Blocked, no further TopUp Vouchers or SMSs will be sent to the account handset and all SMSs received are written to the 'Potential Fraud Log File'

Matt does not tell Kristy he has attempted to crack her Password. A Customer Care Operator accepting a call from an Account Holder with a blocked account will forward the call to an Scheme Administrator who determines whether a fraudulent attempt has been made to access PINs.

Kristy makes two attempts to request a TopUp Voucher without receiving any replies from TopItUp. Eventually Kristy calls Customer Care to report the problem. Kristy is passed through to Joe who determines that Kristy is the Account Holder by asking her personal details and verbally verifying her Password. Joe

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 249 of 1360

informs her that there have been three recent attempts to request with bad passwords followed by two attempts with correct passwords giving her the date and times. Kristy verifies the two most recent attempts were hers. She is horrified when Joe tells her that a caller identifying themself as Matt had handsetd to ask for the Password.

Joe is satisfied that while a fraudulent activity has occurred, that it will remain in the family and that the account can be Acivated which he does. He records the converstion against the account. Kristy can now request a TopUp Voucher.

Unregistered user attempts to use TopItUp

Greg (Mark's friend) tells his father about TopItUp. Greg hasn't been to a Network Store. His dad had just bought him a Optus Prepaid Starter Kit from the Post Office. Greg has seen Mark request a TopUp Voucher. He puts his PrePaid Sim into his father's handset and sends an SMS to TopItUp's SMS number using Mark's Password. He knows Mark's Password, after all Mark had been told not to give out his Password, but, after all, Greg is his best mate.

When TopItUp gets his SMS, TopItUp does not have an account for the Greg's mobile number and sends back an SMS to Greg's handset informing him "You must Register your handset to use TopItUp at your nearest Network Store or ring 1300 TOPUPS". TopItUp records his handset number in case he decides to send additional requests before Registering with TopItUp. If any subsequent SMSs are sent by Greg, TopItUp will write these attempts to the 'Potential Fraud Log File' to be investigated by an Account Administrator for potential fraud. No further SMSs are sent by TopItUp.

Greg goes to a Network Store and signs up to TopItUp. When his account is Registered on TopItUp's Customer Base, any logic that TopItUp used in dealing with Unregistered Attempts made previously by Greg is broken and Greg's account is conducted normally.

One Bad Attempt is allowed by a user attempting to use an Unregistered Handset. One SMS is sent as a response to the first Bad Attempt. Subsequent SMS received from the same handset are automatically logged to the 'Potential Fraud Log File'. TopItUp will also create an entry for the mobile used to initiate the SMS in the 'unregistered handset database' maintained by TopItUp and will maintain logic regarding additional 'Bad Attempts' from this handset.

Any Mobile Scenarios

'Any Mobile' is an advance feature that allows a TopItUp user to use any other mobile to send an SMS to TopItUp to request a TopUp in the event that the user's handset does not have sufficient credit to send an SMS. TopItUp requires that any mobile that sends a Request a TopUp to TopItUp is to have the handset setting for 'Caller ID' to be switched ON. This applies to Any Mobile scenarios as well.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 250 of 1360

Kristy sends a TopUp Voucher to Matt using 'Any Mobile'

There are two ways Kristy can use TopItUp to provide a TopUp Voucher to Matt.

The first method requires Matt to give Kristy his handset. Normally, Kristy would TopUp Matt's handset for him by simply grabbing his handset and sending a TopUp request using the password she created for Mark, sending the SMS and deleting the sent SMS from Matt's handset.

However, Matt has gone to camp and Kristy cannot access his handset. Matt is still trying to work out how he can get the password to his TopItUp account. He rings Kristy asking Kristy to provide the password so that he can TopUp his handset himself. Kristy remembers that the TopItUp User Guide explains how she can send a TopUp Voucher using the 'Any Mobile' feature of TopItUp to Matt without having access to his handset. The User Guide says "Type in the Password, then a space and then the TopItUp Account Number eg 'PASS 0412123456' ". Kristy writes an SMS on her handset. She types in Matt's password followed by a space followed by Matt's mobile handset number. She sends the SMS. The User Guide informs Kristy that she has a maximum of two tries to use 'Any Mobile', so she is careful to make sure the Password and Matt's Mobile Number are correct and are separated by a space.

When TopItUp receives her request, it reads the password supplied and verifies the password against the 10 digit handset number following the space. *Any additional spaces entered in the handset number are ignored.* They match, so TopItUp sends an SMS to Matt's handset with the TopUp Voucher as if the request were sent from Matt's handset. Matt reads the SMS and enters the TopUp Voucher number after calling '555'. Meanwhile, TopItUp places Matt's account as pending and starts the Draw Down on the bank account details provided by Kristy (as the account holder) when she registered Matt's handset.

Mark runs out of Credit and uses 'Any Mobile'

Mark has gone out on Friday night and is using his handset to contact friends deciding where to go. He dials Jenny, he hears a prerecorded message telling him to TopUp before making this call. He tries to send an SMS and finds the same problem. He remembers that he can he can still use TopItUp if he can get a friend to allow him to use their handset to send an SMS. Greg has his dad's mobile which uses a Telstra postpaid account . Mark uses Greg's mobile to send an SMS to TopItUp. Mark punches in his Password followed by a space followed by his handset number. He sends the SMS. However, his Password is not correct.

Bad Attempts Using 'Any Mobile'

For security reasons, when TopItUp checks the password against the account number provided in the SMS (sent as Mark's handset number), TopItUp sends an SMS to Mark's handset informing him "This is your first attempt using 'Any Mobile' and the password entered is incorrect". TopItUp also writes an entry into Mark is excited when his mobile gets the SMS from TopItUp. He reads the SMS and is dismayed that the Password he entered is wrong.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 251 of 1360

Mark forms another SMS on Greg's handset and tries again. This time when TopItUp receives the second request it knows this is the second attempt using 'Any Mobile' from the same handset. Mark gets the Password right but gets his own handset number wrong by missing one of the digits. When TopItUp received the SMS it can't find a match for the account number to verify the password. TopItUp registers this is the second bad attempt from the same 'Any Mobile' handset. Only two attempts are allowed using the 'Any Mobile' feature from the same handset. TopItUp will not respond by sending an SMS on the second attempt or subsequent attempts from the same handset and writes the details of all attempts from the same handset using the 'Any Mobile' feature to a logfile that is reviewed by Joe or another Scheme Administrator as a potential fraud attempt or a denial of service attack.

Had Mark not entered his handset number correctly on the first attempt, TopItUp would have sent the notification SMS to Greg's handset as the Account Number could not be verified. The SMS sent would inform him "This is your first attempt using 'Any Mobile' and the Handset Number entered is incorrect."

Mark is out of luck again unless he uses another friends handset or a TopUp voucher from a store.

Two Bad Attempts are allowed by a user attempting to use 'Any Mobile' using the same mobile handset. One SMS is sent as a response to the first Bad Attempt. Subsequent SMS received from the same handset are automatically logged to the 'potential fraud log file'. TopItUp will also create an entry for the mobile used to initiate the SMS in the 'unrgeistered handset database' maintained by TopItUp and will maintain logic regarding additional 'bad attempts' from this handset. Since the bad attempts do not originate from the account holders handset, it is not appropriate to Block the account.

Account Holder wants to Close Account

Closing an account by a customer request involves the Account Holder calling a Customer Care Officer who has the authority to close the Account requiring the Account Holder to supply the Password to verify the action. Once the Account is Cancelled any additional SMSs sent to TopItUp for this account are logged in the 'Potential Fraud Log File' and no other action is taken by TIU. TIU retains all transactions and file notes associated with Cancelled Accounts for database integrity reasons but only an SA and an FA can view the Personal Information.

If a CCO receives a call from someone claiming to be the Account Holder of a Cancelled Account, the CCO can only verify that the Account Holders name, the Account Number and the fact that the Account was closed on a specific date. Only an SA or an FA can reactivate a Cancelled Account.
The following scenarios apply to an Account Holder closing an Account.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 252 of 1360

Active Account is Cancelled – Send TopUp by SMS

Matt keeps bugging Kristy for her Password. Kristy thinks enough is enough and decides to close Matt's account. She rings George at Customer Care. After George has identified Kristy as the Account Holder to Matt's Account, Kristy asks George to close the account. *Had Matt handsetd and tried to close the account, George would have identified Matt as the Account User and told Matt that only the Account Holder can close the account.*

As a CCO, George through five steps to close the account.

- STEP 1 - He asks Kristy for her Password and enters it into the 'Confirm Password Entry' box on his screen. *The Confirm Password Entry box must be completed successfully for a CCO to either change the Password on an Account or to Cancel an Account.*

- STEP 2 - George asks Kristy if she doesn't mind telling him why she is cancelling the account. George has a number of codes that summarise why an Account may be closed which are

Code	Reason for closing account
1.	Customer doesn't need the service anymore
2.	Customer handset has been stolen
3.	Customer dissatisfied with service – delivery of TopUps
4.	Customer dissatisfied with service – bad encounter with dealer
5.	Customer dissatisfied with service – bad encounter customer service
6.	Customer dissatisfied with service – problem with bank
7.	Customer – other eg privacy, security concerns
8.	TIU SA - Customer has attempted to defraud system
9.	TIU SA - Customer has incurred too many bad debts
10.	TIU SA – Customer is PreRegistered_BadDebt for too long
11.	TIU SA – Customer is PreRegistered_BadBank for too long
12.	TIU SA – Customer's account considered dormant
13.	TIU SA - Other

When Kristy explains, George sees this as a customer who has security concerns and enters a Code 7 with the file note. *George only gets to see Reasons 1 to 6 on his entry screen as they all relate to customer initiated reasons for closing the account. An Scheme Administrator would use Codes 8 to12 only to Cancel an Account.*

- STEP 3 - George checks the State of the Account to determine the Account Holders entitlement to a TopUp Voucher. George can only issue a TopUp Voucher immediately if the State of the Account is Active. The State is Active, so George knows Kristy is entitled to a TopUp Voucher and informs

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 253 of 1360

Kristy of her entitlement and that TopItUp will SMS the TopUp Voucher to Matt's mobile. Kristy agrees, so George Cancels the Account using the 'Cancel with SMS Option' which changes the State of the Account to Cancelled, SMSs the TopUp Voucher to the Account's Mobile with the message "You have requested your account be closed. Your final $30 TopUp Voucher is 1234567890. Thank you for using TopItUp. You can rejoin" and removes Kristy's entitlement of the TopUp Voucher from the allocated $30 pool.

- STEP 4 - George tells Kristy the TopUp Voucher is on its way and that should she desire to reactivate the Account, please handset Customer Care. Thank you for using TopItUp.

- STEP 5 – Kristy receives her TopUp Voucher entitlement by SMS. Any additional SMSs sent to TopItUp are logged in the 'Potential Fraud Log File' and no other action is taken by TIU.

Active Account is Cancelled – Send TopUp by Mail

Had the State of Kristy's Account been Active but she could not or did not want to receive her TopUp Voucher by SMS, George would sent it by Mail. Steps 1 and Step 2 are repeated as above.

- STEP 3 (CCO) - Kristy may have told George that Matt's had been lost/stolen or that she just doesn't want the TopUp Voucher sent to the Account's Mobile. In these circumstances, George would have have checked Kristy's address details and then used the 'Cancel with Letter' option which changes the State of the Account to Cancelled, prints a personalised letter to Kristy as the Account Holder informing her '*You have requested to have her account closed. Your final $30 TopUp Voucher is 1234567890. Thank you for using TopItUp and you can rejoin at any time by calling Customer Care on 1300 TOPUPS*" and removes Kristy's entitlement of the TopUp Voucher from the allocated $30 pool.

- STEP 4 - George tells Kristy the TopUp Voucher is being mailed and that should she desire to reactivate the Account, please handset Customer Care. Thank you for using TopItUp.

- STEP 5 – George then mails the letter with the TopUp Voucher number to Kristy's address.

Pending or PreRegistered Account is Cancelled

Had the State of Kristy's Account been Pending or PreRegistered when she handsetd George, George would have repeated Steps 1 and Step 2 as if the account was Active.

- STEP 3 (CCO) - George would have explained to Kristy that TopItUp was clearing funds with her account. As a result he can start the process of closing her Account which will not allow further

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 254 of 1360

TopUp Vouchers to be requested or delivered. When the funds are cleared, TIU will mail your TopUp Voucher to you. Kristy agrees.

In these circumstances, George would have checked Kristy's address details, Updates the File Note and used the 'Cancel with Letter Option'. This time the letter does not print and cannot therefore be mailed. When the State is Pending, this action flags the Account as 'Blocked' which allows TIU to complete the Draw Down and at the same time disable the Account from sending TopUp Vouchers or replying to SMSs sent by the customer.

- STEP 4. George tells Kristy that should she desire to reactivate the Account, please handset Customer Care. Thank you for using TopItUp.

TIU has not Cancelled the Account. Blocking the Account means that whenever an SA runs a Blocked Accounts Report, Kristy's account will show.

As an extension of STEP 3 performed by an Scheme Adminstrator to complete the process with two possible outcomes depending on whether the funds clear:-

- STEP 3 (Funds Clear) - If the funds clear, the State is automatically changed to Active. The Account is still flagged as 'Blocked'. The next time an SA runs 'Blocked Account Report', they will notice that Kristy had attempted to close her Account and that the funds have cleared. The SA can now Cancel her Account. The SA opens the Account and selects the 'Cancel with Letter Option'. This action prints a personalised letter to Kristy as the Account Holder informing her that she has requested to have her account closed. Your final $30 TopUp Voucher is 1234567890. Thank you for using TopItUp and you can rejoin at any time by calling Customer Care on 1300 TOPUPS" and removes Kristy's entitlement of the TopUp Voucher from the allocated $30 pool.

- STEP 3 (Bad Debt or Bad Bank) - If the funds do not clear, TIU will automatically change the State of the Account to Bad Debt or Bad Bank as appropriate. The Account is still flagged as 'Blocked'. The next time an SA runs 'Blocked Account Report', they will notice that Kristy had attempted to close her Account and the funds have not cleared. The SA can now Cancel her Account without providing her a TopUp Voucher as she does not have an entitlement because of the Bad Debt or Bad Bank details. The SA opens the Account and selects the 'Cancel with Letter Option'. This action prints a personalised letter to Kristy as the Account Holder informing her *'that she has requested to have her account closed and that her account is in Bad Debt. Consequently, you are not entitled to a TopUp Voucher. You can ring TopItUp's Financial Department on XXXXXXX to discuss'* and Cancels the Account.

- STEP 5 – George then mails the letter without the TopUp Voucher number to Kristy's address.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 255 of 1360

Bad Debt or PreRegistered_BadDebt Account is Cancelled

Had the State of Kristy's Account been a Bad Debt or PreRegistered_BadDebt when she handsetd George, George would have repeated Steps 1 and Step 2 as if the account was Active.

STEP 3 (CCO) - George would have explained to Kristy that her Account does not have an entitlement to a TopUp Voucher as the funds did not clear on the last attempt to draw funds. George says he can close the Account. Kristy agrees. George updates the File Note and uses the 'Cancel as Bad Debt' option. No letter or SMS is printed and TIU Cancels the Account.

Had Kristy complained, George would still take this action and give Kristy the contact handset number for the Financial Administrator to call to discuss.

- STEP 4. George thanks Kristy you for using TopItUp. He does not invite her to rejoin.
- STEP 5. No action as the account is cancelled and no entitlement exists.

Bad Bank or PreRegistered_BadBank Account is Cancelled

Had the State of Kristy's Account been a Bad Bank or PreRegistered_BadBank when she handsetd George, George would have repeated Steps 1 and Step 2 as if the account was Active.

STEP 3 (CCO) - George would have explained to Kristy that her Account does not have an entitlement to a TopUp Voucher as the funds did not clear on the last attempt as the Bank Account details were not correct. George says he can close the Account. Kristy agrees. George updates the File Note and uses the 'Cancel as Bad Bank' option. No letter or SMS is printed and TIU Cancels the Account.

Had Kristy complained, George would still take this action and give Kristy the contact handset number for the Financial Administrator to call to discuss.

- STEP 4. George thanks Kristy you for using TopItUp. He does not invite her to rejoin.
- STEP 5. No action as the account is cancelled and no entitlement exists.

Other Scenarios

Greg's Mobile is Stolen

Greg's mobile (his Dad's actually) is stolen with Greg's Prepaid SIM in the handset at the time. When an SMS is sent using this SIM, TopItUp ascertains Greg's account number from the SIM. Greg handsets

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 256 of 1360

Customer Care using his home handset and speaks to Craig. Craig establishes that Greg is the Account Holder and Greg reports the handset as stolen.

Craig asks Greg for his other contact handset number and verifies the Personal Information on TopItUps database on Greg is accurate.

Craig flags Greg's account as 'Blocked' and records a file note on his account. Blocking an account does not interfere with the processing state of an account. Whatever the processing state was associated with the account prior to the Greg's call is also recorded in the file note. This information is used in any subsequent actions by TopItUp staff to allow consistency to be maintained with the account.

Greg's account is currently Active which means prior to Greg's call, TopItUp would have issed a TopUp Voucher had it been requested. If Greg had received a TopUp Voucher within the past 24 hours, TopItUp would have made a Draw Down on his bank account and TopItUp's logic would continue unaffected updating the processing state of his account regardless of whether the account is flagged Blocked or Unblocked including the rules associated with bad debt processing etc.

Craig explains to Greg that even if someone knows his Password and uses the solen handset in an attempt to request a TopUp Account, that since the handset has been reported stolen, TopItUp will log the SMS request to be investigated for fraud. When an Scheme Administrator reviews the 'potential fraud log files', a decision is made according to TopItUp's current security policy whether to inform the Police. The potential fraud log files contain all details of SMS's sent to TopItUp that are written to the potential fraud log file.

Craig explains that if the handset is found or returned intact, Greg should handset Customer Care and the state of his account will be 'Unblocked' allowing him to use his account normally again.

Until Greg either gets a new SIM or the handset (with SIM) is returned, Greg cannot use his account.

The state of Greg's account was Active when the SIM was reported stolen so Greg is entitled to a TopUp Voucher. Unless the State of Greg's account is 'Bad Debt' or ' PreRegistered_Pending', Greg would eventually be entitled to a TopUp Voucher. Craig asks Greg if he is going to get another Starter Kit and if so, does he want the new SIM to be re-registered with TopItUp in place of the stolen SIM. Greg says 'Yes' and Craig asks Greg to purchase a new Starter Kit from his nearest Network Store and tell the Dealer he is re-registering his account. Craig records Greg's decision on the file note to his account.

Had Greg decided not to register a new SIM, he is entitled to a TopUp Voucher. Had this been the case, Craig would have printed a TopUp voucher and mailed the voucher to Greg's account address (after verifying the address). The voucher is mailed to protect the accountholders right to the TopUp Voucher in the event that this was an attempt by another person to defraud the system. Accompanying the TopUp Voucher

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 257 of 1360

would be a thankyou letter from TopItUp. The Account State would be manually changed by Craig to Cancelled.

Greg Re-Registers his Stolen Account

The state of Greg account remains Blocked until he gets a new Starter Kit (and possibly a new or secondhand handset to replace his Father's stolen handset). He goes to the Dapto Network Communication Store and tells Jock that he wants to buy a Starter Kit and use it to Re-Register a his account. Jock gets Greg to complete a Registration Form and Direct Debit Authority. When completing the Registration Form, Jock gets him to tick the 'Are you Re-Registering an Existing Account' box and Jock asks him to complete the space titled 'Old Handset Number' with the number of his stolen mobile. Jock explains his new account should be registered overnight.

Jock faxes Greg's Registration Form to TopItUp. When Ann goes through the Registration forms the following morning, she notices that Greg's Application is for a Re-Registration. She creates the new account which sets the state of the new account to Pre-Registered. Ann opens up the 'Account Cancellation' screen and picks the 'Cancel an account and transfer Entitlement to a New Account' option. Ann is prompted to enter the account number of the account to be cancelled and enters Greg's old handset number. She notes that the state of this account is 'Active' which means that Greg has an entitlement to a TopUp Voucher.

Ann is prompted to enter the account number of the Pre-Registered Account which she does. TopItUp then asks her to confirm the cancellation of the old account and to change the entitlement. Ann presses the OK button.

The system changes the state of the old account to Cancelled, creates a link to the new account, changes the state of the new account to Active and sends an SMS to Greg's new account welcoming him to TopItUp. Greg could Request a TopUp immediately and TopItUp would send the TopUp Voucher to his new account.

Had the state of Greg's old account been pending when the handset was stolen, it would be unlikely that the state was still pending one day after he had been ins tore for a new Starter Kit, but if had been the case, TopItUp would transfer the state as Pending and not sent the Welcoming SMS until the Draw Down of funds had been cleared. Had the DrawDown resulted in a Bad Debt, the state of the new account would be a Bad Debt.

Greg initially signed up with Network Wollongong. Each TopUp Voucher ordered on his old account resulted in a commission to this store. When Greg re-registered, he did this through Network Dapto. Dapto will not get the commission for the entitlement transferred to the new account, but every TopUp Voucher that is successfully Drawn Down will result in a commission to Jock at Dapto.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 258 of 1360

James does not live near a Network Store

Greg writes to his brother James at Tennant Creek telling him about TopItUp. Greg knows that James uses Optus Prepaid but has trouble getting TopUp vouchers.

James handsets Greg and asks where he can signup. Greg checks the Hot to Guide and notices that James can get a Registration Form and Direct Debit Authority Network to complete by

- downloading the forms from TopItUps website www.topitup.com.au; or
- ringing Customer Care and requesting the forms be mailed out.

James downloads the forms as 'pdf' files and prints them out. There is no dealer account nominated on the form. The download also includes the 'How to Use Guide' and instructions on how to complete the forms correctly and where to fax or mail them. James completes the forms nominates his prepaid number and signs the T&Cs, and the Direct Deposit form. He mails the forms to TopItUp which starts the Registration process.

Kristy is Concerned about her Privacy

TopItUp will provide Personal Information to Registered Account Holders only.

Kristy saw a special last Sunday night on 60 Minutes regarding the new Privacy obligations on Private Sector organizations.

On Monday morning she gets an SMS from TopItUp telling her about a new range of ringtones that she can get using TopItUp. She remembers that she checked the Send Info box on the Registration Form when she signed up which gives TopItUp permission to send her this SMS.

She did not notice that Lee had TopItUp's Privacy Statement on the sales counter. She checks the 'How to Guide' and reads that she view her Personal Information at a Network Communication Store after mailing, emailing or faxing her request to Jayson Packett, TopItUps Privacy Officer.

She decides to email TopItUp requesting that she views the Peronal Information for both Matt's account and her account at Network Wollongong. When Jayson reads her email, her arranges for Joe to print the Personal Information for both accounts. Joe rings Lee and informs him that Personal Information has been requested by Kristy and that she desires to view this in Lee's store. He asks Lee to stand by his Fax and to ring Kristy to arrange a convenient time for her to view the Personal Information. Joe than faxes both accounts to Lee.

When Kristy comes into store, Lee shows Kristy TopItUps Privacy Statement framed on his sales counter. Kristy is entitled to ask Lee for a copy which she does. Lee provides Kristy with the Personal Information for both accounts. Kristy notices that her street name has been mistyped when Ann originally typed Kristy's details into the TopItUp Registration Database. Kristy is in her rights to have TopItUp keep her information accurate and up to date. She asks Lee to fix the street address. While Kristy is in store, Lee handsets TopItUp

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 259 of 1360

Customer Care centre handing the handset over to Kristy so she can identify herself and the change to her address is updated.

Kristy Wants to Change Matt's Password

Kristy has been concerned that Matt stills wants to know his Password and Kristy is becoming nervous. The Password she created for Matt's account when she registered the account is the cat's name and is very easy to guess. She decides to change it. She rings Customer Care and talks to Crig. After Craig verifies that she is the Account Holder of Matt's account, Craig asks her to provide him with the old password. Craig cannot view the Account Holders Password. To change the Password, he must ask the Account Holder for thei Password, type this in and get a match from TopItiUp.

If he does get a match he will ask Kristy to spell her new password and type the new password in. To ensure this is performed correctly, Craig asks Kristy to spell the Password again as he re-enters it. If both entries for the new Password are the same, the new Password is accepted and the Account Holders account is updated.

If the Account Holder and the User are the same person, TopItUp will send an SMS to account holders handset "Your password has been successfully changed". In this instance, the Account Holder and User are different people, so TopItUp does not send an SMS.

Kristy Forgets the Password

Kristy's forgets the new Password for Matt's handset. She rings Customer Care and talks to George. After George verifies that she is the Account Holder of Matt's account and that she has rung using Matt's handset. George asks her additional questions about recent account activity, such as when did you last Request a TopUp. The additional questions are only asked when someone forgets their Password and require that enough information is provided to George for him to believe that she is not someone who may have stolen Kristy's handset and wallet.

If George is confident she is genuine, George will direct TopItUp to send the Password to Matt's handset as an SMS. George as a Customer Care Officer, does not have sufficient access to obtain Kristy's Password.

The TopUp Voucher Value Changes

The System handles the situation of a TopUp Voucher changing value. Since the Account Holder has an entitlement to a TopUp Voucher, the next time a Recharge Order is received, the TopUp delivered is valued at the old TopUp Voucher value and the new voucher is ordered and payment made at the new TopUp Voucher Value.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 260 of 1360

Vouchers are supplied GST Free

In accordance with existing recharge vouchers purchased through stores, GTS is not paid by the customer on purchase but is levied and paid by the carrier as the service is used independent of the System.

Hostile Attacks

TopItUp will not allow a user to attempt to use the 'Any Mobile' feature using a web based SMS service such as Optus' Info2You service for security reasons.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 261 of 1360

Legend:
P – indicates Primary responsibility. For TIU means automatic function.
S – indicates secondary responsibility. For TIU means system is used to perform function

	TopItUp IT Infastructure	SMS - T sent by TIU or - C sent by Customer	Scheme Operator	Scheme Administrator	Financial Administrator	Customer Care Operator	System Administrator	Software Support	Dealer Support	Privacy Officer	TopItUp Website	Dealer	Customer	Customer Bank	Diamond - CBA	CBA Online Banking
Customer Enquiries	S			S		P					P	P	P			
Dealer Enquiries				S					P			P				
Instore/Web Registration											P web	P store	P			
Deliver Rego Forms												P store	P web			
PreRegister Customer	P		P													
Initial Draw Down including load RBFM	P		P	S										S	P	
Payment & Exception Report			S	P	S											P
Initial Bad Debts	P		P										S			
Customer Activation	P															
Welcome Message	P	T														
Request a TopUp	P	C											P			
SMS TopUp Voucher to Account Handset	P	T											S			
Draw Down including load both R & ABFM	P			P										S	P	
Bad Debt Management	S			P												P
Replenish Unallocated Vouchers	S			P		S										
Pay Dealer Commissions	S				P										P	S
Bad Attempt – Fraud Investigation	P	C/T		S		S	P									
Cancel an Account	S	T		P		P							P			
Privacy Issues	P		S	S		P	P		P		P	P	S			
Operations Reports	S		S	P			P									
Financial Reports	S			P			P									
End of Day Processing	S				S		P	S							P	S

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 262 of 1360

The Claims defining the Invention are as follows:

1. A system and method comprising a scheme "scheme" including infrastructure, computer software and components requiring a user "customer" to enrol into the scheme by purchasing an entitlement to a prepaid product or service, which scheme subsequently allows the customer to utilise the entitlement by allowing the customer to have wireless and instant access and delivery of the prepaid product and/or service in accordance with the business rules of the scheme.
2. A system and method as claimed in claim 1, whereby a scheme customer authenticates and authorises the scheme transaction by use of a scheme user name or number and password combination or by other biometric means such as face recognition or by any other means capable of being implemented on a wireless device.
3. A system and method as claimed in claim 1, which requires a customer to authorise the scheme to acquire funds from the customer's financial institution account or facility so as to initiate and maintain the customer's entitlement to a prepaid product or service while ever the customer participates in the scheme.
4. A system and method as claimed in claim 3, wherein the scheme management software initiates a process to interact with the customer's financial institution or facility to acquire appropriate funds to the value equivalent of the enrolment entitlement of the prepaid product and/or service.
5. A system and method as claimed in claim 1, wherein the customer initiates a request using an electronic wireless device to the scheme management infrastructure to acquire the entitlement, which if approved by the scheme, allows the scheme to provide such prepaid products and/or services to be delivered electronically to the same said device or to an alternate customer nominated device.
6. A system and method as claimed in claim 5, wherein once an entitlement has been delivered by the scheme management software to fulfil a customer's request, the scheme management software then initiates a process to interact with the customer's financial institution or facility to acquire additional funds to the equivalent value of the enrolment entitlement or any subsequent changes made by the customer to an alternate or additional prepaid product or service.
7. A system and method as claimed in claim 1, whereby a customer requesting cancellation from the scheme has the right to submit a final request to the scheme for their remaining entitlement according to the business rules of the scheme.
8. A system and method as claimed in claim 1, whereby an agent or agents that are service providers to the scheme and have been authorised to be part of the components that allow a customer to enrol are provided a margin paid and settled by the scheme, based on the value of the prepaid products and services purchased both initially and subsequently by customer's signed up by them using the scheme.
9. A system and method as claimed in claim 1, that allows a customer to purchase a product and /or service on a non-recurring entitlement basis and which are delivered instantly to the customer's wireless device and are subsequently indirectly paid by the customer to the scheme by the scheme

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 263 of 1360

initiating a funds transfer from the customer's financial institution or facility by means of the payment authority provided by the customer in claim 3.

10. A system and method as claimed in claim 9, which allows third parties to provide products and/or services to the scheme, through a scheme provided "content gateway", for resale to customers of the scheme and to be paid a price less a margin on the value of prepaid products and/or services provided which margin is retained by the scheme.

11. A system and method as claimed in claim 1, that allows a scheme authorised third party, using the third parties own system and method "third party scheme", to sell their products and/or services to customers of the scheme by sending a payment request to the scheme by using an authentication link provided by the scheme's infrastructure and components, allowing the third party to be paid a price less a margin for the products and/or services purchased by the customer by way of the scheme's payment facility, if such payment request is approved by the scheme.

12. A system and method as claimed in claim 11, whereby the customer uses the scheme's authentication framework to be identified.

13. A system and method as claimed in claim 11; whereby the customer uses the scheme's payment framework and does not provide any of their financial institution payment or facility details to the third party scheme.

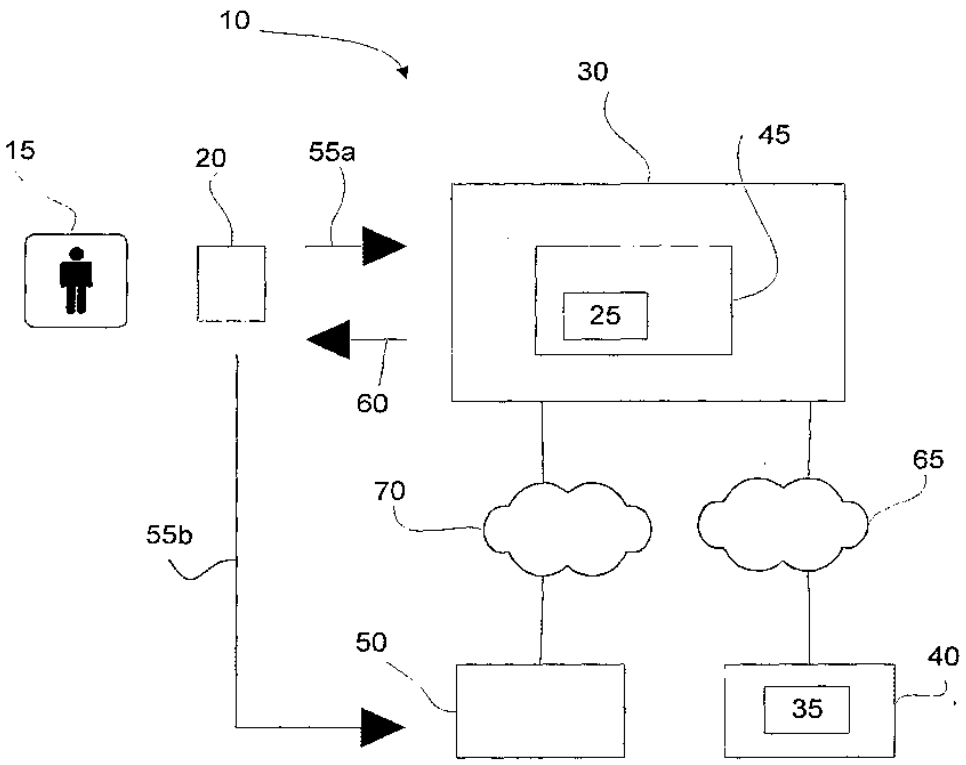
14. A system and method as claimed in claim 13; whereby the scheme allows the customer to purchase or pay for products and/or services at time of request "online" from the scheme authorised third party, if said customer has authorised the scheme to participate in such third party schemes.

15. A system and method as claimed in claim 13; whereby the scheme allows the customer to purchase products and/or services that are subsequently delivered to the customer after the customer payment has settled with the scheme's financial institution "off line" from the scheme authorised third party, if said customer has authorised the scheme to participate in such third party scheme.

16. A system and a method substantially and hereinbefore described with reference to the accompanying drawings.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 264 of 1360

Figure 1



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 265 of 1360

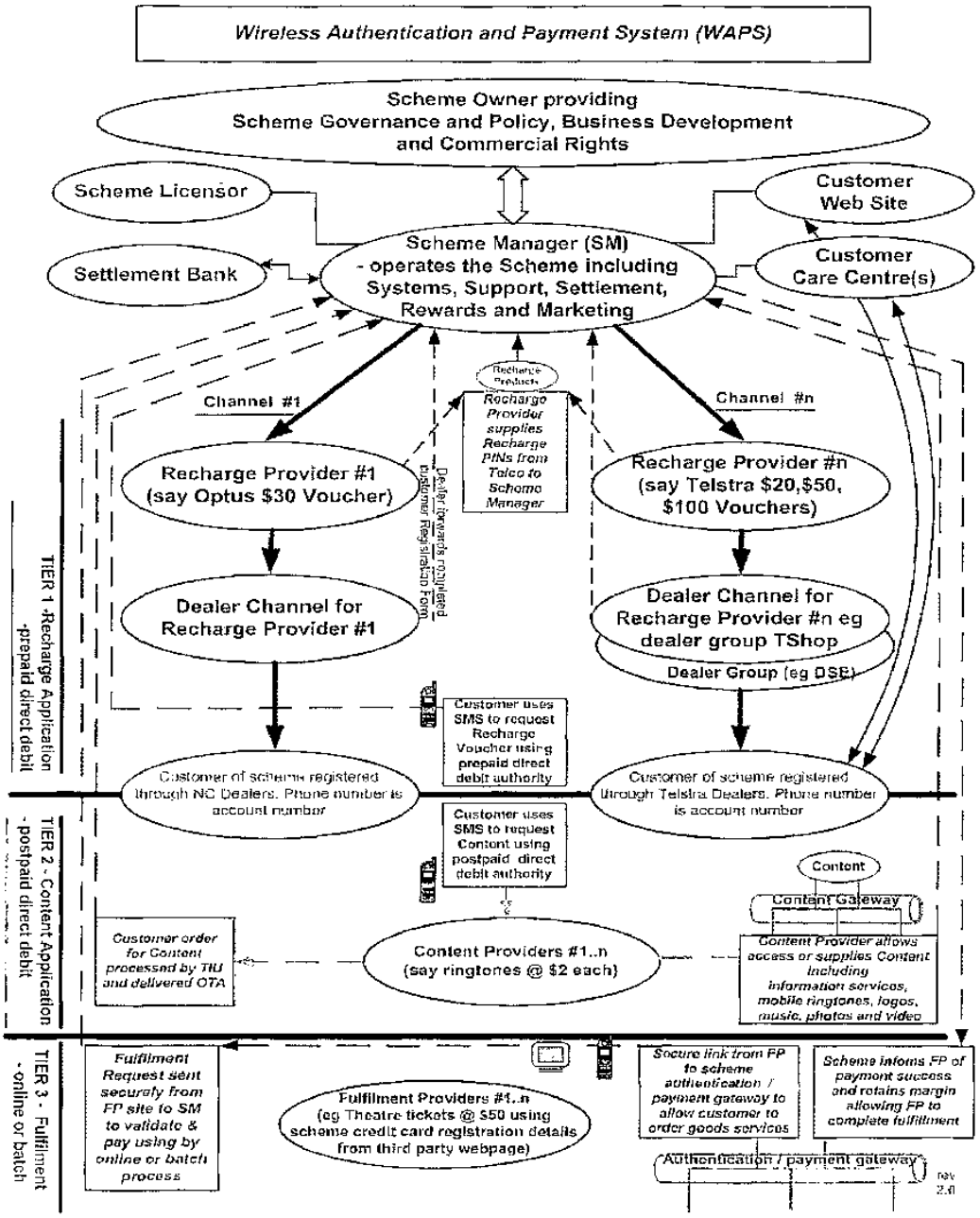


Figure 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 266 of 1360

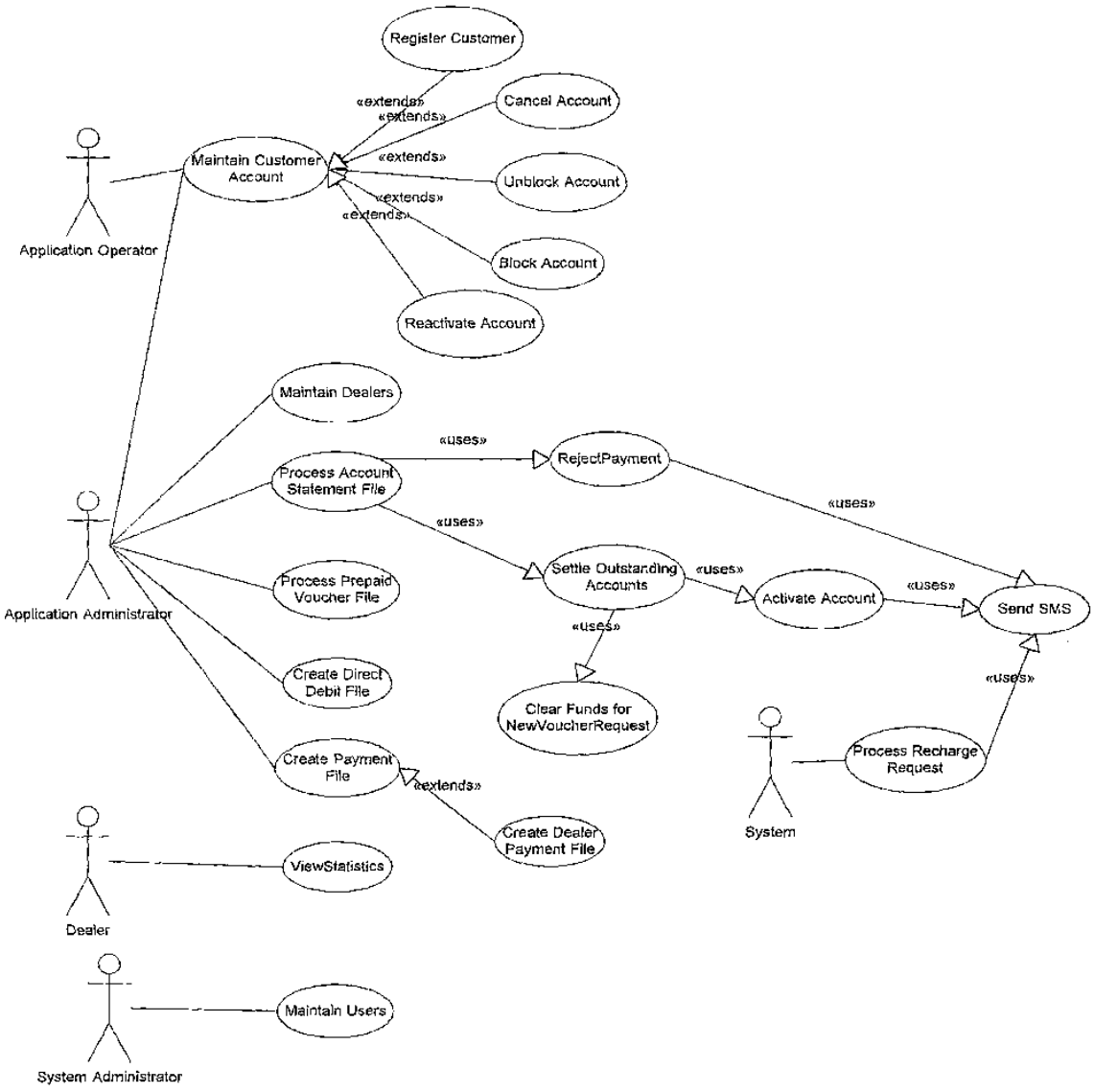


Figure 3

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 267 of 1360

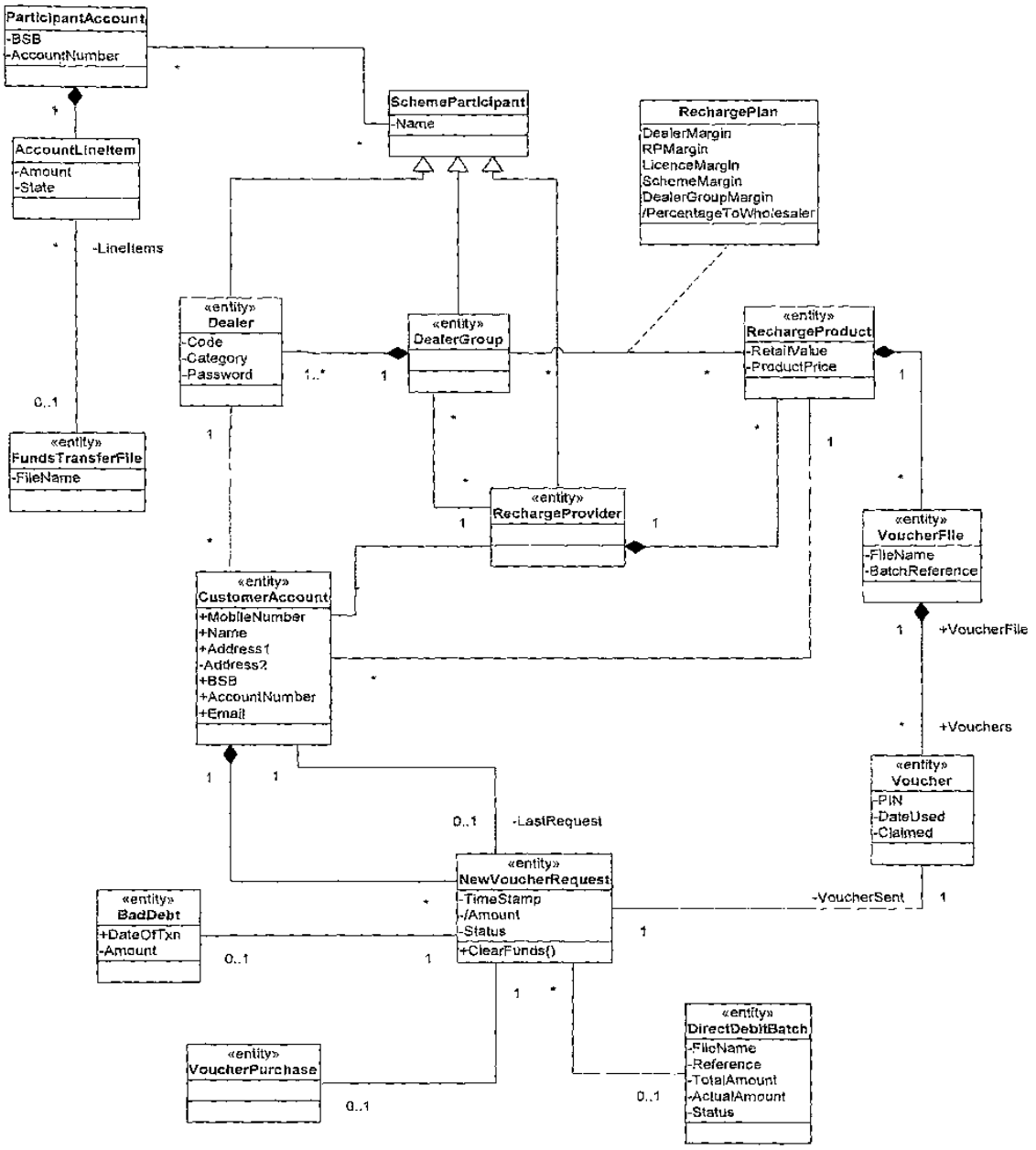


Figure-4

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 268 of 1360

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/01126

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 17/60, G06F 153/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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)
DWPI: IPC G06F 17/60, 153/00 and keywords: prepaid, recharg+, voucher?, wireless, mobile?, telecommunication?, payment, paying and similar terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0115424 A (BAGOREN et al.) 22 August 2002 entire document, see in particular paragraphs [0006] to [0010]	1-16
X Y	WO 01/74974 A (SIEMENS AKTIENGESELLSCHAFT) 11 October 2001 abstract abstract	1 2-7
X Y	US 4706275 A (KAMIL) 10 November 1987 entire document see in particular columns 3 and 4	1 2-7

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier 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
23 October 2003	29 OCT 2003
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **CHARLES BERKO** Telephone No : (02) 6283 2169

Form PCT/ISA/210 (second sheet) (July 1998)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/01126

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	US 2002/0065774 A (YOUNG et al.) 30 May 2002	
X	entire document	1
Y	see in particular paragraphs [0007] to [0025]	2-16
	US 6236851 B (FOUGNIES et al.) 22 May 2001	
X	entire document	1
Y	see in particular column 3 line 49 to column 4 line 51	2-16

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 270 of 1360

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU03/01126

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	2002115424	WO	02082797				
WO	0174974	BR	0109641	EP	1269739	US	2003071115
US	4706275						
US	2002065774	AU	20491/01	EP	1014646	EP	1107198
		JP	2001243386	US	2002123965	WO	0141419
		WO	02069085				
US	6236851	US	5722067	US	5854975	US	6157823
		US	2001021648				

END OF ANNEX

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 271 of 1360

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 October 2004 (14.10.2004)

PCT

(10) International Publication Number
WO 2004/088641 A2

(51) International Patent Classification[7]: G11B

(21) International Application Number:
PCT/US2004/009149

(22) International Filing Date: 25 March 2004 (25.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/457,716	26 March 2003 (26.03.2003)	US
Not furnished	25 March 2004 (25.03.2004)	US

(71) Applicant *(for all designated States except US)*: **WAY SYSTEMS, INC.** [US/US]; 200 Unicorn Park, Woburn, MA 01801 (US).

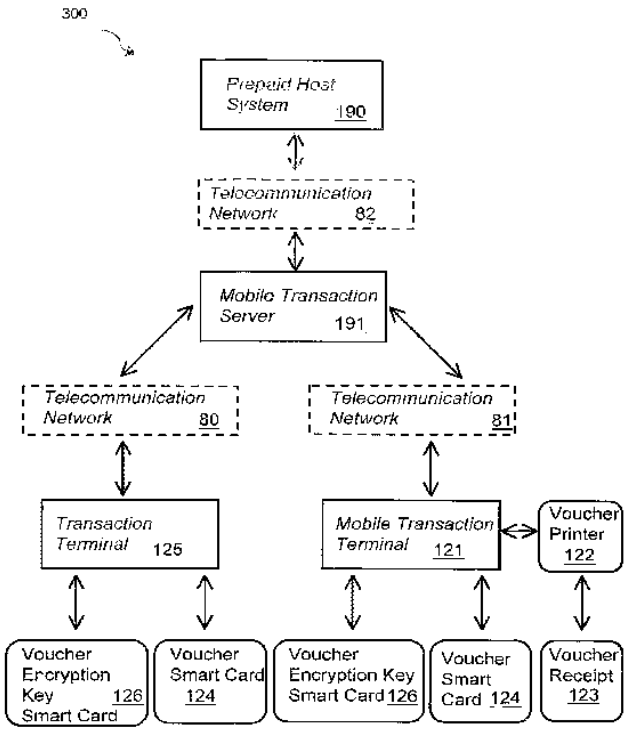
(71) Applicants and
(72) Inventors: **GOLDTHWAITE, Scott** [US/US]; 15 Oregon Court, Hingham, MA 02043 (US). **BALSAN, Damien** [US/US]; 78 Melrose Street, Arlington, MA 02474 (US).

(74) Agent: **COLLINS, Aliki, K., ph. d.**; AKC Patents, 215 Grove Street, Newton, MA 02466 (US).

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

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURELY STORING, GENERATING, TRANSFERRING AND PRINTING ELECTRONIC PREPAID VOUCHERS



(57) Abstract: The present invention describes a system and a method that utilizes transaction terminals (125, 121) equipped with smart card readers to download and store a batch of multiple prepaid electronic vouchers to a smart card (124), retrieve and decrypt individual prepaid vouchers from the smart card and print a voucher receipt with a printer (122) in connection with the transaction terminal. The transaction terminals (125, 121) are in connection with a mobile transaction server (191) that acts as a gateway to a prepaid system (190) and routes transactions between transaction terminals and the prepaid system and between transaction terminals. The present invention also describes a method for storing a voucher encryption key on a second smart card or hardware security module. The voucher encryption key is utilized to decrypt encrypted vouchers on a voucher repository smart card. The present invention also describes a method of transferring encrypted vouchers between voucher smart cards using a single transaction terminal or multiple transaction terminals. The transaction terminals may be mobile devices communicating to the mobile transaction server over wireless networks or computers connected to a wired network.

WO 2004/088641 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 272 of 1360

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 273 of 1360

SYSTEM AND METHOD FOR SECURELY STORING, GENERATING, TRANSFERRING AND PRINTING ELECTRONIC PREPAID VOUCHERS

Cross Reference to related Co-Pending Applications

This application claims the benefit of U.S. provisional application Serial No. 60/457,716 filed on March 26, 2003 and entitled SYSTEM AND METHOD FOR SECURELY STORING, GENERATING, TRANSFERRING AND PRINTING ELECTRONIC PREPAID VOUCHERS, which is commonly assigned and the contents of which are expressly incorporated herein by reference.

This application is also a continuation in part of U.S. applications Serial No. 10/205,768, 10/625,823, and 10/695,585, filed on July 26, 2002, July 23, 2003, and October 28, 2003, and entitled "SYSTEM AND METHOD FOR PAYMENT TRANSACTION AUTHENTICATION", "MOBILE DEVICE EQUIPPED WITH A CONTACTLESS SMART CARD READER/WRITER", and "MOBILE COMMUNICATION DEVICE EQUIPPED WITH A MAGNETIC STRIPE READER", respectively, the contents of which applications are expressly incorporated herein by reference.

Field of the Invention

The present invention relates to a system and a method for securely storing prepaid top up vouchers on a smart card and utilizing mobile devices to generate the vouchers at the time of purchase.

Background of the Invention

The market for mobile/wireless phone usage has rapidly expanded to reach over 1 billion subscribers throughout the world by the end of 2002. Over 60% of these subscribers prepay for mobile phone usage. The greatest growth of mobile phone subscribers occurs in economically underdeveloped and emerging economies, where it is also common to prepay for many other recurring services, such as utility bills, due to the lack of consumer credit infrastructure.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 274 of 1360

Referring to FIG. 1 and FIG. 2, a prior art method 100 for prepaying for mobile phone services includes the following steps. First, a customer 110 pays a merchant 120 (111) and receives a scratch card 160 in return (112). Scratch card 160 includes a hidden authorization code 180 covered with a protective coating 170. Customer 110 removes the protective coating 170 using a coin or fingernail to reveal the hidden authorization code 180. Authorization code 180 is also referred to as a "hidden recharge number" (HRN) or a "voucher" or a "voucher number". Next, customer 110 contacts a mobile operator 130 and provides the mobile operator 130 with the authorization code 180 through the mobile operator's call center or an interactive voice response system (113). Mobile operator 130 validates the authorization code 180, "recharges" or "tops up" customer's mobile account with the value associated with the authorization code 180, and notifies customer 110 upon completion of the top up transaction (114). The merchant 120 purchases scratch cards in bulk in multiple denominations for multiple mobile operators 130 from either a scratch card distributor 150 (115) or a wholesaler 140 (118). Typically wholesaler 140 purchases mobile airtime minutes in bulk in advance from several mobile operators 130 (117), manufactures the scratch cards 160 and sells the cards either directly to merchants 120 (118) or through a distributor 150 (116). Typically, merchants 120 are convenience stores, department stores or supermarkets that sell many other types of consumer merchandise. In one example, merchant 120 is a Sam's Club and scratch card 160 is an AT&T phone card. Although this is the most widely used method for topping up mobile phone accounts, the costs associated with scratch card manufacturing, distribution, inventory and potential fraud result in reduced profitability for the mobile operator 130. These costs could represent up to 30% of the face value of the scratch card 160. For example for a typical scratch card 160 with a face value amount of $100, the mobile operator only realizes about $70 in revenue due to the above mentioned costs associated with scratch cards.

Dedicated Point of Sale (POS) terminals and Automated Teller Machines (ATMs) are also used to provide a more cost effective way to top up mobile prepaid accounts by electronically generating and printing the voucher at the time of the purchase. Referring to FIG 3, a prior art method 200 for topping up mobile prepaid accounts includes the following steps. First, customer 110 pays merchant 120 (211). Merchant 120 engages a Point of Sale (POS) Terminal 121 to connect over a telecommunication

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 275 of 1360

network 80 to a remote prepaid system 190 (210, 215). Merchant 120 generates a voucher number (not shown) and prints the voucher number onto a receipt 123 using a printer 122 that is in connection with the POS terminal 121. Next, merchant 120 provides the customer 110 with the voucher receipt 123 that contains the voucher number (not shown) (212). Next, customer 110 provides the mobile operator 130 with the voucher number printed on the voucher receipt 123 (213), the mobile operator 130 validates the voucher number and tops up the customer's mobile account with the value associated with the voucher number (214). Mobile operator 130 also notifies customer 110 upon completion of top up transaction (214). These electronic vouchers are created "online" one at a time by the POS terminal 121 by connecting to prepaid system 190 for each customer 110. Alternatively, the POS terminal 121 connects to the prepaid system 190 less frequently, downloads a batch of multiple vouchers that are securely stored within the memory of the POS terminal 121 and subsequently generates the electronic vouchers "offline" for each customer 110. The problem with this prior art method is the fact that there are not many POS or ATMs readily available to accommodate the number of transactions and users. Accordingly, there is a need for a low cost alternative for a mobile POS or ATM that can securely, store, generate, transfer and print electronic prepaid vouchers.

Summary of the Invention

In general, in one aspect of this invention features a system for generating and storing one or more prepaid electronic vouchers in a voucher smart card. The system includes a voucher host system adapted to generate the prepaid electronic vouchers and a voucher terminal adapted to receive the prepaid electronic vouchers from the voucher host system over a network connection and to store the prepaid electronic vouchers in the voucher smart card.

Implementations of this aspect of the invention include the following. The system may further include a transaction server adapted to mediate and aggregate transactions and communications between the voucher terminal and the voucher host system over the network connection. The voucher smart card may be a removable smart card such as a "full size" smart credit card, a "full size" smart debit card, a "plug-in" Subscriber Identification Module (SIM) smart card, a "plug-in" Secure Access Module (SAM)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 276 of 1360

smart card, a contactless smart card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card or combinations thereof. The voucher smart card may be a hardware security module (HSM) such as microprocessors or storage accessories. The voucher terminal may be a wireless communication device equipped with a smart card reader/writer module such as a mobile phone, a personal digital assistant (PDA), a pager, a point of sale (POS) terminal, a television remote control, a personal computer or combinations thereof. The smart card reader/writer module is adapted to receive and read/write information stored in/to the voucher smart card, respectively. The voucher terminal may be a wired communication device equipped with a smart card reader/writer module such as a phone, a wired personal digital assistant (PDA), a point of sale (POS) terminal, a television, a personal computer or combinations. The voucher terminal may be a wireless communication device having a subscriber identification module (SIM) card slot, a smart card reader/writer module electrically connected to the SIM card slot and the smart card reader/writer module is adapted to receive and read/write information stored in/to the voucher smart card, respectively. The network may be the Internet, a telecommunications network, a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) or a private communication network. The wireless wide area network (WWAN) may be a Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access (CDMA), CDMA 2000, or wideband CDMA (WCDMA). The communications between the voucher host system and the voucher terminal may have a format such as Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), or proprietary message formats. The system may also include a printer adapted to connect to the voucher terminal for printing hard copies of the prepaid electronic vouchers. The printer may be connected to the voucher terminal via a wired connection such as a serial connection, a parallel connection, a Universal Serial Bus (USB) connection or a mini USB connection. Alternatively, the printer may connect to the voucher terminal via a wireless connection such as infrared, Bluetooth, 801.1x, or other short-range radio frequency connections. The prepaid electronic vouchers may have data such as a mobile operator code, a voucher number, a voucher expiration date, the voucher number in an

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 277 of 1360

encrypted format, a voucher value, a voucher currency code, a voucher product code, a voucher product description, a voucher owner code, or a voucher owner. The prepaid electronic vouchers may have encrypted data and the system may further include a voucher encryption smart card that has a voucher encryption key for decrypting the encrypted data. The voucher encryption key may be a personal identification number (PIN), a private key, a public key, a symmetric key or an asymmetric key. The decrypting may utilize techniques such as symmetric keys, asymmetric keys, data encryption standard (DES, 3DES), RSA, elliptical curve cryptography (ECC), message authentication codes (MAC, HMAC, SHA-1, AES, and public key infrastructure (PKI). The voucher terminal may further include a first voucher application and the first voucher application may provide for retrieving of the stored electronic prepaid vouchers from the voucher smart card and printing hard copies of the prepaid electronic vouchers. The first application may further provide decrypting encrypted data stored in the electronic prepaid vouchers. The voucher terminal may further include a second voucher application and the second voucher application may provide transferring one or more of the stored prepaid electronic vouchers from the voucher smart card to another voucher smart card.

In general in another aspect the invention features a method for generating and distributing one or more prepaid electronic vouchers issued by a merchant for providing a service or a product. The method includes providing a voucher host system adapted to generate the prepaid electronic vouchers and providing a voucher terminal adapted to receive the prepaid electronic vouchers from the voucher host system over a network connection and to store the prepaid electronic vouchers in a voucher smart card. Next, placing a purchase order and paying for one of the one or more prepaid electronic vouchers from the voucher terminal to the voucher host system over the network connection. Next, downloading the one prepaid electronic voucher from the voucher host system to the voucher terminal over the network connection and storing the one prepaid electronic voucher in the voucher smart card. Next, retrieving the one prepaid electronic voucher from the voucher smart card and presenting the one prepaid electronic voucher to the merchant and receiving the service or product.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 278 of 1360

Implementations of this aspect of the invention include the following. The method may further include printing a hard copy of the one prepaid electronic voucher before presenting the one prepaid electronic voucher to the merchant. The electronic prepaid voucher may have encrypted data and the method may further include decrypting the encrypted data by inserting an encryption smart card in the voucher terminal, retrieving an encryption key and using it to decrypt the encrypted data. The method may further include transferring the one prepaid voucher from the voucher smart card to a second voucher smart card or to a second voucher terminal.

Among the advantages of this invention may be one or more of the following. When compared to the scratch card method the advantages to storing vouchers on a smart card instead of printing the vouchers onto scratch cards are cost and security. Although the cost of a smart card is significantly higher than a paper or plastic scratch card, the smart card can be used thousands of times to store vouchers whereas the scratch card is used once by the customer and then discarded. Vouchers represent monetary value and therefore security is extremely important. Storing encrypted voucher numbers on a smart card is inherently more secure than scratch cards for several reasons. Scratch cards themselves have no "built in" securities features and rely on a secure manufacturing, distribution and sales environment. In the event of theft of a batch of scratch cards, the person in possession of the scratch cards needs only to remove the protective coating on the card to access the voucher number, a breach in security can occur at the merchant location or at any point in the scratch card manufacturing and distribution process. Smart Cards, however, have many "built in" security features that establish a tamper resistant environment for securely storing data from logical and physical attacks which is the primary reason that the financial industry is moving away from magnetic stripe cards to smart cards for debit, credit and electronic cash applications and the primary reason that mobile network operators utilize Subscriber Identity Module (SIM) smart cards. In the event of theft of a smart card with vouchers, the person in possession of the smart card would first have to compromise the security of the smart card to access the encrypted vouchers, then compromise the voucher encryption key that may be stored on the same card or on a different card. The expense and time required to successfully carry out such an attack is significantly more costly than the value of the vouchers on the smart card.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 279 of 1360

When compared to other Point of Sale (POS) voucher methods, the present invention has the advantage of mobility. The existing prior art POS voucher methods store the vouchers within the device but do not separate storage from fulfillment, i.e., one device is used for both purposes. In the present invention, vouchers are stored on a removable smart card that can be used by one device for voucher storage transactions and then removed and inserted into another device for voucher generation and printing. The present invention provides secure mobility for voucher generation and printing enabling one transaction device to store transactions on a smart card and multiple devices can be deployed to service customer needs remotely.

Brief Description of the Drawings

FIG. 1 is a block diagram of a prior art system for prepaying for mobile phone services;

FIG. 2 is a schematic diagram of a prior art prepaid phone scratch card;

FIG. 3 is schematic diagram of a prior art electronic prepaid voucher system;

FIG. 4 is schematic diagram of an electronic prepaid voucher system that utilizes smart cards according to this invention;

FIG. 5 is a flow diagram of a voucher download transaction to a smart card according to this invention;

FIG. 6 is a flow diagram of a voucher generation transaction from a smart card and print transaction according to this invention;

FIG. 7 is a diagram representing the screen flow and application logic of a mobile transaction terminal application according to this invention;

FIG. 8 is a flow diagram of a voucher transfer transaction according to this invention; and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 280 of 1360

FIG. 9 is a diagram representing the screen flow and application logic of a voucher transfer transaction according to this invention.

Detailed Description of the Invention

The present invention describes a system and a method for using a transaction terminal for downloading and storing prepaid electronic vouchers on a first smart card, retrieving and decrypting prepaid vouchers from the first smart card and printing a voucher receipt in a printer that is connected with the transaction terminal. The present invention also describes a system and a method for storing a voucher encryption key on a second smart card and then using the second card to decrypt encrypted vouchers on the first smart card. The present invention also describes a system and a method of transferring prepaid vouchers between voucher smart cards.

Referring to FIG. 4, a system 300 for downloading and storing prepaid electronic vouchers on a smart card includes a Prepaid Host System 190, a Mobile Transaction Server 191, a Transaction Terminal 125, a Mobile Transaction Terminal 121, a Printer 122, a Voucher Smart Card 124, a Voucher Encryption Key Smart Card 126, and a Voucher Receipt 123. The Prepaid Host System 190 is the primary source for generating voucher information. The Mobile Transaction Server 191 connects to the Prepaid Host System 190 over telecommunication network 82 and to the transaction terminal 125 and the mobile transaction terminal 121 over telecommunication networks 80, and 81 respectively. Mobile Transaction Server 191 functions as a gateway that mediates and aggregates the transactions between the Prepaid Host System 190 and the transaction terminal 125 and the mobile transaction terminal 121. In one example, Voucher Smart Card 124 and Voucher Encryption Key Smart Card 126 are removable smart cards including "full-size" smart cards, such as credit cards, debit cards, contactless smart cards, stored-value cards, coupon cards, reward cards, electronic cash cards, loyalty cards, identification cards and secure access application or "plug in" format smart cards like those used for Subscriber Identity Modules (SIM's) smart cards utilized by mobile telephones or Secure Access Modules (SAM's) smart cards utilized by Point of Sale (POS) devices. In another example Voucher Smart card 124 and Voucher Encryption Card are hardware security modules (HSM) including accessories that are added to computers, servers and Personal Digital Assistants (PDA's) for banking and secure access applications and secure

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 281 of 1360

microprocessors that are utilized by Point of Sale (POS) devices. Voucher Encryption Key smart cards have the ability to securely store data and resist tampering and can generate cryptographic keys and encrypt/decrypt data utilizing a cryptographic co-processor. Telecommunications networks 80, 81 and 82 can be the Internet, a public telecommunication network, a private telecommunication network, a local area network (LAN) wireless wide area network (WWAN), a wireless local area network (WLAN) or a personal area network (PAN). The data exchanged using telecommunications networks 80, 81 and 82 have a format such as Short Message Service (SMS), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), or Simple Network Management Protocol (SNMP) over Transmission Control Protocol/Internet Protocol (TCP/IP). Transaction Terminal 125 and Mobile Transaction Terminal 121 are capable of receiving a voucher smart card and printing a voucher receipt 123 via a printer 122 (not shown for Terminal Transaction 125).

Referring to FIG. 10, in one example, the transaction terminal 125 is a mobile phone that is capable of receiving smart cards 902, 903, 904 as described in PCT application WO 99/66752 entitled "Communication Method and Apparatus Improvement", the entire content of which is incorporated herein by reference. In other examples, the transaction terminal 125 is a Point of Sale terminal equipped with a smart card reader, or a Personal Computer (i.e. lap top, desk top, workstation) equipped with a smart card reader or a Personal Digital Assistant (PDA) equipped with a smart card reader. Similarly, the mobile transaction terminal 121 is a mobile phone as shown in FIG. 10 equipped with a smart card reader, or a Personal Computer (i.e. lap top, desk top, workstation) equipped with a smart card reader or a Personal Digital Assistant (PDA) equipped with a smart card reader. In another example, the mobile transaction terminal 121 is a smart card reader equipped with a keypad and a display.

A merchant utilizes the present invention to sell prepaid vouchers to consumers, and the consumers use this invention to recharge their prepaid account. For example, at the beginning of each day, the merchant uses the transaction terminal device described in this invention to connect to a prepaid host system and download a batch of prepaid vouchers in various denominations to a smart card. The merchant may be a small convenient storeowner, a large supermarket sales clerk, an independent sales representative or a sales representative working for a telecommunication company.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 282 of 1360

Throughout the day the merchant sells the prepaid vouchers to customers who are interested in purchasing a voucher. The customers pay the merchant with cash, credit or debit card. Alternatively, a customer approaches the merchant for purchasing a voucher. The merchant uses the transaction terminal device of this invention to retrieve a voucher from the smart card and prints a receipt for the customer with the voucher number on it. The customer then contacts his service provider and gives the voucher number to the service provider at which point the service provider validates the voucher number and "tops up' or "recharges" the customer's account. The voucher numbers are encrypted on the smart card. The encryption key required to decipher the encrypted information is stored on another smart card. Both cards, i.e., the smart card with the encrypted voucher number and the smart card with the encryption key, need to be present in the transaction terminal device of this invention in order to decrypt, retrieve and present a voucher number for the customer. This process of batch downloading and individual retrieving of vouchers may be distributed among several individuals. For example, a sales manager may download batches of vouchers to multiple smart cards and give each smart card to individual sales representatives. The sales manager may utilize separate smart cards for individual prepaid products, i.e. one card for a mobile operator and another smart card for a long distance telecommunication provider. The sales manager may require the individual sales representatives to pay a deposit or the full amount of value of the vouchers stored on the smart card in advance. Throughout the day, as the sales representatives deplete their inventory the sales manager may also transfer additional vouchers to sales representatives remotely using the transaction terminal device and system described in the present invention. At the end of the day, the sales representatives return their smart cards to the sales manager at which point the sales representatives and the merchant reconcile the financial transactions. Alternatively, the financial settlement may occur remotely and electronically.

Referring to FIG. 5, the process of downloading a voucher includes the following steps. First, the transaction terminal 125 establishes a connection with the mobile transaction server 190 over network 80 (410). Next, mobile transaction server 191 routes the transaction request to the prepaid host system 190 through network 82 (411). The prepaid host system 190 validates the connection and transmits a specified

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 283 of 1360

quantity and types of vouchers to the mobile transaction server 191 over network 82 (412). The mobile transaction server 191 routes the downloaded vouchers to the transaction terminal 125 through network connection 80 (413). In one example, the data in the voucher download transaction for a single voucher include, a code representing the mobile operator that the voucher is associate with, a voucher serial number, a voucher expatriation date, the voucher number in its encrypted format, the voucher value and a code representing the currency of the voucher value. Upon completion of the voucher download transaction, the transaction terminal 125 transmits a transaction complete acknowledgement to the mobile transaction server 191 through network connection 80 (416) and the mobile transaction server 191 transmits this acknowledgement to the prepaid host system 190 over network 82 (417). The transaction terminal 125 is in connection with a voucher smart card 124 and sends the voucher data to the voucher smart card 124 (414). Upon completion of the transaction the transaction terminal 125 receives an acknowledgement from the voucher smart card 124 (415). In one embodiment, the Prepaid Host System 190 determines the quantity and types of vouchers that are downloaded to the Transaction Terminal 125. In this embodiment the connection is initiated by the prepaid host system 190 (408, 409). In another embodiment, the Transaction Terminal 125 determines the quantity and types of vouchers that are downloaded to the Transaction Terminal 125.

Referring to FIG. 6 and FIG. 7, a method 500 for retrieving a voucher from a smart card 124 and printing a voucher receipt 124 includes the following steps. First, a user utilizes a mobile transaction application 600 stored on the mobile transaction terminal 121 to start a new transaction (610). The user is then prompted to insert the voucher smart card 124 into the mobile transaction terminal 121 (612). The mobile transaction application 600 on the mobile transaction terminal 121 accesses the voucher smart card 124 (517) and retrieves the inventory of available vouchers (518). The inventory of available mobile operators is displayed on the mobile transaction terminal application and the user is prompted to make a selection (614). Following the selection of a specific mobile operator, the inventory of available voucher values for the selected mobile operator is displayed and the user is prompted to make a selection (616). Following the selection of a specific voucher, the user is prompted to confirm the selection (618). Upon confirmation, the mobile transaction application

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 284 of 1360

600 accesses voucher smart card 124 (519), retrieves the voucher data associated with the confirmed selection (520), updates the inventory on the voucher smart card 124 (521) and stores the voucher data within the memory (not shown) of the mobile transaction terminal 121. Next, the mobile transaction application 600 accesses the voucher encryption key smart card 126 (510), and if the mobile transaction terminal 121 is not in connection with the voucher encryption key smart card 126, the user is prompted to insert the voucher encryption key smart card 126 (620). The mobile transaction application 600 accesses the voucher encryption key smart card 126 to retrieve smart card profile information (511). If the mobile transaction terminal 121 is configured to receive only one smart card, the user is asked to remove the voucher smart card 124 and replace it with the voucher encryption key smart card 126. In one example, the voucher encryption key smart card 126 is protected from unauthorized access with a Personal Identification Number (PIN) and the user is prompted to enter a valid PIN (622). The users types the PIN and the mobile transaction application 600 presents the PIN to the voucher encryption key smart card 126 (512) for authorization. The authorization result is returned to the mobile transaction application 600 (513) and upon successful authorization, the mobile transaction application 600 retrieves the voucher encryption key (not shown) (514). The voucher encryption key is utilized by the mobile transaction application 600 to decrypt the encrypted voucher information that was previously retrieved by the mobile transaction application 600 from the voucher smart card 124. The decryption process (not shown) utilizes symmetric keys or asymmetric keys and cryptographic techniques such as Data Encryption Standard (DES, 3DES), RSA, Elliptical Curve Cryptography (ECC), Message Authentication Codes (MAC, HMAC), SHA-1, AES and Public Key Infrastructure (PKI). When the voucher decryption is completed, the user is prompted to either print or view the decrypted voucher information on the screen (626). The mobile transaction terminal 121 is in connection with a printer 122. Communication 70 with the printer 122 is either wired (i.e. serial, parallel, USB) or wireless (i.e. infrared, Bluetooth, 802.1x). If the user selects the print option, the mobile transaction terminal 121 establishes connection 70 with the printer 122 and sends the voucher data to the printer (522). The printer 122 formats the voucher data accordingly, generates voucher receipt 123 (524) and acknowledges results of print process to the mobile transaction terminal 121 (523). Alternatively, the user selects to present the voucher data on the display (not shown) of the mobile transaction terminal

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 285 of 1360

121. The mobile transaction application 600 reestablishes connection with the voucher smart card 124 to update the voucher inventory with the completed transaction details (525). Once a voucher is retrieved, the voucher is either deleted from the inventory or its status is changed such that it can no longer be retrieved.

The present invention also defines a process for transferring vouchers between voucher smart cards. In one case, the voucher transfer process is local and it uses the same transaction terminal (mobile or otherwise) to transfer vouchers from one voucher smart card to another voucher smart card. In another case the voucher transfer process is remote and it uses one transaction terminal (mobile or otherwise) to transmit voucher data to another transaction terminal (mobile or otherwise). Referring to FIG. 8 and FIG. 9, using voucher transfer application 800, a user initiates a voucher transfer transaction 700. The user is prompted to insert the origin voucher smart card 124 that stores the vouchers into the transaction terminal 125. The voucher transfer application 800 accesses voucher smart card 124 (717) and retrieves the inventory of available vouchers (718). The inventory of available mobile operators is displayed on the transaction terminal application and the user is prompted to make a selection (814). Following the selection of a mobile operator, the inventory of available voucher values for the selected mobile operator is displayed and the user is prompted to make a selection (816). Following the selection of a voucher value, the inventory of available vouchers for the selected operator and value denominations are displayed and the user is prompted to select a quantity of vouchers that is less than or equal to the total quantity of vouchers available (818). Following the selection of one or more vouchers, the use is prompted to confirm the selection (819). Upon confirmation, the voucher transfer application 800 accesses voucher smart card 124 (719), retrieves the voucher data associated with the confirmed selection (720), updates the inventory on the voucher smart card 124 and stores the voucher data within the memory (not shown) of the transaction terminal 125 (721). In one example, the transfer of vouchers requires authorization. If the transaction terminal 125 is configured to receive only one smart card, the user is required to remove the voucher smart card 124 and replace it with the voucher encryption key smart card 126. In one example, the voucher encryption key smart card 126 is protected from unauthorized access with a Personal Identification Number (PIN) and the user is prompted to enter a valid PIN (822). The users types the PIN, the voucher transfer

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 286 of 1360

application 800 presents the PIN to the voucher encryption key smart card 126 for authorization (712) and the authorization result is returned to the voucher transfer application 800 (713). Upon successful authorization, the voucher data are transferred from the memory (not shown) of the transaction terminal 125 to a temporary storage repository on the voucher encryption key smart card 126 (714) and then the user is prompted to choose the transfer method (824). The transfer method is either a local "card to card" transfer or a remote transfer. If the user selects the local "card to card" transfer option, the user is prompted to insert the destination voucher smart card 124a (828). The voucher transfer application 800 retrieves the voucher data from the temporary storage repository on the voucher encryption key smart card 126 (715) and appends the voucher data to the destination voucher smart card 124a (722). After receiving the voucher data, the destination voucher smart card 124a provides an acknowledgement response to the transaction terminal application (723) that is further routed to the voucher encryption key smart card 126 to complete the card transfer transaction (716). If the transaction terminal is configured to receive only one smart card, the user is prompted to remove and insert the origin voucher smart card 124, the voucher encryption key smart card 126 and the destination voucher smart card 124a in the appropriate sequence to complete the transaction (830). If the user selects the remote transfer option, the user is prompted to enter the Identification Number of the destination transaction terminal (826). The voucher transfer application 800 transmits the voucher data to the mobile transaction server 191 over network 80 (724). Mobile transaction server 191 transmits an acknowledgment of the receipt of the voucher data over network 80 to transaction terminal 125 which is then routed to the voucher encryption key smart card 126 to complete the transaction from the origin of the transfer (716). The mobile transaction server 191 transmits a notification to the mobile transaction terminal 121 designated by the origin 826 over network 81 (726). The mobile transaction terminal 121 receives the notification (726) and transmits an acknowledgement and a download request from the mobile transaction server 191 over network 81 (727). The mobile transaction server 191 transmits the voucher download to mobile transaction terminal 121 over network 81 (728). The user is prompted to insert the voucher smart card 124b and a voucher transaction application 800a on the mobile transaction terminal 121 appends the voucher data to the destination voucher smart card 124b (729). A voucher data transfer acknowledgement is transmitted to the mobile transaction

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 287 of 1360

terminal 121(730) and routed to the mobile transaction server 191 over network 81 to complete the remote transfer transaction (731).

In another embodiment, the transaction terminal (mobile or otherwise) is also a payment terminal that enables the user to accept and process electronic payments as described in a co-pending patent application entitled "System and method for payment transaction authentication", the entire content of which is incorporated herein by reference. In another embodiment, the transaction terminal (mobile or otherwise) is also configured to receive magnetic stripe payment cards as described in a co-pending patent application entitled "Mobile Communication Device Equipped with a Magnetic stripe Reader". In another embodiment, the mobile transaction terminal 121 has no connection to the mobile transaction server. The voucher encryption key smart card 126 and the voucher smart card 124 l store all transaction information that is transferred to another transaction terminal utilizing the "card to card" transfer method described in FIG. 8 and FIG. 9. In another embodiment, the Prepaid Host System 190 is any type of service that utilizes vouchers such as utilities, local phone service, long distance phone service, pay-per-view entertainment, electronic ticketing. In another embodiment, the encrypted vouchers are stored in the memory of the mobile transaction terminal 121 or transaction terminal 125. The memory is either internal to the mobile device or external and in connection with the mobile device (i.e. Compact Flash, Secure Digital, USB Flash memory, external hard drive). In yet another embodiment, the encrypted vouchers are stored in the memory 901 of the mobile phone attachment as described in PCT application WO 99/66752 entitled "Communication Method and Apparatus Improvement", shown in FIG. 10. Referring to FIG. 4, in another embodiment the mobile transaction terminal 121 has no network connection 81 with the mobile transaction server 191 and is a non-network connected device with the ability to interact with voucher encryption key smart card 126, voucher smart card 124 and optionally voucher printer 122.

Several embodiments of the present invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the following claims.

What is claimed is:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 288 of 1360

1. A system for generating and storing one or more prepaid electronic vouchers comprising:

a voucher host system adapted to generate said prepaid electronic vouchers;

a voucher smart card; and

a voucher terminal adapted to receive said prepaid electronic vouchers from said voucher host system over a network connection and to store said prepaid electronic vouchers in said voucher smart card.

2. The system of claim 1 further comprising a transaction server adapted to mediate and aggregate transactions and communications between said voucher terminal and said voucher host system over said network connection.

3. The system of claim 1 wherein said voucher smart card comprises a removable smart card selected from a group consisting of a "full size" smart credit card, a "full size" smart debit card, a "plug-in" Subscriber Identification Module (SIM) smart card, a "plug-in" Secure Access Module (SAM) smart card, a contactless smart card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card and combinations thereof.

4. The system of claim 1 wherein said voucher smart card comprises a hardware security module (HSM) selected from a group consisting of microprocessors and storage accessories.

5. The system of claim 1 wherein said voucher terminal comprises a wireless communication device equipped with a smart card reader/writer module selected from a group consisting of a mobile phone, a personal digital assistant (PDA), a pager, a point of sale (POS) terminal, a television remote control, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 289 of 1360

6. The system of claim 1 wherein said voucher terminal comprises a wired communication device equipped with a smart card reader/writer module selected from a group consisting of a phone, a wired personal digital assistant (PDA), a point of sale(POS) terminal, a television, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

7. The system of claim 1 wherein said voucher terminal comprises a wireless communication device comprising a subscriber identification module (SIM) card slot, a smart card reader/writer module electrically connected to said SIM card slot and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

8. The system of claim 1 wherein said network is selected from a group consisting of the Internet, a telecommunications network, a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) and a private communication network.

9. The system of claim 8 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

10. The system of claim 2 wherein said communications comprise a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

11. The system of claim 1 further comprising a printer adapted to connect to said voucher terminal for printing hard copies of said prepaid electronic vouchers.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 290 of 1360

12. The system of claim 11 wherein said printer is connected to said voucher terminal via a wired connection selected from a group consisting of a serial connection, a parallel connection, a USB connection and a mini USB connection.

13. The system of claim 11 wherein said printer is connected to said voucher terminal via a wireless connection selected from a group consisting of infrared, Bluetooth, 801.1x, and short-range radio frequency (RF) connections.

14. The system of claim 1 wherein said prepaid electronic vouchers comprise data selected from a group consisting of a mobile operator code, a voucher number, a voucher expiration date, said voucher number in an encrypted format, a voucher value, voucher currency code, voucher product code, voucher product description, voucher owner code, and voucher owner.

15. The system of claim 1 wherein said prepaid electronic vouchers comprise encrypted data.

16. The system of claim 15 further comprising a voucher encryption smart card wherein said voucher encryption smart card comprises a voucher encryption key for decrypting said encrypted data.

17. The system of claim 16 wherein said voucher encryption key is selected from a group consisting of a personal identification number (PIN), a private key, a public key, a symmetric key and an asymmetric key.

18. The system of claim 16 wherein said decrypting utilizes techniques selected from a group consisting of symmetric keys, asymmetric keys, data encryption standard (DES, 3DES), RSA, elliptical curve cryptography (ECC), message authentication codes (MAC, HMAC, SHA-1, AES, and public key infrastructure (PKI).

19. The system of claim 1 wherein said voucher terminal further comprises a first voucher application wherein said first voucher application provides retrieving of said

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 291 of 1360

stored electronic prepaid vouchers from said voucher smart card and printing hard copies of said prepaid electronic vouchers.

20. The system of claim 19 wherein said first application further provides decrypting encrypted data stored in said electronic prepaid vouchers.

21. The system of claim 1 wherein said voucher terminal further comprises a second voucher application wherein said second voucher application provides transferring one or more of said stored prepaid electronic vouchers from said voucher smart card to another voucher smart card.

22. A method for generating and distributing one or more prepaid electronic vouchers issued by a merchant for providing a service or a product, said method comprising:

providing a voucher host system adapted to generate said prepaid electronic vouchers;

providing a voucher terminal adapted to receive said prepaid electronic vouchers from said voucher host system over a network connection and to store said prepaid electronic vouchers in a voucher smart card;

placing a purchase order and paying for one of said one or more prepaid electronic vouchers from said voucher terminal to said voucher host system over said network connection;

downloading said one prepaid electronic voucher from said voucher host system to said voucher terminal over said network connection and storing said one prepaid electronic voucher in said voucher smart card;

retrieving said one prepaid electronic voucher from said voucher smart card; and

presenting said one prepaid electronic voucher to said merchant and receiving said service or product.

23. The method of claim 22 further comprising providing a transaction server adapted to mediate and aggregate transactions and communications between said voucher terminal and said voucher host system over said network connection.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 292 of 1360

24. The method of claim 22 further comprising printing a hard copy of said one prepaid electronic voucher before presenting said one prepaid electronic voucher to said merchant.

25. The method of claim 22 wherein said one electronic prepaid voucher comprises data selected from a group consisting of a mobile operator code, a voucher number, a voucher expiration date, said voucher number in an encrypted format, a voucher value, voucher currency code, voucher product code, voucher product description, voucher owner code, and voucher owner.

26. The method of claim 22 wherein said one prepaid electronic voucher comprises encrypted data.

27. The method of claim 26 wherein an encryption key for said encrypted data is stored in an encryption smart card.

28. The method of claim 27 further comprising decrypting said encrypted data by inserting said encryption smart card in said voucher terminal, retrieving said encryption key and using it to decrypt said encrypted data.

29. The method of claim 22 wherein said voucher smart card comprises a removable smart card selected from a group consisting of a "full size" smart credit card, a "full size" smart debit card, a "plug-in" Subscriber Identification Module (SIM) smart card, a "plug-in" Secure Access Module (SAM) smart card, a contactless smart card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card and combinations thereof.

30. The method of claim 22 wherein said voucher smart card comprises a hardware security module (HSM) selected from a group consisting of microprocessors and storage accessories.

31. The method of claim 22 wherein said voucher terminal comprises a wireless communication device equipped with a smart card reader/writer module selected from a group consisting of a mobile phone, a personal digital assistant (PDA), a

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 293 of 1360

pager, a point of sale (POS) terminal, a television remote control, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

32. The method of claim 22 wherein said voucher terminal comprises a wired communication device equipped with a smart card reader/writer module selected from a group consisting of a phone, a wired personal digital assistant (PDA), a point of sale(POS) terminal, a television, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

33. The method of claim 22 wherein said voucher terminal comprises a wireless communication device comprising a subscriber identification module (SIM) card slot, a smart card reader/writer module electrically connected to said SIM card slot and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

34. The method of claim 22 wherein said network is selected from a group consisting of the Internet, a telecommunications network, a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) and a private communication network.

35. The method of claim 34 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

36. The method of claim 23 wherein said communications comprise a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 294 of 1360

37. The method of claim 22 wherein said prepaid electronic vouchers comprise data selected from a group consisting of a mobile operator code, a voucher number, a voucher expiration date, said voucher number in an encrypted format, a voucher value, voucher currency code, voucher product code, voucher product description, voucher owner code, and voucher owner.

38. The method of claim 27 wherein said voucher encryption key is selected from a group consisting of a personal identification number (PIN), a private key, a public key, a symmetric key, and an asymmetric key.

39. The method of claim 28 wherein said decrypting utilizes techniques selected from a group consisting of symmetric keys, asymmetric keys, data encryption standard (DES, 3DES), RSA, elliptical curve cryptography (ECC), message authentication codes (MAC, HMAC, SHA-1, AES, and public key infrastructure (PKI).

40. The method of claim 22 wherein said voucher terminal further comprises a first voucher application wherein said first voucher application provides said retrieving of said stored electronic prepaid vouchers from said voucher smart card and printing hard copies of said prepaid electronic vouchers.

41. The method of claim 40 wherein said first application further provides decrypting of encrypted data stored in said electronic prepaid vouchers.

42. The method of claim 40 wherein said voucher terminal further comprises a second voucher application wherein said second voucher application provides transferring one or more of said stored prepaid electronic vouchers from said voucher smart card to another voucher smart card.

43. The method of claim 22 further comprising transferring said one prepaid voucher from said voucher smart card to a second voucher smart card.

44. The method of claim 22 further comprising transferring said one prepaid voucher from said voucher smart card to a second voucher terminal.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 295 of 1360

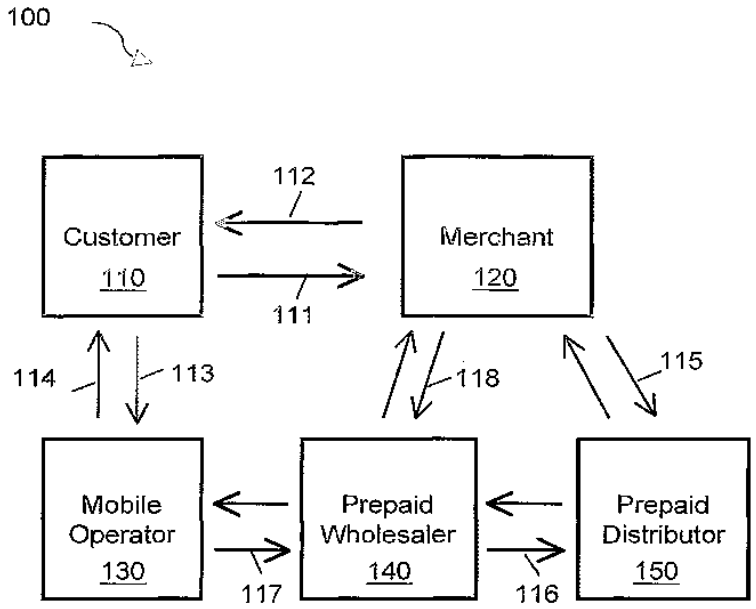


FIG. 1
(Prior Art)

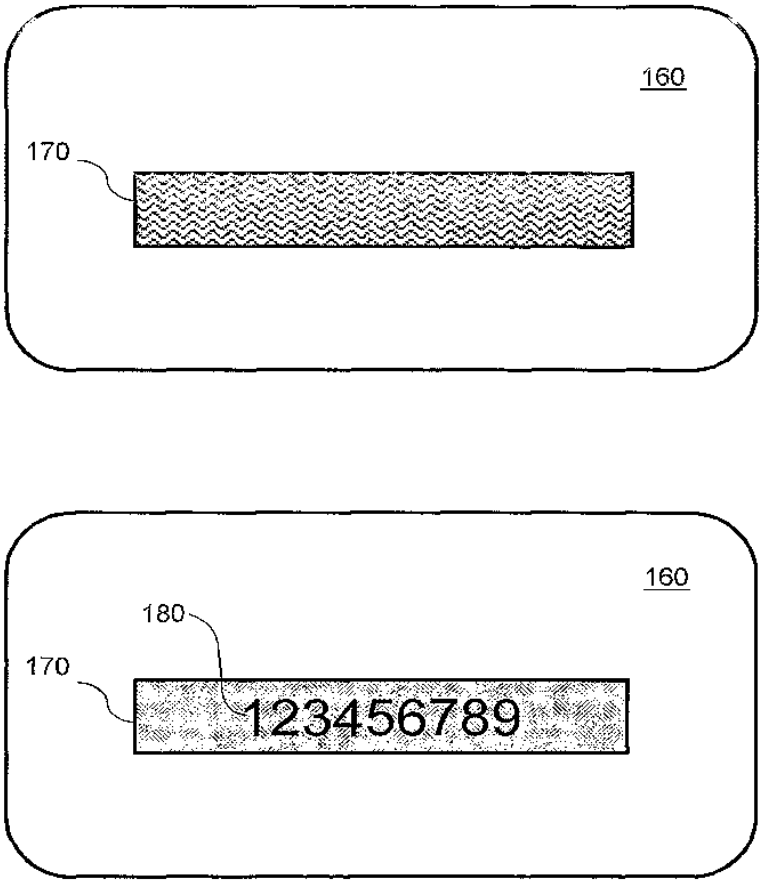


FIG. 2
(Prior Art)

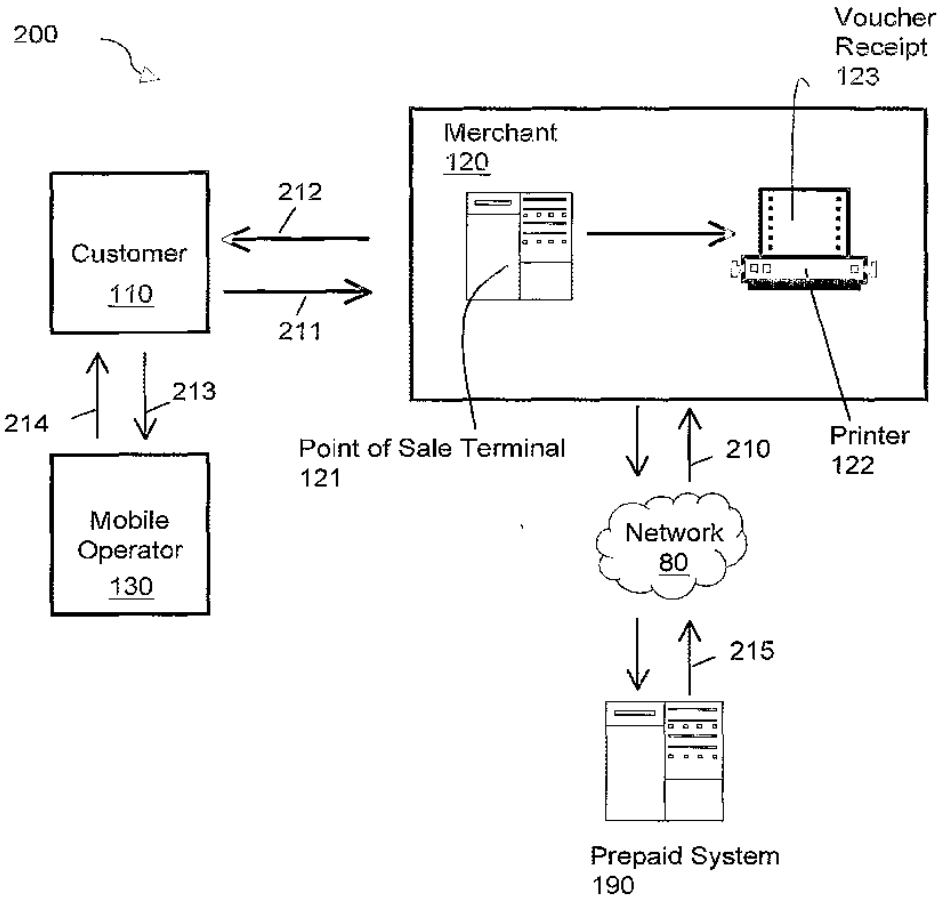


FIG. 3
(Prior Art)

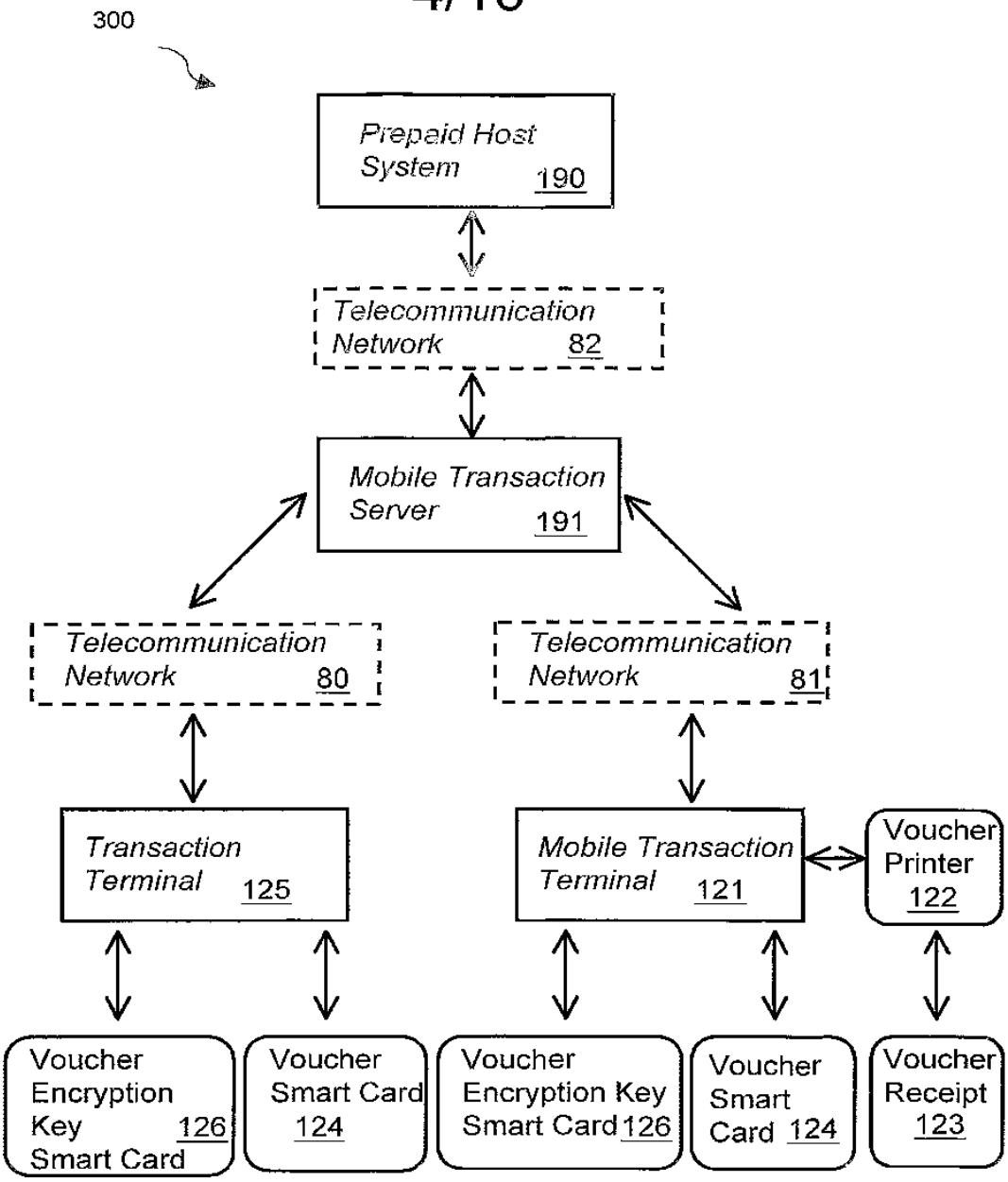

300
Prepaid Host System 190
Telecommunication Network 82
Mobile Transaction Server 191
Telecommunication Network 80
Telecommunication Network 81
Transaction Terminal 125
Mobile Transaction Terminal 121
Voucher Printer 122
Voucher Encryption Key Smart Card 126
Voucher Smart Card 124
Voucher Encryption Key Smart Card 126
Voucher Smart Card 124
Voucher Receipt 123

FIG. 4

5/10

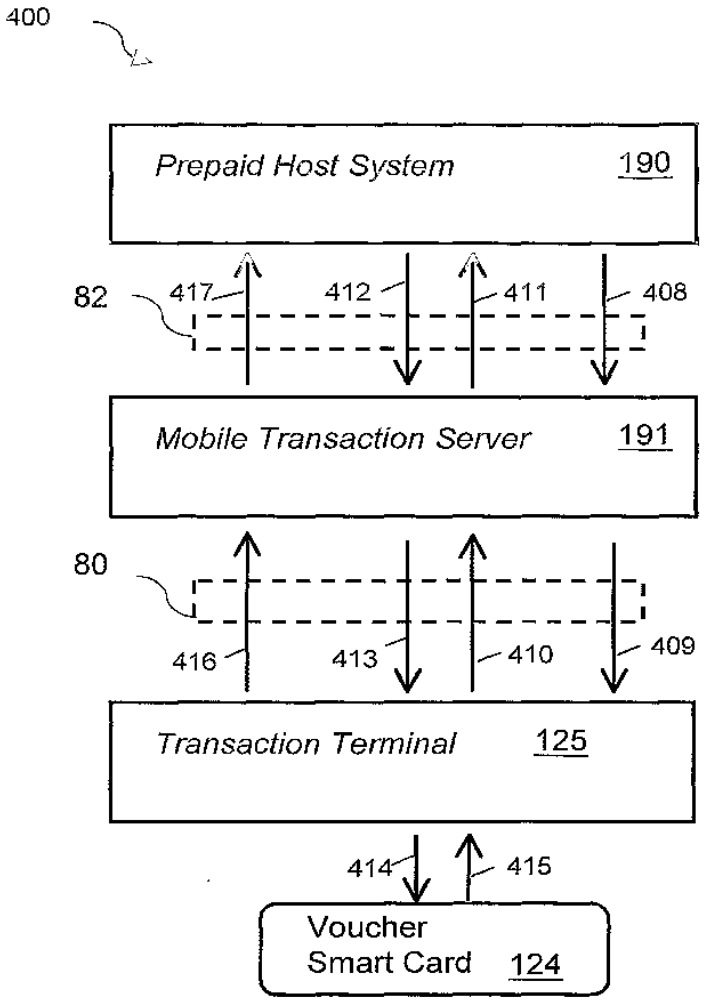

400
Prepaid Host System 190
82
417
412
411
408
Mobile Transaction Server 191
80
416
413
410
409
Transaction Terminal 125
414
415
Voucher
Smart Card 124

FIG. 5

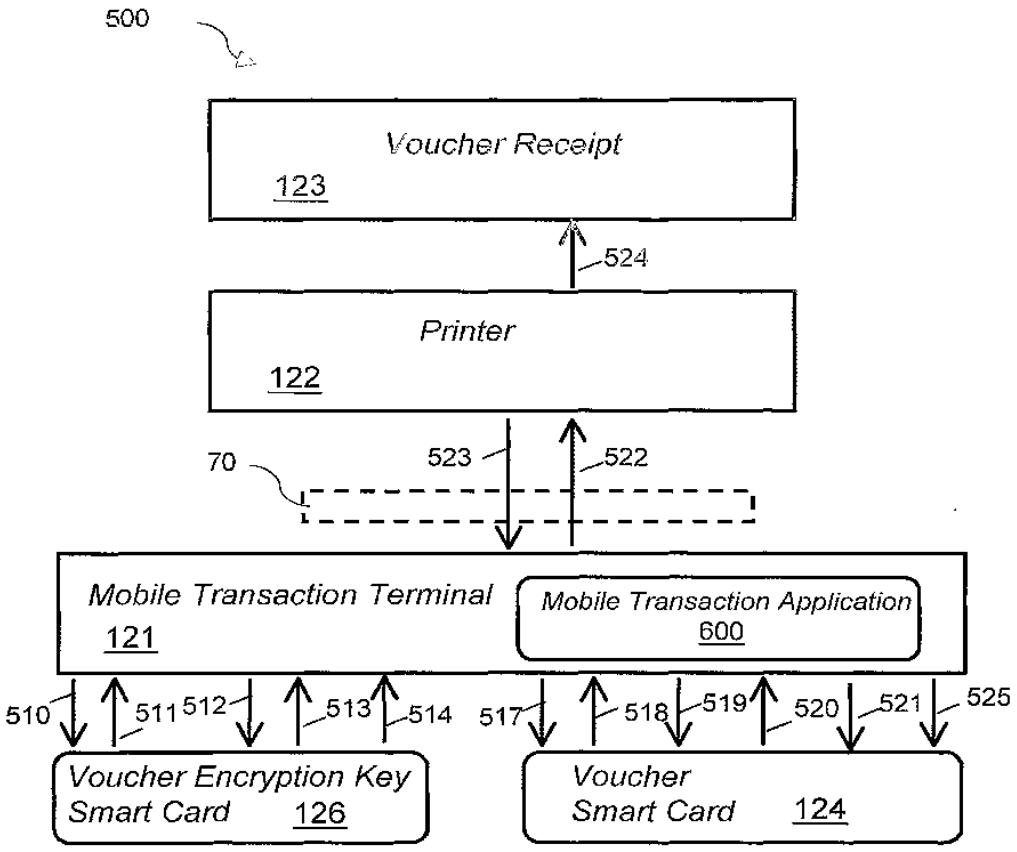

500
Voucher Receipt
123
524
Printer
122
70
523
522
Mobile Transaction Terminal
121
Mobile Transaction Application
600
510
511
512
513
514
517
518
519
520
521
525
Voucher Encryption Key
Smart Card
126
Voucher
Smart Card
124

FIG. 6

7/10

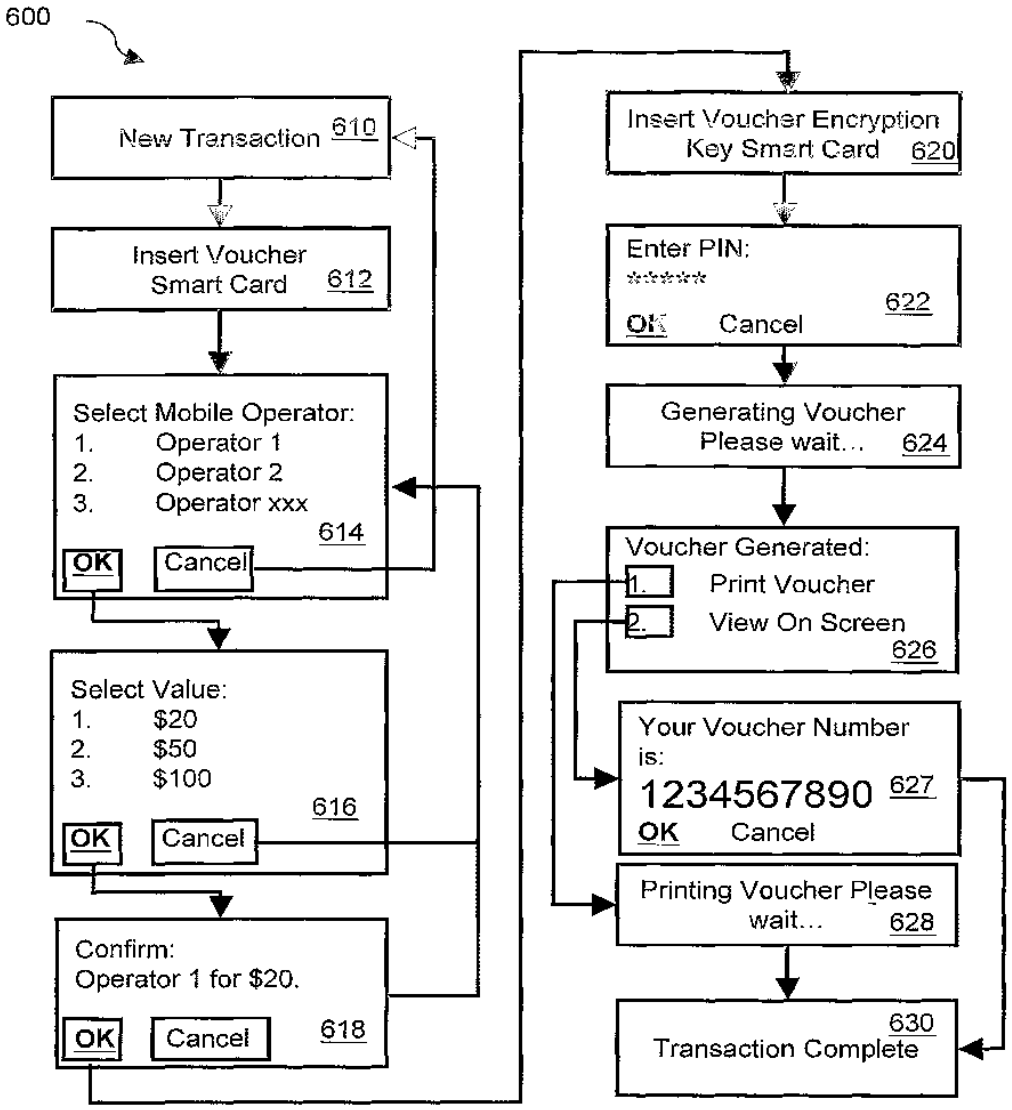

600
New Transaction 610
Insert Voucher Smart Card 612
Select Mobile Operator:
1. Operator 1
2. Operator 2
3. Operator xxx
614
OK
Cancel
Select Value:
1. $20
2. $50
3. $100
616
OK
Cancel
Confirm:
Operator 1 for $20.
OK
Cancel
618
Insert Voucher Encryption Key Smart Card 620
Enter PIN:
******
622
OK
Cancel
Generating Voucher Please wait... 624
Voucher Generated:
1. Print Voucher
2. View On Screen
626
Your Voucher Number is:
1234567890 627
OK
Cancel
Printing Voucher Please wait... 628
630
Transaction Complete

FIG. 7

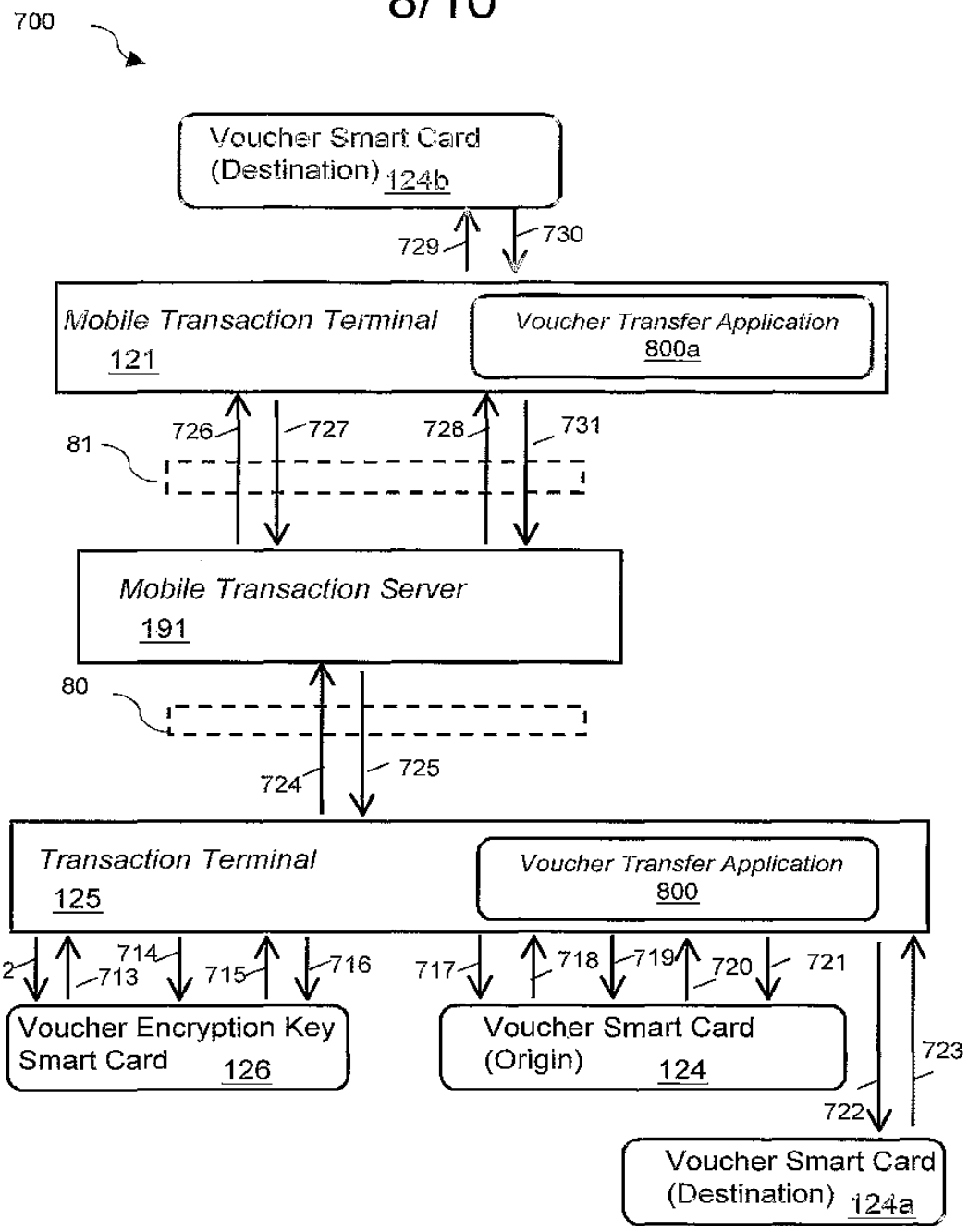

700
Voucher Smart Card (Destination) 124b
729
730
Mobile Transaction Terminal 121
Voucher Transfer Application 800a
81
726
727
728
731
Mobile Transaction Server 191
80
724
725
Transaction Terminal 125
Voucher Transfer Application 800
712
713
714
715
716
717
718
719
720
721
723
722
Voucher Encryption Key Smart Card 126
Voucher Smart Card (Origin) 124
Voucher Smart Card (Destination) 124a

FIG. 8

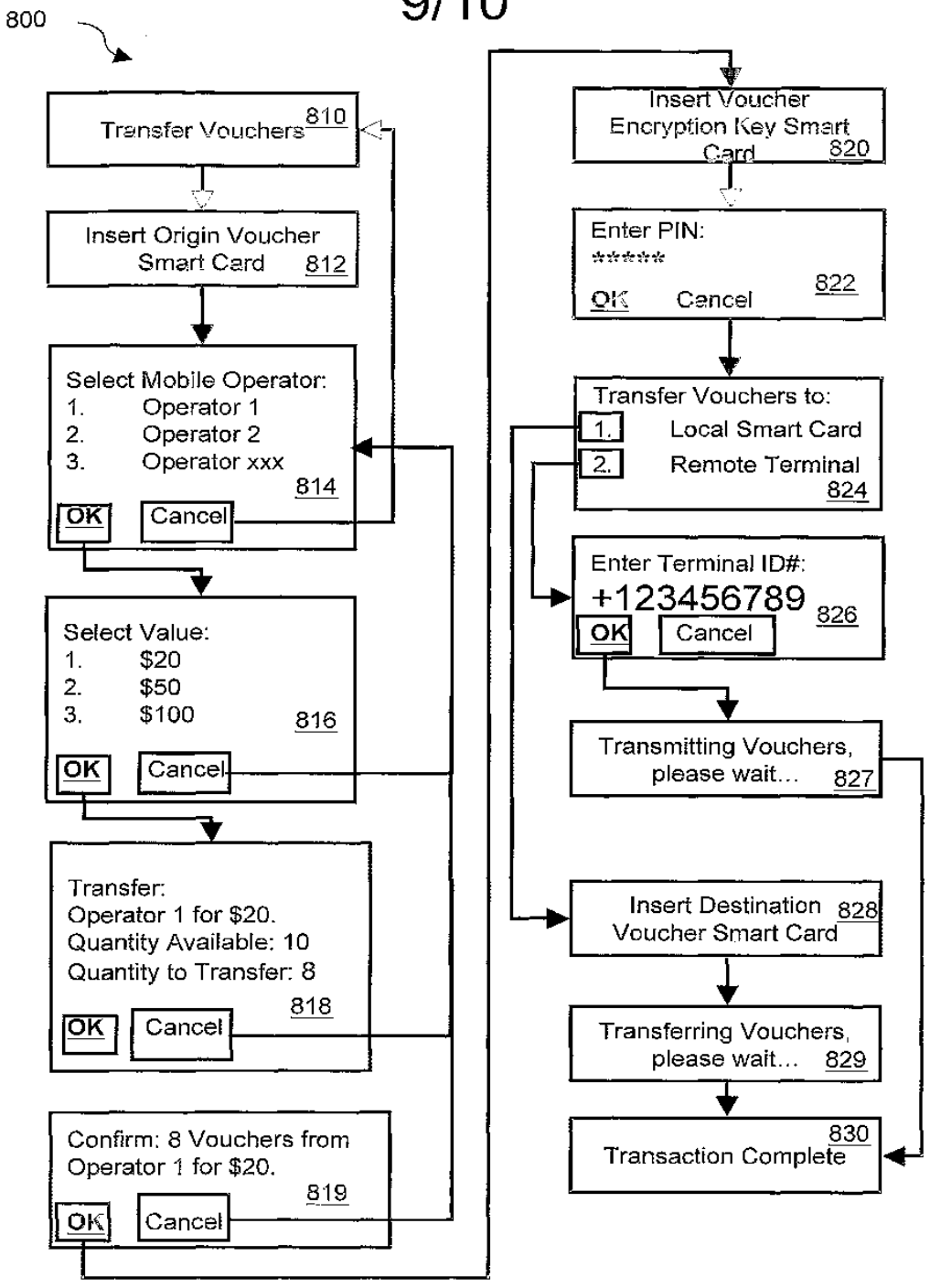

800
Transfer Vouchers 810
Insert Origin Voucher Smart Card 812
Select Mobile Operator:
1. Operator 1
2. Operator 2
3. Operator xxx
814
OK
Cancel
Select Value:
1. $20
2. $50
3. $100
816
OK
Cancel
Transfer:
Operator 1 for $20.
Quantity Available: 10
Quantity to Transfer: 8
818
OK
Cancel
Confirm: 8 Vouchers from Operator 1 for $20.
819
OK
Cancel
Insert Voucher Encryption Key Smart Card 820
Enter PIN:
*****
822
OK
Cancel
Transfer Vouchers to:
1. Local Smart Card
2. Remote Terminal
824
Enter Terminal ID#:
+123456789
826
OK
Cancel
Transmitting Vouchers, please wait... 827
Insert Destination Voucher Smart Card 828
Transferring Vouchers, please wait... 829
830
Transaction Complete

FIG.9

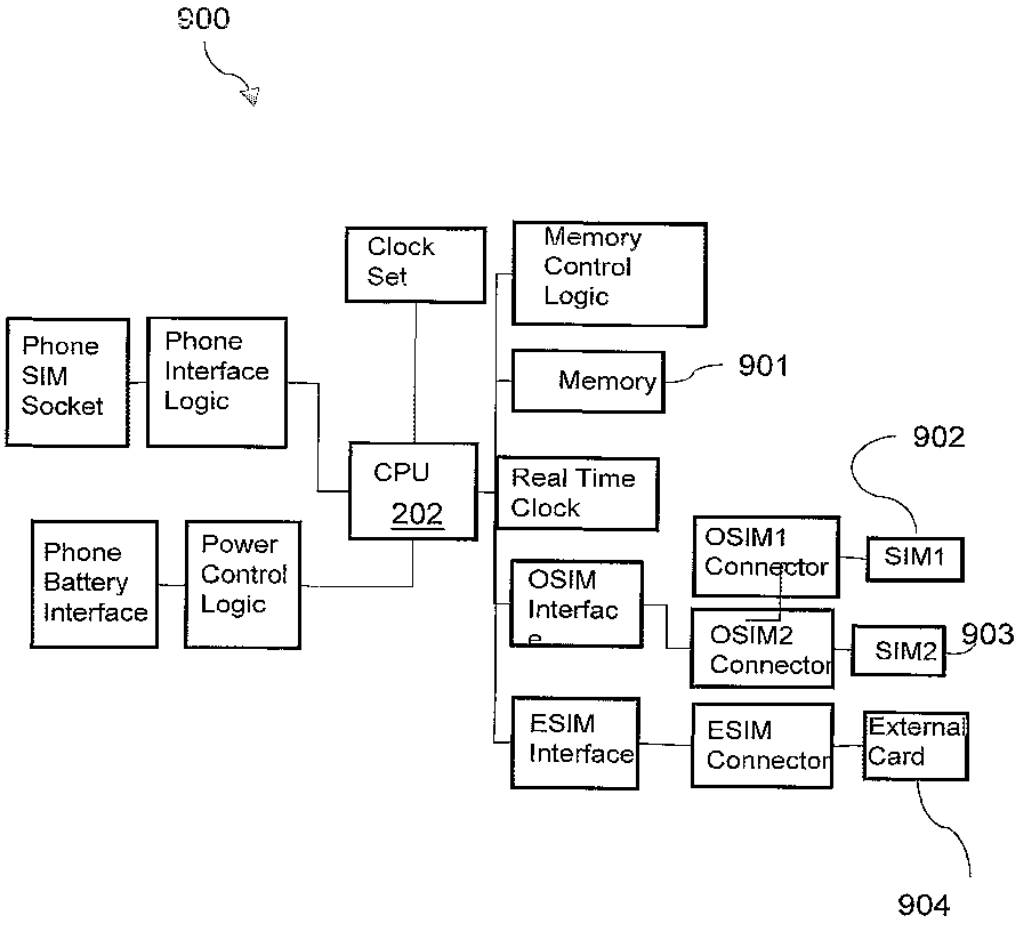

900
Clock Set
Memory Control Logic
Phone SIM Socket
Phone Interface Logic
Memory
901
CPU 202
Real Time Clock
902
Phone Battery Interface
Power Control Logic
OSIM Interfac e
OSIM1 Connector
SIM1
OSIM2 Connector
SIM2
903
ESIM Interface
ESIM Connector
External Card
904

FIG. 10

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 June 2004 (24.06.2004)

PCT

(10) International Publication Number
WO 2004/053640 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2003/038692

(22) International Filing Date: 5 December 2003 (05.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/431,567 6 December 2002 (06.12.2002) US

(71) Applicant *(for all designated States except US)*: **WAY SYSTEMS, INC.** [US/US]; 200 Unicorn Park, Woburn, MA 01801 (US).

(71) Applicants and
(72) Inventors: **GOLDHWAITE, Scott** [US/US]; 15 Oregon court, Hingham, MA 02043 (US). **GRAYLIN, William** [US/US]; 229 Washington Street, Woburn, MA 01801 (US).

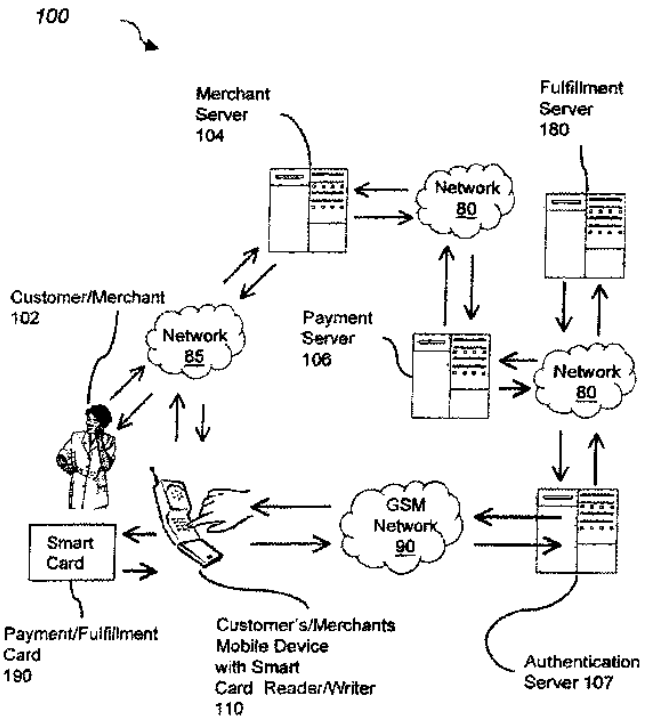
(74) Agent: **COLLINS, Aliki, K., PH., D.**; AKC Patents, 215 Grove Street, Newton, MA 02466 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR MOBILE PAYMENT AND FULFILMENT DIGITAL GOODS



(57) Abstract: An electronic payment and fulfillment system utilized by a customer for purchasing a digital good includes a merchant server 104, a payment server 106, an authentication server 107, a fulfillment server 180 and a communication device 110. The communication device 110 includes a payment card module and the payment card module receives a payment card 190 and reads payment card identification information stored in the payment card. The communication device 110 transmits the payment card identification information to the payment server 106 and then receives the digital good from the fulfillment server 180 and stores it onto the payment card 190. Communications from and to the communication device 110 pass through the authentication server 107.

WO 2004/053640 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 306 of 1360

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR MOBILE PAYMENT AND FULFILLMENT OF DIGITAL GOODS

Cross Reference to related Co-Pending Applications

This application claims the benefit of U.S. provisional application Serial No. 60/431,567 filed on December 6, 2002 and entitled SYSTEM AND METHOD FOR MOBILE PAYMENT AND FULFILLMENT OF DIGITAL GOODS which is commonly assigned and the contents of which are expressly incorporated herein by reference.

This application is also a continuation in part of U.S. applications Serial No. 10/205,768, 10/625,823, and 10/695,585, filed on July 26, 2002, July 23, 2003, and October 28, 2003, and entitled "SYSTEM AND METHOD FOR PAYMENT TRANSACTION AUTHENTICATION", "MOBILE DEVICE EQUIPPED WITH A CONTACTLESS SMART CARD READER/WRITER", and "MOBILE COMMUNICATION DEVICE EQUIPPED WITH A MAGNETIC STRIPE READER", respectively, the contents of which applications are expressly incorporated herein by reference.

Field of the Invention

The present invention relates to a system and a method for mobile payment and fulfillment of digital goods, and more particularly to a mobile payment transaction and fulfillment of digital goods with a strong authentication.

Background of the Invention

Smart Cards used in the financial services industry are rapidly replacing magnetic stripe cards. The primary reason for the migration to smart cards is the increased level of security that smart cards can provide. Smart Cards have an embedded Integrated Circuit (IC) that enables a highly secure computing environment to store sensitive information, such as credit card information, medical information, digital certificates and biometric data. Smart Cards are also used as a secure repository for "digital goods", such as electronic cash (e-Cash), electronic tickets (e-Tickets), electronic coupons (e-Coupons), loyalty points (i.e. frequent flyer miles, frequent shopper points), credits for pre-paid mobile airtime, credits for pre-paid utilities, and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 308 of 1360

digital rights management (DRM) certificates for accessing multi-media applications. The greatest use of these "e-Purses" on smart cards are e-Cash schemes from Visa International and MONDEX International and transit token systems that comply to the MIFARE (Philips) and Octopus (Sony). While the use of smart cards has been the catalyst for e-Purse business, the challenge is the expense in installing and maintaining the card reader/writer infrastructure required to enable users to "top up" or "reload" or "download" digital goods and monetary value to their smart cards. Typically, users can load/reload digital goods and value onto the card by using an Automated Teller Machine (ATM), a kiosk or a Point of Sale (POS) system in a store to transfer money from a checking account, savings account, a credit card account or by inserting cash into the ATM. These ATMs are typically located at the entrance to the transit stations, small merchant stores and bank outlets. The number and availability of the smart card reader/writer equipment determine the amount of usage of smart cards. There is a need for a secure, low cost system that can be used to fulfill and pay for digital goods.

Summary of the Invention

This invention features an electronic payment and digital good fulfillment system utilized by a customer to pay for the purchase of a good and/or a service with a physical or virtual payment instrument. The present invention provides consumers or merchants with the ability to download digital goods such as electronic cash (e-Cash), electronic coupons (e-Coupon), electronic tickets (e-Ticket), electronic transit tokens, credits for pre-paid mobile airtime, credits for pre-paid utilities, credits for other types of pre-paid accounts, a digital receipt or ticket that can be utilized at a later point to further receive digital goods (i.e., a Hidden Rechargeable Number "HRN" for pre-paid top up), digital rights management (DRM) certificates and digital media such as music, software, movies, books and other digital content to a smart card, contactless smart card or magnetic stripe card.

In general, in one aspect of this invention features an electronic payment and fulfillment system utilized by a customer for purchasing a digital good including a merchant server, a payment server, an authentication server, a communication device, and a fulfillment server. The merchant server is programmed to receive a purchase order from the customer for the purchase of the digital good, and to create a digital

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 309 of 1360

order comprising purchase order information. The payment server is programmed to receive the digital order from the merchant server and to further route the digital order. The authentication server is programmed to receive the digital order from the payment server, format the digital order into a first message and further route the first message. The communication device includes a payment card module and the payment card module is adapted to receive a payment card and read payment card identification information stored in the payment card. The communication device is also adapted to receive the first message from the authentication server, display the first message to the customer, request and receive authorization for payment for the purchase order with the payment card from the customer, retrieve the payment card identification information, request and receive payment card security information from the customer, and route the authorization and the payment card identification and security information to the authentication server. The authentication server further routes the authorization and payment card identification and security information to the payment server and from the payment server to a financial institution. The financial institution is asked to execute the payment and to send a payment confirmation through the payment server to the merchant server and to the authentication server. The fulfillment server is programmed to receive the payment confirmation from the payment server and transmit the digital good via the authentication server to the communication device. The communication device then stores the digital good onto the payment card.

Implementations of this aspect of the invention include the following. The communication device may be a wireless communication device or a wired communication device. The merchant server, the payment server, the authentication server, the fulfillment server and the communication device are adapted to send and receive messages among each other via a first network and the wireless communication device is adapted to send and receive messages to the authentication server via a second network and the second network may be a wireless network. The wireless communication device may be a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, programmable versions thereof or combinations thereof. The wireless network may be a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) or a private communication network The wireless wide

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 310 of 1360

area network (WWAN) may be a Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access (CDMA), CDMA 2000, or wideband CDMA (WCDMA). The wired communication device may be a telephone and the first network may be a telecommunications network. The wired communication device may be a computer and the first network may be the Internet. The payment card may be a smart card such as a full size smart card, a contactless smart card, a SIM smart card, a USIM smart card, a credit card, a debit card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card or combinations thereof. The payment card may be a magnetic stripe card. The merchant server may receive the purchase order from the customer via the Internet, telephone connection, mail order form, fax, e-mail, voice recognition system, shot message service, interactive voice recording (IVR), or face-to-face communication with the customer. The wireless communication device may have a subscriber identification module (SIM) card slot and the payment card module may be electrically connected to the SIM card slot. The payment card information may be cardholder identification information, card identification information, authentication information, card issuer information, or financial institution information. The digital good may be electronic cash, electronic tickets, electronic coupons, loyalty points, credits for pre-paid mobile airtime, credits for pre-paid utilities, electronic gift certificates, digital rights managements (DRM) certificates, electronic transit tokens, music, software, movies, or books. The merchant server and the fulfillment server may be one entity. The customer may place the purchase order to the merchant server via the communication device. The communication device may further include a shopping application and the customer may utilize the shopping application, to select the digital good, to place the purchase order, to authorize, authenticate and pay with the payment card, and to store the digital good onto the payment card. The payment card module may include a payment card reader and writer module. The communication device may further include a digital good generation application and the digital good generation application may receive a digital receipt for the digital good and generate the digital good. The first message may have a format such as Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), or proprietary message formats.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 311 of 1360

In general in another aspect the invention features an electronic payment and fulfillment method utilized by a customer for purchasing a digital good including placing a purchase order with a merchant server for the digital good and choosing to pay via a communication device. Next, providing the merchant server with identification information for the communication device and creating a digital order comprising purchase order information and the identification number for the communication device by the merchant server. Next, routing the digital order to a payment server and from the payment server to an authentication server. Next, formatting the digital order into a first message by the authentication server and routing the first message to the communication device. Next, displaying the first message on the communication device and requesting and receiving authorization of payment from the customer. Next, retrieving identification information of a payment card from the communication device and requesting and receiving security information of the payment card from the customer via the communication device. Next, routing the authorization and the payment card identification and security information through the authentication server to the payment server and from the payment server to a financial institution. Next, executing the payment at the financial institution and sending a payment confirmation to the payment server. Next, routing the payment confirmation from the payment server to the merchant server and to a fulfillment server and transmitting the digital good from the fulfillment server via the authentication server to the communication device. Finally, storing the digital good onto the payment card by the communication device.

Among the advantages of this invention may be one or more of the following. Combining a smart card reader (contact or contactless) with a mobile phone can dramatically increase the number of smart card reader points of sales in the marketplace to create more convenience for consumers and more opportunities for merchants. Consumers or merchants with a mobile phone equipped with a smart card reader would be able to load value to their cards (contact or contactless) anytime, anywhere. Using a secure, non-repudiatable payment enables the secure over-the-air download of digital goods. In countries or locations where a "land-line" telephone connection required by an Automated Teller Machine (ATM) or merchant Point of

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 312 of 1360

Sale (POS) system is either too expensive or not feasible, a mobile device equipped with a smart card reader is significantly more cost effective and convenient.

Brief Description of the Drawings

FIG. 1 is a schematic diagram of a system for digital goods purchase and fulfillment using a mobile device with a smart card reader according to this invention.

FIG. 2 illustrates prior art circuitry for the mobile device attachment that converts a Single-SIM GSM phone into a Dual-SIM/Dual-Slot GSM phone.

FIG. 3 illustrates circuitry for a mobile device attachment that converts a Single-SIM GSM phone into a Dual-SIM/Dual-Slot GSM phone with a contactless smart card reader/writer.

FIG. 4 is a diagram of a payment and digital goods fulfillment system according to this invention.

FIG. 4A is a diagram of another embodiment of a payment and digital goods fulfillment system according to this invention.

FIG. 4B is a diagram of another embodiment of a payment and digital goods fulfillment system according to this invention.

FIG. 4C is a diagram of another embodiment of a payment and digital goods fulfillment system according to this invention.

FIG. 5 illustrates circuitry for a mobile device attachment that converts a Single-SIM GSM phone into a Dual-SIM/Dual-Slot GSM phone with a magnetic stripe card reader/writer.

FIG. 6 is a flow diagram for a shopping application on a mobile device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 313 of 1360

FIGS. 6A – 6L illustrate an example user scenario for mobile payment and digital goods fulfillment.

Detailed Description of the Invention

The present invention provides a smart card payment and digital goods fulfillment system. The smart card has the ability to retain stored value or other types of information within the card. These "digital goods" are electronic, virtual information that represents value such as electronic cash (e-Cash), electronic coupons (e-Coupon), electronic tickets (e-Ticket), electronic transit tokens, credits for pre-paid mobile airtime, credits for pre-paid utilities, credits for other types of pre-paid accounts, a digital receipt or ticket that can be utilized at a later point to further receive digital goods (i.e., a Hidden Rechargeable Number "HRN" for pre-paid top up), digital rights management (DRM) certificates and digital media such as music, software, movies, books and other digital content. The payment transaction and digital goods fulfillment system allows the purchase of digital goods and reception and storage of the digital goods on a smart card.

Referring to FIG. 1 and FIG 4, a payment transaction and digital goods fulfillment system 100 includes a customer 102 with a smart card 190 and a mobile phone device 110 equipped with a smart card reader/writer, a merchant server 104, a payment server 106, an authentication system 108, a financial institution 112 and a fulfillment server 180. The authentication system 108 includes an authentication server 107 that is adapted to send and receive messages in a short message service (SMS) format to the mobile phone 110 via an SMS carrier 109. The mobile phone 110 is adapted to receive the payment card 190 or has a built-in payment card (not shown). After having placed an order for digital goods via the Internet, Short Message Service (SMS), Wireless Application protocol (WAP), or voice 85, customer 102 is asked to choose a payment method. The customer 102 chooses to pay via her mobile phone 110 and gives her mobile phone identification information to the merchant server 104 (114). In one example, the mobile phone identification information is the mobile phone number. The merchant server 104 routes the customer's mobile phone number and information about the purchase order to the payment server 106 (116). The payment server 106 contacts the authentication server 107 and routes the customer's mobile phone number and information about the purchase (118). The authentication

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 314 of 1360

server 107 sends an SMS message to the customer's mobile phone 110 through an SMS carrier 109 (120). The customer 102 receives the SMS message asking her to authorize the purchase and choose a payment card (122). The customer 102 authorizes the purchase, uses the smart card 190 that is associated with her mobile phone 110 (188) and enters a security code associated with the smart card to pay and authenticate her purchase (124). In one example, the security code is a personal identification number (PIN). Other examples include a password, digital signature, and a biometric identifier, i.e., retina scan, fingerprint, DNA scan, voice characteristics. The payment card 190 is identified with information that is embedded in the card. In one example the identification information is a payment card number. Other examples of payment card identification include an encrypted transaction signature that can only be decrypted by the financial institution that has issued the payment card, expiration date of the payment card, and a digital signature. The mobile phone 110 sends an SMS message via the SMS Carrier 109 to the authentication server 107. The SMS message includes the authorization result and payment transaction information (126). The authentication server 107 routes the authorized purchase order and authenticated card to the payment server 106 (128). The payment server 106 contacts the financial institution 112 that has issued the payment card and routes the payment card information and the purchase order information (130). The financial institution 112 processes the payment transaction and sends a confirmation of the payment transaction to the payment server 106 (132). The payment server 106 routes the payment confirmation to the merchant server 104 (134), presents a digital receipt to the fulfillment server 180(181) and routes the payment confirmation to the authentication server 107 (136). The authentication server 107 sends an SMS message confirming the payment transaction to the customer's mobile phone 110 (138). Finally the fulfillment server 180 fulfills the customer's order for digital goods by sending the electronic information that represents the digital goods to the authentication server 107 (140). The authentication server 107 transfers the digital goods and sends an SMS message to the customer's mobile phone 110 through the SMS carrier 109 (120). The mobile phone 110 receives the digital goods from the authentication server 107 and the customer 102 receives a message that digital goods are available for the smart card. Finally, the digital goods are transferred from the mobile phone 110 to the smart card 190 (189).

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 315 of 1360

The message routing 114 occurs over communication network 85, message routing 116, 134, occurs over communication network 82, message routing 118, 128, 136 occurs over communication network 86, message routing 120, 122, 124, 126, 138, occurs over communication network 90, and message routing 130, 132, occurs over communication network 84. Communication between the authentication server 107 and the SMS carrier 109 occurs over network 88, and communication between the fulfillment server 180 and the authentication server 107 is over network 80. In one example, communication networks 80, 82, 84, 85, 86, and 88 are the Internet and communication network 90 is a wireless network. In another example communication network 85 is wireless or wire line, voice or data network. The wireless network 85 and 90 may be a Wireless Wide Area Network (WWAN) (i.e., GSM, TDMA, CDMA, 3G, iDEN, Mobitex, and DataTac), a Wireless Local Area Network (WLAN) (i.e., 802.11a, 802.11b), or a Personal Area Network (PAN) (i.e., Bluetooth, Infrared). Other examples of communication networks 80, 82, 84, 85, 86, 88 and 90 include private voice and data networks, and public voice and data networks. Message routing 114-140 is encrypted.

In the embodiments of FIG. 1 and FIG.4, the fulfillment server 180 and the merchant server 104 are two separate entities. For example, the merchant server 104 contains the merchant catalog of music or documents that can be downloaded and the fulfillment server 180 is the storage repository for the actual digital media. In another embodiment the fulfillment server 180 and the merchant server 104 are the same entity (not shown).

In the embodiment of FIG. 4A an order is initiated directly from the mobile phone device. The customer 102 interacts with a shopping application 600 on the mobile phone device 110 (shown in FIG. 6 and FIGS. 6A – 6L) to initiate, place, authorize and fulfill an order.

Referring to FIG. 4A, the system for placing an order directly from the mobile phone device includes a customer 102 with a smart card 190 and a mobile phone device 110 equipped with smart card reader/writer, a merchant server 104, a payment server 106, an authentication system 108, a financial institution 112 and a fulfillment server 180. The authentication system 108 includes an authentication server 107 that is adapted to

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 316 of 1360

send and receive messages in a short message service (SMS) format to mobile phone 110 via an SMS carrier 109. The mobile phone 110 is adapted to receive the payment card 190 or has a built-in payment card (not shown). The customer 102 makes the purchase selection on the mobile device using a shopping application 600 and is prompted to authorize the purchase and choose a payment card (122). The customer 102 authorizes the purchase, uses a smart card 190 that is associated with her mobile phone 110 (188) and enters a security code associated with the smart card to pay and authenticate her purchase (124). The mobile phone 110 sends an SMS message via the SMS Carrier 109 to the authentication server 107(126). The SMS message includes the order details, merchant information, authorization result, and payment transaction information. The authentication server 107 routes the authorized purchase order and authenticated card to the payment server 106 (128). The payment server 106 contacts the financial institution 112 that has issued the payment card and routes the payment card information and the order information (130). The financial institution 112 processes the payment transaction and sends a confirmation of the payment transaction to the payment server 106 (132). The payment server 106 routes the payment confirmation to the merchant server 104 (134), presents a digital receipt to the fulfillment server 180 (181) and routes the payment confirmation to the authentication server 107 (136). The authentication server 107 sends an SMS message confirming the payment transaction to the customer's mobile phone 110 (138). Finally the fulfillment server 180 fulfills the customer's order for digital goods by sending the electronic information that represents the digital goods to the authentication server 107 (140). The authentication server 107 transfers the digital goods and sends an SMS message to the customer's mobile phone 110 through the SMS carrier 109 (120). The mobile phone 110 receives the digital goods from the authentication server 107 and the customer 102 receives a message that digital goods are available for the smart card and the digital goods are transferred to the smart card 190 (189).

In one example the mobile phone device 110 is a programmable device, such as a Personal Digital Assistance (PDA)-type phone and the shopping application 600 is a series of menus on the mobile phone device that guide the customer through the shopping process. In another example, the mobile phone device 110 is a non-programmable phone and the shopping application 600 is an application that is

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 317 of 1360

installed on the mobile phone and accessed via the phone's interface. Referring to FIG. 6 and FIG. 6A to FIG. 6L, the shopping application 600 includes the following operations. The customer 102 selects a transit ticket purchase application on her PDA-type phone (602). Next, the customer 102 selects the desired fare amount (604). Alternatively, the customer 102 selects the origin station (605), the destination station (606), the fare type (607), and the fare is calculated by the application (608). Next, the customer 102 initiates the payment transaction and inserts a payment card (610). Next, the customer 102 selects the payment instrument on the card (i.e., VISA, Master Card, Amex) (612), and authenticates the payment transaction with her PIN number (614). If her PIN number is valid (616) the transaction is transmitted to the authentication server 107 and processed by the payment server 106, merchant server 104, financial institution 112, and fulfillment server 180 (618). When the payment is confirmed and the desired fare amount is ready to be transferred to the transit card, the application 600 prompts the customer 102 to insert her transit card in the phone card reader (620). Finally, the desired fare amount is transferred to the transit card (622) and the transaction is completed (624).

Referring to FIG. 4B, in another embodiment, the authentication server 107 presents the digital receipt to the fulfillment server. Following the payment authorization from the financial institution 112 a confirmation of the payment transaction is transmitted to the payment server 106 (132). The payment server 106 routes the payment confirmation to the merchant server 104 (134) and routes the payment confirmation to the authentication server 107 (136). The authentication server 107 sends an SMS message confirming the payment transaction to the customer's mobile phone 110 (138) and then presents a digital receipt to the fulfillment server 180 (181). The fulfillment server 180 fulfills the customer's order for digital goods by sending the electronic information that represents the digital goods to the authentication server 107 (140). The authentication server 107 transfers the digital goods and sends an SMS message to the customer's mobile phone 110 through the SMS carrier 109 (120). The mobile phone 110 receives the digital goods from the authentication server 107 and the customer 102 receives a message that digital goods are available for the smart card and the digital goods are transferred to the smart card 190 (189).

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 318 of 1360

Referring to FIG. 4C, in another embodiment, the mobile phone device receives a digital receipt that is then transmitted to the smart card, and is then utilized by an application on the smart card such as a transit token or e-Cash application as the authorization to generate digital goods. Following the payment authorization from the financial institution 112 a confirmation of the payment transaction is transmitted to the payment server 106 (132). The payment server 106 routes the payment confirmation to the merchant server 104 (134) and routes the payment confirmation to the authentication server 107 (136). The authentication server 107 sends a digital receipt 110 and an SMS message confirming the payment transaction to the customer's mobile phone (138). The mobile phone 110 receives the confirmation message and the digital receipt for digital goods from the authentication server 107 and the customer 102 receives a message that digital goods are available. An application on the smart card or on the mobile phone generates the digital goods based on the information contained within the digital receipt. The digital goods are created and transferred to the smart card 190 (189).

In another embodiment, the payment authentication instrument may be contained on one or many Subscriber Identity Module (SIM) smart cards for GSM wireless networks or Universal Subscriber Identity Module (USIM) smart cards for 3G wireless networks within the mobile phone 110, or within full-size smart cards inserted into a smart card reader 153 that is either attached to or embedded in the mobile phone device 110 or contained on a contactless smart card that can be accessed by a mobile phone device 110 with a contactless reader. The general concept of connecting additional smart card readers by implementing a connection to the existing SIM connector on a mobile phone is defined in the prior art "Communication Method and Apparatus Improvements" (PCT International Publication Number WO 99/66752), the entire content of which is incorporated herein by reference. This prior art defines the implementation of a mobile phone device attachment 200 that utilizes a Central Processor Unit to coordinate the activities of multiple SIM cards and full-size smart cards (See FIG. 2). The prior art defines the basic design of a mobile phone that provides a smart card reader either attached to the phone as an accessory or embedded into the design of the phone. Co-pending patent application entitled "Mobile Device Equipped with a Contactless Smart Card Reader", the entire content of which is incorporated herein by reference, describes a mobile phone that provides a

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 319 of 1360

"contactless" smart card reader 300 to read/write data to a contactless smart card (see FIG. 3).

In another embodiment, the receiver of the digital goods can be one or many Subscriber Identity Module (SIM) smart cards for GSM wireless networks or Universal Subscriber Identity Module (USIM) smart cards for 3G wireless networks within the mobile phone 110, or a full-size smart cards inserted into a smart card reader that is either attached to or embedded in the mobile phone device 110 or a contactless smart card that can be accessed by a mobile device 110 with a contactless reader or the mobile phone itself.

In another embodiment, the payment authentication card can be a magnetic stripe payment card that is accessed by the mobile phone device utilizing the magnetic stripe card reader 500 described in a co-pending patent application entitled "Mobile Communication Device Equipped with a Magnetic Stripe Reader", the entire content of which is incorporated herein by reference, (see FIG 5).

Other embodiments are within the scope of the following claims. For example, the smart card reader and/or payment card reader is adapted to connect to the mobile phone device through the mobile phone device's accessory connection point such as serial, USB, Compact Flash, Infrared, Bluetooth and Secure Digital. The digital goods may be fulfilled to a dual-interface contact/contactless smart card, or to a multi application "combi" contact/contactless smart card. The authentication of the customers Personal Identification Number (PIN) may be processed online at the financial institution or with a third-party server-side wallet account. The payment instrument may an account established with a server-side wallet. A browser on the mobile device may be utilized for entering the payment information. The payment information may be verbally transcribed to a customer service representative or a speech recognition system. The payment information may also be transcribed utilizing an Interactive Voice Response system. The digital goods are transferred to a customer's virtual or server-side account. The digital goods that are downloaded may be a digital receipt for goods to be fulfilled at a later time by the customer such as the online generation of a Hidden Rechargeable Number (HRN) for pre-paid top up that the customer will utilize to top up a pre-paid mobile, utility or other type of pre-paid

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 320 of 1360

account. The mobile device may be held by a merchant to accept payment from and fulfill digital goods to a plurality of customers. In addition to SMS messaging via the SMS Carrier 109 between the authentication server 107 and the mobile phone 110, the communication between the authentication server 107 and the mobile phone 110 may be via a proprietary message protocol that utilizes User Datagram Protocol (UDP) on top of Internet Protocol (IP). This proprietary message protocol is adapted to be used with wireless networks that support Transmission Control Protocol/Internet Protocol (TCP/IP). These wireless networks include Bluetooth, 3G, GPRS, 2.5G, Infrared, WCDMA, CDMA200, 802.11a and 802.11b. The mobile phone identification information may be an Internet Protocol (IP) address. The communication networks 80, 82, 84, 86, 88 and 90 may be wireless or wired networks. The communication networks 80, 82, 84, 86, 88 and 90 may be non face-to-face via the Internet, VPN (Virtual Private Network), cable network, data network, telephone network, private voice and data networks, public voice and data networks, and mail or person to person. Payment card identification may occur via the payment card number or via an encrypted transaction signature that can only be decrypted by the financial institution that has issued the payment card. The authentication server may also utilize a password, digital signature, or a biometric identifier, i.e., retina scan, fingerprint, voice characteristics, to authenticate the payment transaction. The payment authentication instrument may be contained in the contactless smart card, on the SIM smart cards within the mobile phone 110, or within another full-size smart card that needs to be inserted into a smart card reader slot. The communication mobile phone device may be a mobile wireless device and the second network may be a wireless network. The mobile wireless device may be a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, or combinations thereof. The second network may be a wireless wide area network (WWAN), a wireless local area network (WLAN) or a wireless personal area network (PAN). The communication device may also be a wired communication device and the second network may be a wired network. The wired communication device may be a telephone or a computer and the wired network may be a telecommunications network or the Internet, respectively. The first network may be the Internet or a telecommunication network.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 321 of 1360

Several embodiments of the present invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the following claims.

What is claimed is:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 322 of 1360

1. An electronic payment and fulfillment system utilized by a customer for purchasing a digital good comprising:

a merchant server adapted to receive a purchase order from said customer for the purchase of said digital good, and to create a digital order comprising purchase order information;

a payment server adapted to receive said digital order from said merchant server and to further route said digital order;

an authentication server adapted to receive said digital order from said payment server, format said digital order into a first message and further route said first message;

a communication device comprising a payment card module wherein said payment card module is adapted to receive a payment card and read payment card identification information stored in said payment card, and wherein said communication device is adapted to receive said first message from said authentication server, display said first message to said customer, request and receive authorization for payment for said purchase order with said payment card from said customer, retrieve said payment card identification information, request and receive payment card security information from said customer, and route said authorization and said payment card identification and security information to the authentication server, and wherein said authentication server further routes said authorization and payment card identification and security information to said payment server and from said payment server to a financial institution, wherein said financial institution is asked to execute said payment and to send a payment confirmation through said payment server to said merchant server and to said authentication server; and

a fulfillment server adapted to receive said payment confirmation from said payment server and transmit said digital good via said authentication server to said communication device, wherein said communication device stores said digital good onto said payment card.

2. The system of claim 1 wherein said communication device comprises a wireless communication device.

3. The system of claim 1 wherein said communication device comprises a wired communication device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 323 of 1360

4. The system of claim 3 wherein said merchant server, said payment server, said authentication server, said fulfillment server and said communication device are adapted to send and receive messages among each other via a first network.

5. The system of claim 2 wherein said merchant server, said payment server, said authentication server, and said fulfillment server are adapted to send and receive messages among each other via a first network and said wireless communication device is adapted to send and receive messages to said authentication server via a second network and wherein said second network comprises a wireless network.

6. The system of claim 2 wherein said wireless communication device is selected from a group consisting of a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, programmable versions thereof and combinations thereof.

7. The system of claim 5 wherein said wireless network is selected from a group consisting of a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) and a private communication network.

8. The system of claim 7 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

9. The system of claim 4 wherein said wired communication device comprises a telephone and said first network comprises a telecommunications network.

10. The system of claim 4 wherein said wired communication device comprises a computer and said first network comprises the Internet.

11. The system of claim 1 wherein said payment card comprises a smart card selected from a group consisting of a full size smart card, a contactless smart card, a SIM smart card, a USIM smart card, a credit card, a debit card, a stored-value card, a

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 324 of 1360

coupon card, a reward card, an electronic cash card, a loyalty card, an identification card and combinations thereof.

12. The system of claim 1 wherein said payment card comprises a magnetic stripe card.

13. The system of claim 1 wherein said merchant server receives said purchase order by said customer via a route selected from a group consisting of the Internet, telephone connection, mail order form, fax, e-mail, voice recognition system, shot message service, interactive voice recording (IVR), and face-to-face communication with the customer.

14. The system of claim 2 wherein said wireless communication device comprises a subscriber identification module (SIM) card slot and said payment card module is electrically connected to said SIM card slot.

15. The system of claim 1 wherein said payment card information is selected from a group consisting of cardholder identification information, card identification information, authentication information, card issuer information, and financial institution information.

16. The system of claim 1 wherein said digital good is selected from a group consisting of electronic cash, electronic tickets, electronic coupons, loyalty points, credits for pre-paid mobile airtime, credits for pre-paid utilities, electronic gift certificates, digital rights managements(DRM) certificates, electronic transit tokens, music, software, movies, and books.

17. The system of claim 1 wherein said merchant server and said fulfillment server comprise one entity.

18. The system of claim 1 wherein said customer places said purchase order to said merchant server via said communication device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 325 of 1360

19. The system of claim 1 wherein said communication device further comprises a shopping application and wherein said customer utilizes said shopping application, to select said digital good, to place said purchase order, to authorize, authenticate and pay with said payment card, and to store said digital good onto said payment card.

20. The system of claim 1 wherein said payment card module comprises a payment card reader and writer module.

21. The system of claim 1 wherein said communication device further comprises a digital good generation application and wherein said digital good generation application receives a digital receipt for said digital good and generates said digital good.

22. The system of claim 1 wherein said first message comprises a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

23. An electronic payment and fulfillment method utilized by a customer for purchasing a digital good comprising:

placing a purchase order with a merchant server for said digital good and choosing to pay via a communication device;

providing said merchant server with identification information for said communication device;

creating a digital order comprising purchase order information and said identification number for said communication device by said merchant server;

routing said digital order to a payment server and from said payment server to an authentication server;

formatting said digital order into a first message by said authentication server and routing said first message to said communication device;

displaying said first message on said communication device and requesting and receiving authorization of payment from the customer;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 326 of 1360

retrieving identification information of a payment card from said communication device;

requesting and receiving security information of said payment card from said customer via said communication device;

routing said authorization and said payment card identification and security information through said authentication server to said payment server and from said payment server to a financial institution;

executing said payment at said financial institution and sending a payment confirmation to said payment server;

routing said payment confirmation from said payment server to said merchant server and to a fulfillment server;

transmitting said digital good from said fulfillment server via said authentication server to said communication device; and

storing said digital good onto said payment card by said communication device.

24. The method of claim 23 wherein said communication device comprises a payment card module adapted to receive said payment card and read said payment card identification information stored in said payment card and to receive a digital good and store said digital good onto said payment card.

25. The method of claim 23 wherein said communication device comprises a wireless communication device.

26. The method of claim 23 wherein said communication device comprises a wired communication device.

27. The method of claim 26 wherein said merchant server, said payment server, said authentication server, said fulfillment server and said communication device are adapted to send and receive messages among each other via a first network.

28. The method of claim 25 wherein said merchant server, said payment server, said authentication server, and said fulfillment server are adapted to send and receive messages among each other via a first network and said wireless communication

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 327 of 1360

device is adapted to send and receive messages to said authentication server via a second network and wherein said second network comprises a wireless network.

29. The method of claim 25 wherein said wireless communication device is selected from a group consisting of a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, programmable versions thereof and combinations thereof.

30. The method of claim 28 wherein said wireless network is selected from a group consisting of a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) and a private communication network.

31. The method of claim 30 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

32. The method of claim 26 wherein said wired device comprises a telephone and said first network comprises a telecommunications network.

33. The method of claim 26 wherein said wired device comprises a computer and said first network comprises the Internet.

34. The method of claim 23 wherein said payment card comprises a smart card selected from a group consisting of a full size smart card, a contactless smart card, a SIM smart card, a USIM smart card, a credit card, a debit card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card and combinations thereof.

35. The method of claim 23 wherein said payment card comprises a magnetic stripe card.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 328 of 1360

36. The method of claim 23 wherein said placing a purchase order comprises placing a purchase order via a route selected from a group consisting of the Internet, telephone connection, mail order form, fax, e-mail, voice recognition system, shot message service, interactive voice recording (IVR), and face-to-face communication with the customer.

37. The method of claim 24 wherein said communication device comprises a subscriber identification module (SIM) card slot and said payment card module is electrically connected to said SIM card slot.

38. The method of claim 23 wherein said payment card information is selected from a group consisting of cardholder identification information, card identification information, authentication information, card issuer information, and financial institution information.

39. The method of claim 23 wherein said digital good is selected from a group consisting of electronic cash, electronic tickets, electronic coupons, loyalty points, credits for pre-paid mobile airtime, credits for pre-paid utilities, electronic gift certificates, digital rights managements(DRM) certificates, electronic transit tokens, music, software, movies, and books.

40. The method of claim 23 wherein said merchant server and said fulfillment server comprise one entity.

41. The method of claim 23 wherein said customer places said purchase order to said merchant server via said communication device.

42. The method of claim 23 wherein said communication device further comprises a shopping application and wherein said customer utilizes said shopping application, to select said digital good, to place said purchase order, to authorize, authenticate and pay with said payment card, and to store said digital good onto said payment card.

43. The method of claim 24 wherein said payment card module comprises a payment card reader and writer module.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 329 of 1360

44. The method of claim 23 wherein said communication device further comprises a digital good generation application and wherein said digital good generation application receives a digital receipt for said digital good and generates said digital good.

45. The method of claim 23 wherein said first message comprises a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 330 of 1360

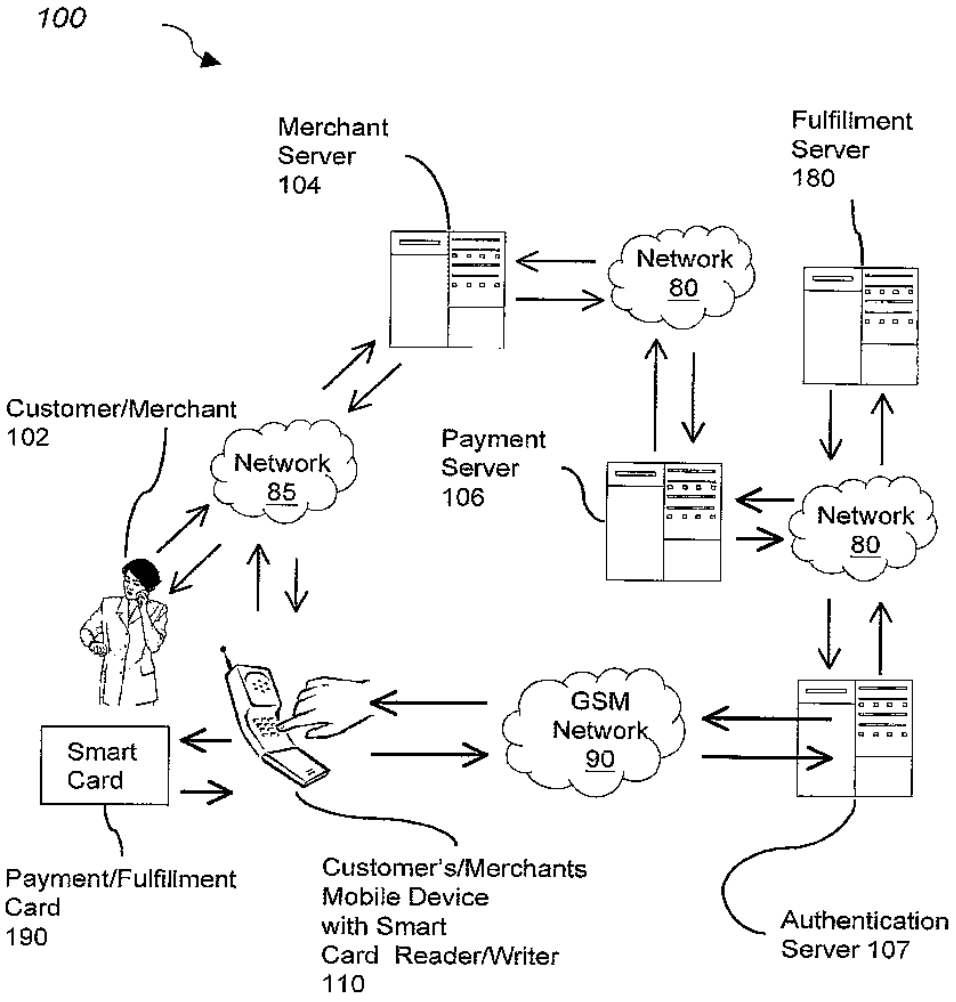

100
Merchant Server 104
Fulfillment Server 180
Network 80
Customer/Merchant 102
Network 85
Payment Server 106
Network 80
GSM Network 90
Smart Card
Payment/Fulfillment Card 190
Customer's/Merchants Mobile Device with Smart Card Reader/Writer 110
Authentication Server 107

FIG. 1

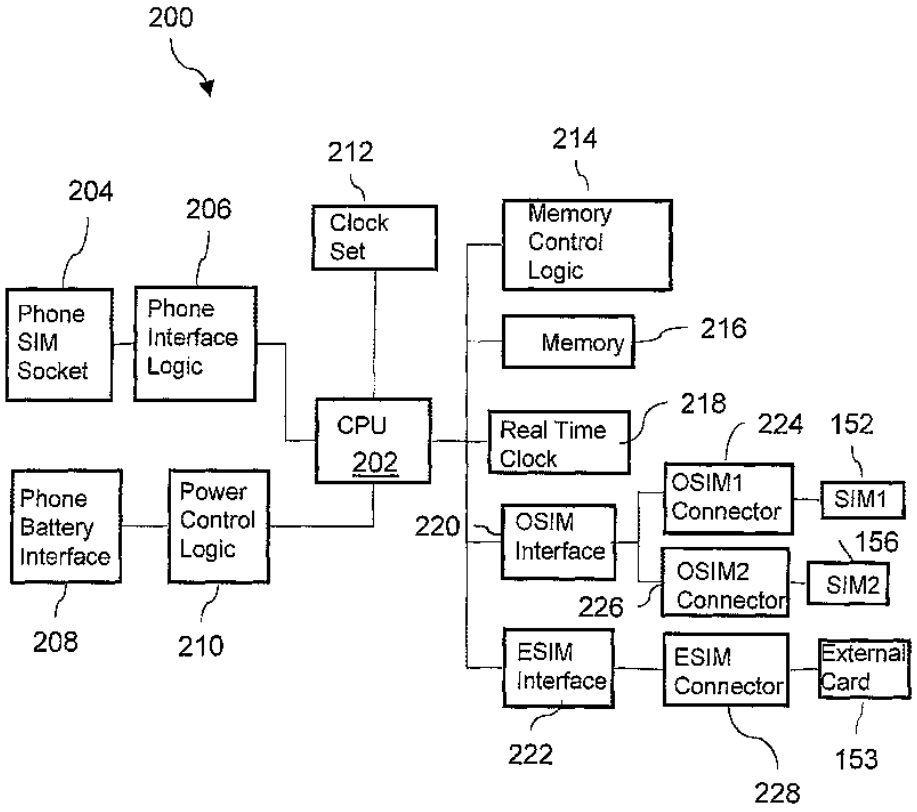


FIG. 2
(Prior Art)

300

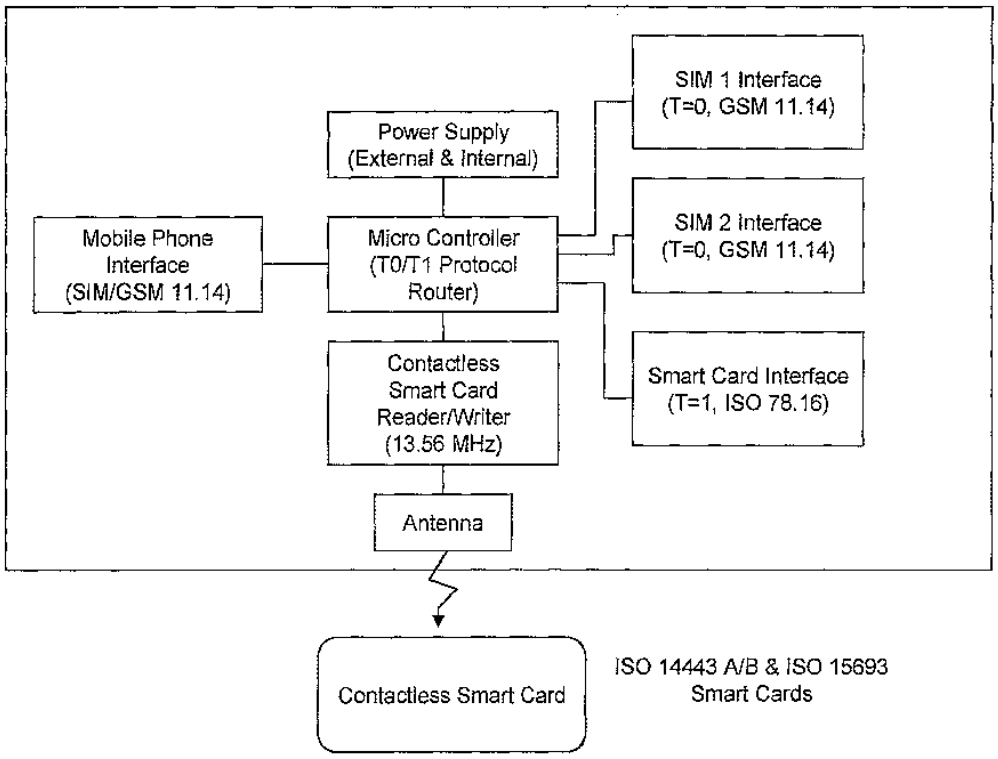

SIM 1 Interface
(T=0, GSM 11.14)
Power Supply
(External & Internal)
SIM 2 Interface
(T=0, GSM 11.14)
Mobile Phone
Interface
(SIM/GSM 11.14)
Micro Controller
(T0/T1 Protocol
Router)
Smart Card Interface
(T=1, ISO 78.16)
Contactless
Smart Card
Reader/Writer
(13.56 MHz)
Antenna
Contactless Smart Card
ISO 14443 A/B & ISO 15693
Smart Cards

FIG. 3

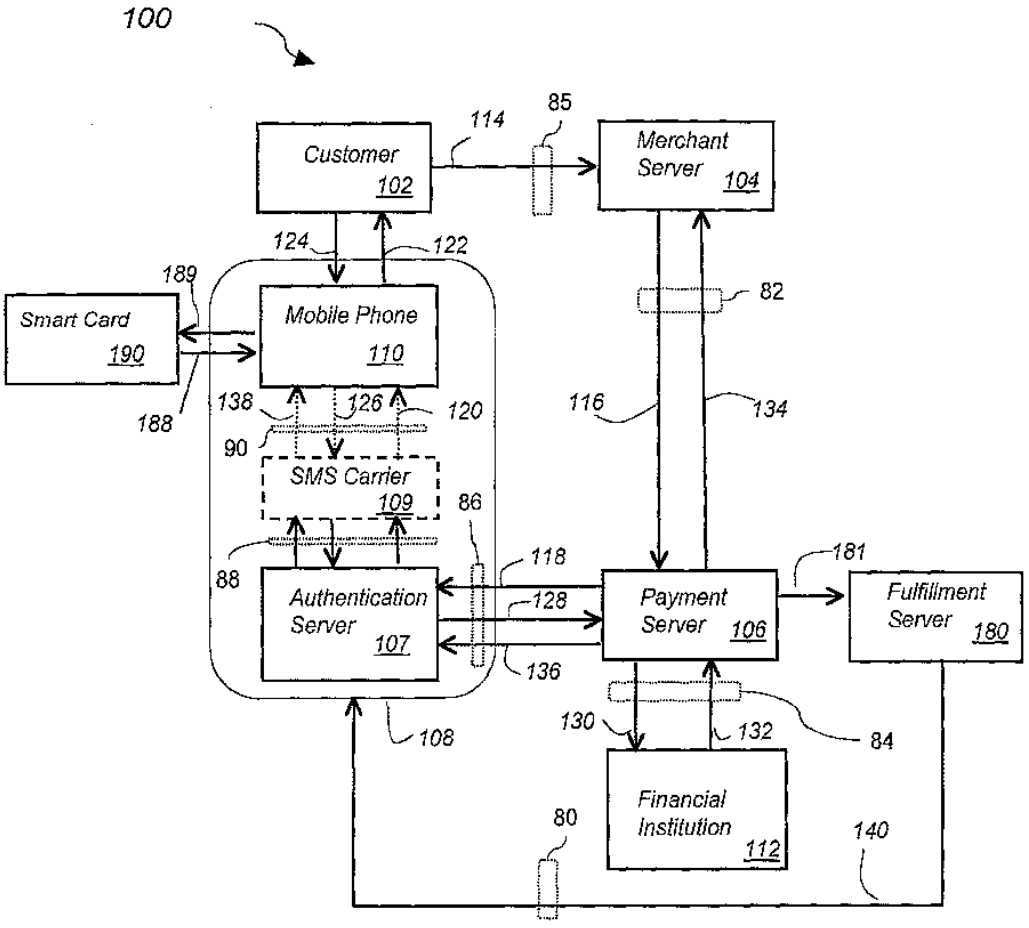

100
Customer 102
114
85
Merchant Server 104
124
122
189
Smart Card 190
Mobile Phone 110
82
138
126
120
116
134
188
90
SMS Carrier 109
86
88
118
181
Authentication Server 107
128
Payment Server 106
Fulfillment Server 180
136
130
132
84
108
Financial Institution 112
80
140

FIG. 4

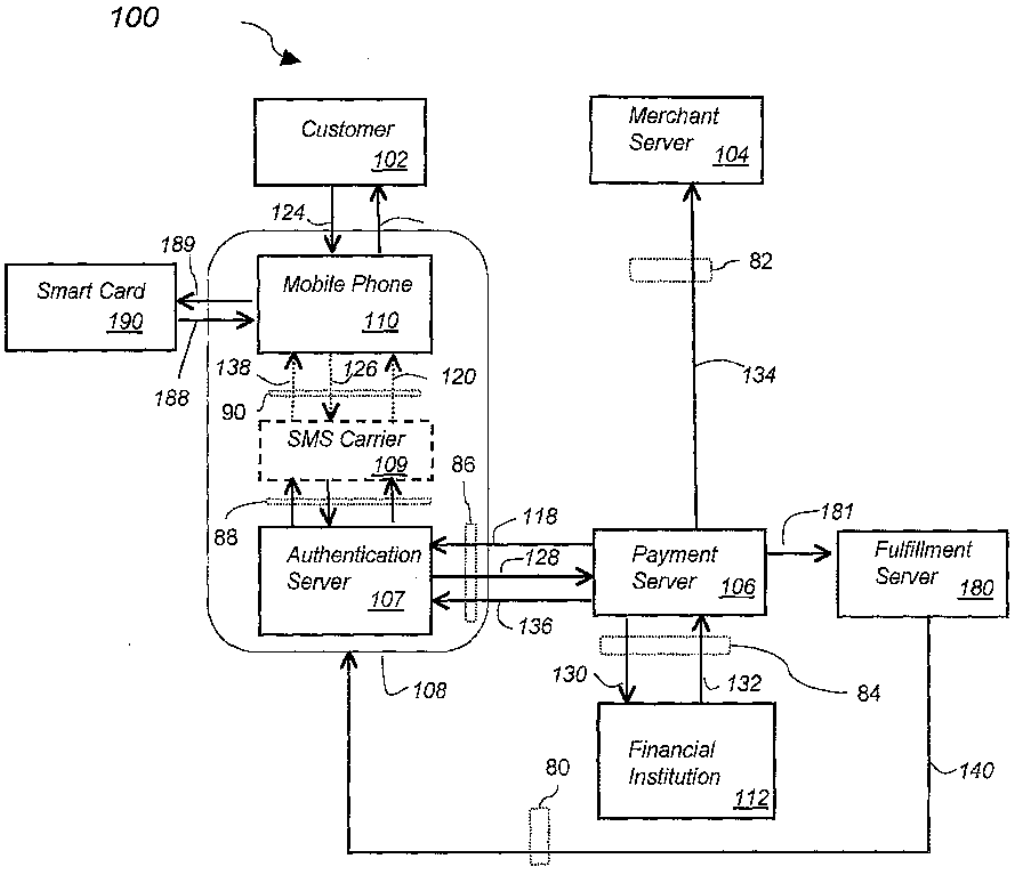

100
Customer 102
Merchant Server 104
124
189
Smart Card 190
Mobile Phone 110
82
138
126
120
134
188
90
SMS Carrier 109
86
118
181
88
Authentication Server 107
128
Payment Server 106
Fulfillment Server 180
136
130
132
84
108
Financial Institution 112
80
140

FIG. 4A

6/16

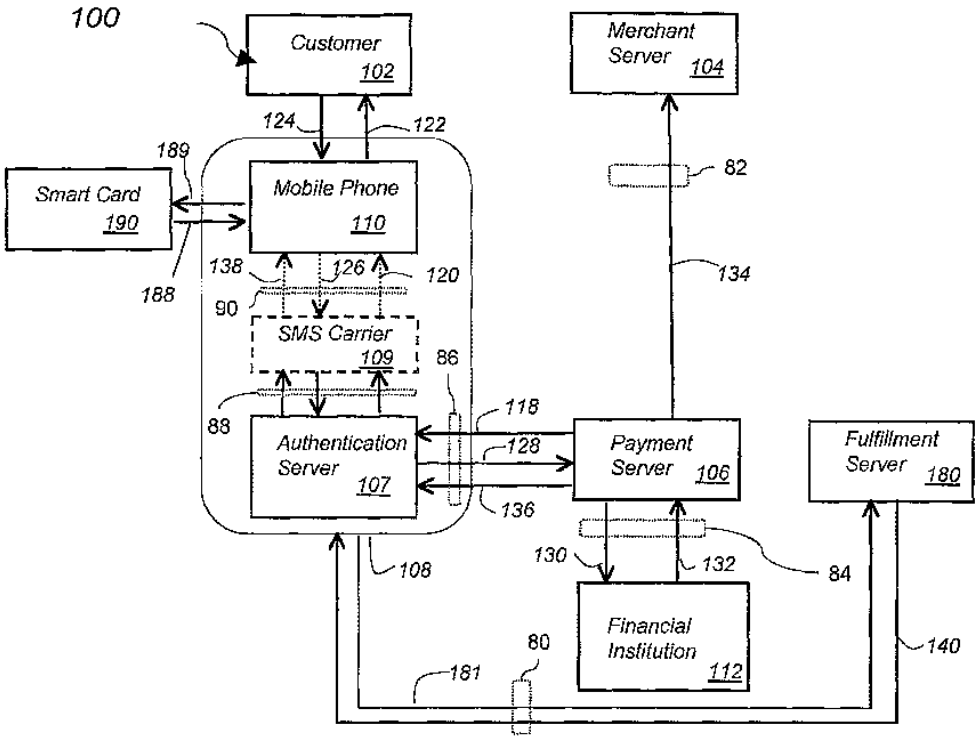

100
Customer 102
Merchant Server 104
124
122
189
Smart Card 190
Mobile Phone 110
82
138
126
120
134
188
90
SMS Carrier 109
86
118
88
Authentication Server 107
128
Payment Server 106
Fulfillment Server 180
136
130
132
84
108
Financial Institution 112
80
140
181

FIG. 4B

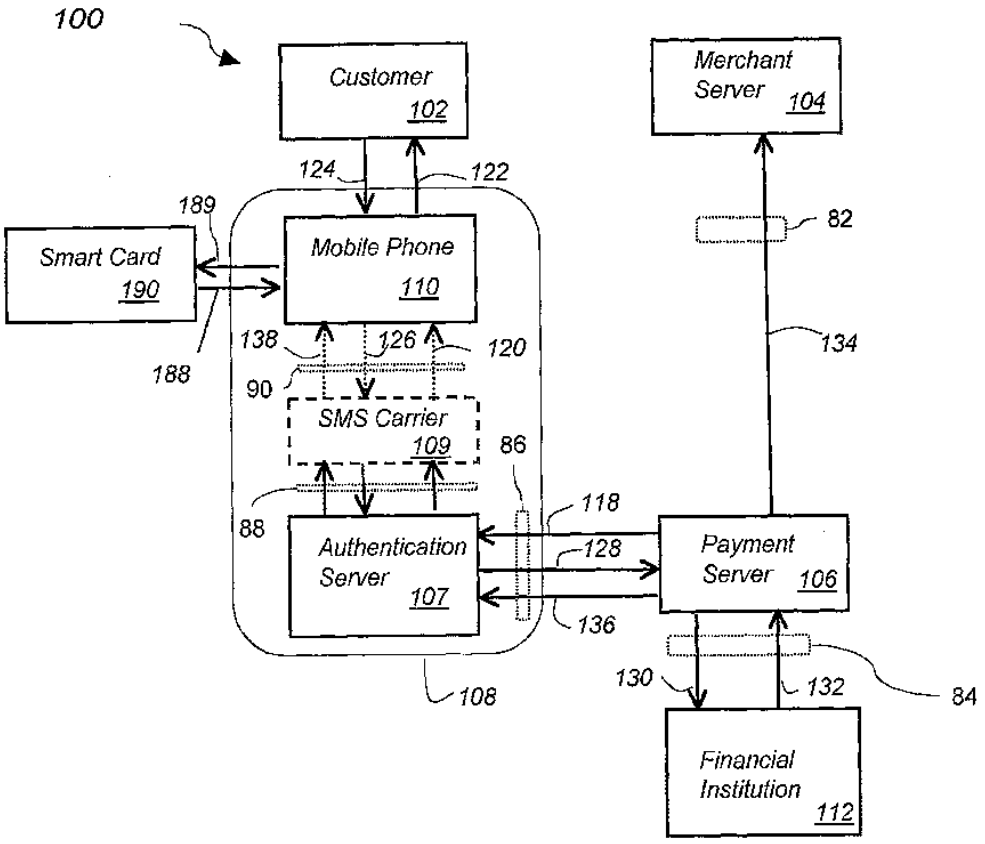

100
Customer
102
Merchant
Server
104
124
122
189
Smart Card
190
Mobile Phone
110
82
138
126
120
134
188
90
SMS Carrier
109
86
118
88
Authentication
Server
107
128
Payment
Server
106
136
130
132
84
108
Financial
Institution
112

FIG. 4C

500

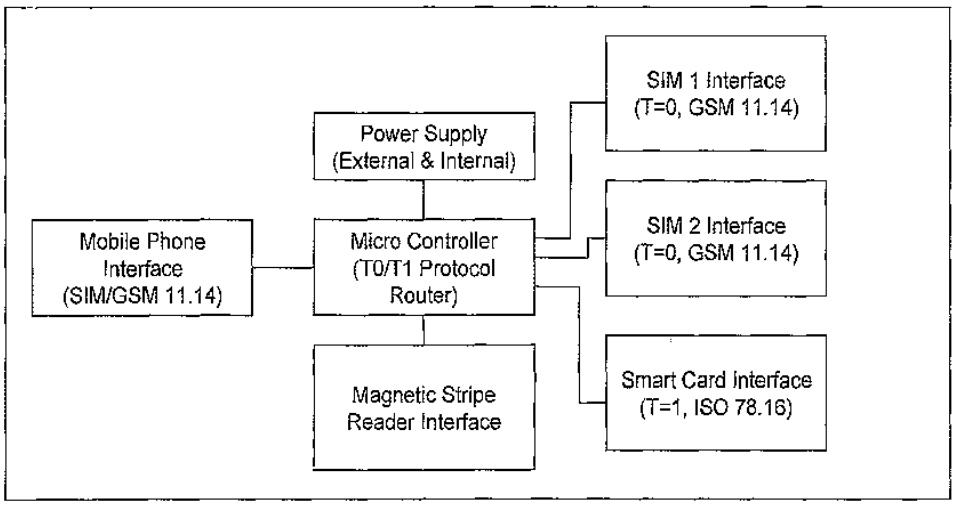


FIG. 5

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 338 of 1360

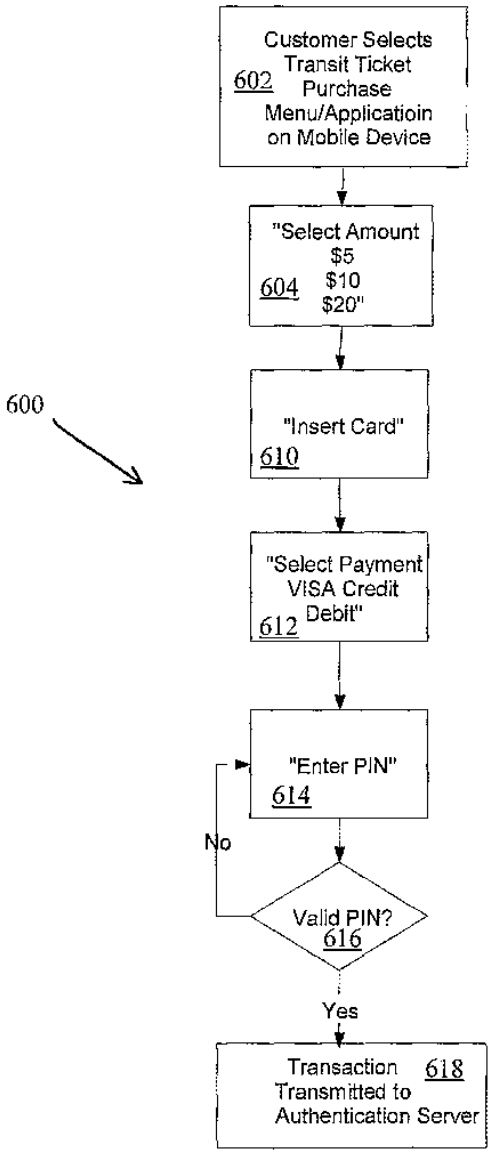

600
Customer Selects Transit Ticket Purchase Menu/Applicatioin on Mobile Device
602
"Select Amount $5 $10 $20"
604
"Insert Card"
610
"Select Payment VISA Credit Debit"
612
"Enter PIN"
614
No
Valid PIN?
616
Yes
Transaction Transmitted to Authentication Server
618

FIG. 6

602

Customer chooses the Purchase Ticket option from the Phone's GO Transit Menu.

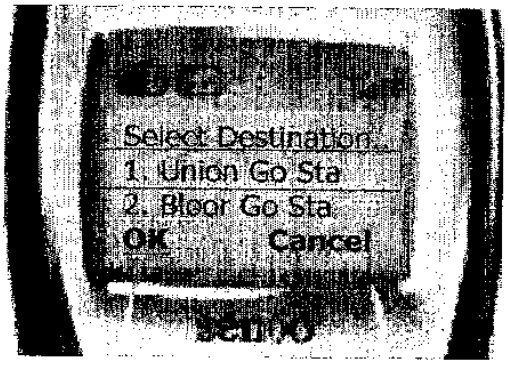
FIG. 6A

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 340 of 1360

605

Customer Selects Origin...

FIG. 6B

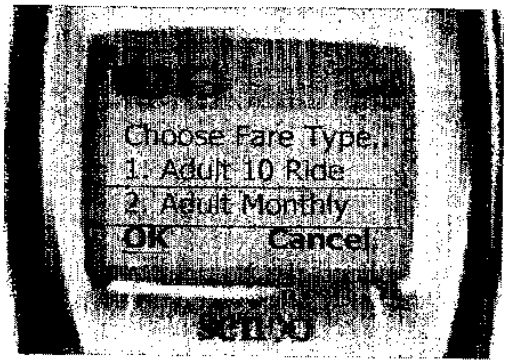


606

Customer Selects Destination...

FIG. 6C

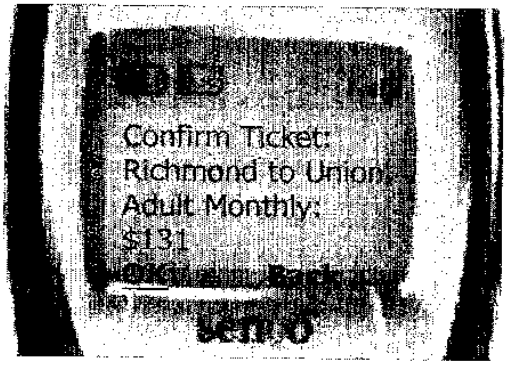
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 341 of 1360



607

Customer chooses fare type...

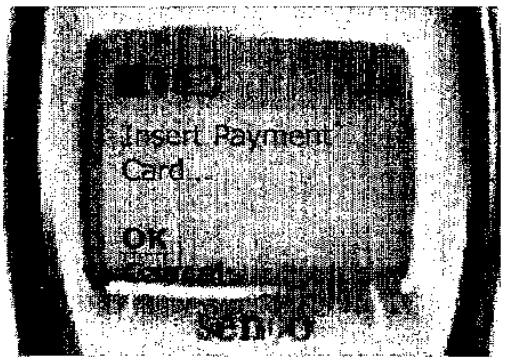
FIG. 6D



608

Fare is calculated and customer confirms ticket purchase

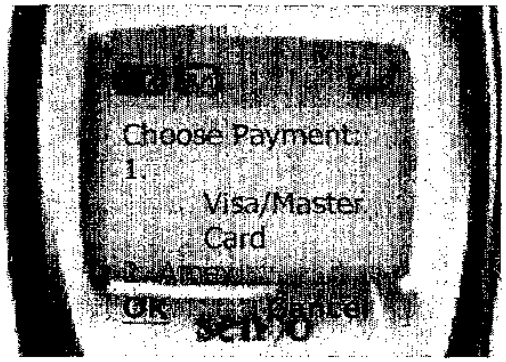
FIG. 6E



610

Customer Initiates Payment and Inserts Payment Card

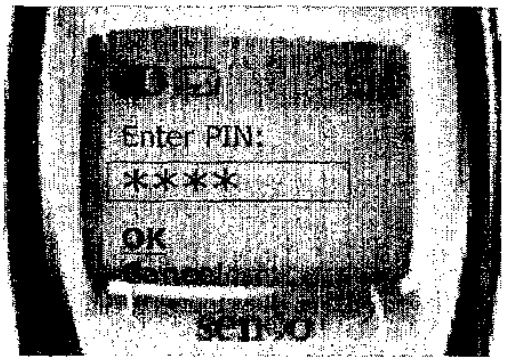
FIG. 6F



612

Customer Selects Payment Instrument on Card

FIG. 6G



614

Customer Authenticates transaction with Personal Identification Number (PIN)

FIG. 6H

618

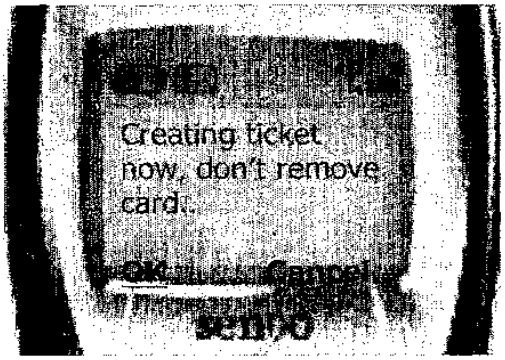
Transaction Transmitted to Authentication Server and then processed by Merchant, Financial Institution and Fulfillment Server

FIG. 6I

620

Customer presents transit card to the mobile phone

FIG. 6J

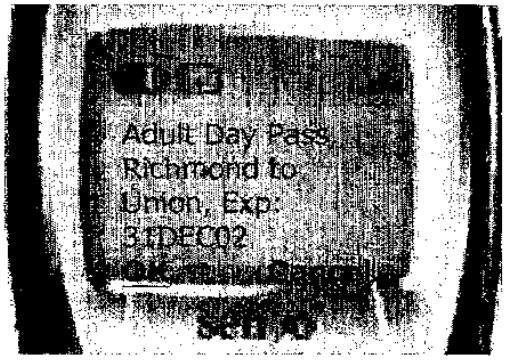


622

Digital Goods are fulfilled to the Transit Card

FIG. 6K

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 345 of 1360



624

Digital Goods fulfillment is completed

FIG. 6L

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 September 2002 (12.09.2002)

PCT

(10) International Publication Number
WO 02/071354 A2

(51) International Patent Classification[7]: G07F 19/00

(21) International Application Number: PCT/CA02/00272

(22) International Filing Date: 4 March 2002 (04.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/272,300 2 March 2001 (02.03.2001) US

(71) Applicant *(for all designated States except US)*: **SOFT TRACKS ENTERPRISES LTD.** [CA/CA]; Suite 1258, 13351 Commerce Parkway, Richmond, British Columbia V6V 2X7 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SWAIN, Alan, L.** [CA/CA]; 9740 Snowdon Avenue, Richmond, British Columbia V7A 2M1 (CA). **WOO, Kevin, K., M.** [CA/CA]; 10368 - 167th Street, Surrey, British Columbia V4N 1Z2 (CA).

(74) Agent: **FASKEN MARTINEAU DUMOULIN LLP**; Toronto Dominion Bank Tower, Box 20, Suite 4200, Toronto Dominion Centre, Toronto, Ontario M5K 1N6 (CA).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/071354 A2

(54) Title: SYSTEM AND METHOD FOR FACILITATING AN M COMMERCE TRANSACTION

(57) Abstract: A method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, the method comprising the steps of receiving at an application server first information indicative of the transaction device authentication; receiving at the application server second information for verification of the user; and using both the first and second information to authorise top-up payment of the prepaid service.

SYSTEM AND METHOD FOR FACILITATING AN M-COMMERCE TRANSACTION

BACKGROUND OF THE INVENTION

Payments in commercial transactions have evolved over time, from cash transactions, to credit card transactions to present day payment via electronic devices. Each step in the evolution has spawned its own industry and infrastructure, and successive levels in the evolution have built on the existing infrastructure. Collectively these infrastructures and processes are referred to as the payment industry.

While wireless and Internet technologies are fuelling change within the current payment industry, there is a need for new innovative payment solutions, which leverage the hard earned trust of existing financial institutions. It is the eventual goal to effect a transformation of the payment industry by enabling secure and trusted payments, in any form of tender, via any electronic device.

In general, mobile e-commerce (m-commerce) is defined as online purchasing of goods and services, including subscription based services, such as news, music and financial services, using a mobile phone service. A major challenge inhibiting widespread adoption of m-commerce solutions today is that purchasers often do not trust a mobile device as a secure way of making online payments.

A first step in overcoming this challenge is to involve the wireless carrier as the merchant in selling its own prepaid subscription service in real time. Mobile carriers currently provide three prepay top up solutions. In the first solution, customers purchase a card such as a magnetic stripe card or similar encoding mechanism to indicate that the customer has paid a predetermined prepaid value for the card. These so-called "prepaid vouchers" are purchased at retail outlets. The code on the prepaid voucher is read by the purchaser and communicated either directly on the phone with a carrier customer service representative, or through the carrier's IVR (Interactive Voice Response) system. The code represents a monetary value, which may be added

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 348 of 1360

to the balance of the customer's prepaid account maintained by the carrier. A second solution is payment via credit card, wherein credit card information is either communicated to a carrier's customer service representative via voice or through a PC based web interface. A third solution involves customers prepaying for airtime through automated telemachines (ATM's). This solution is similar to prepaid vouchers in that a code printed on the ATM receipt is communicated to the carrier's customer service representative or entered through the carrier's IVR system.

As may be seen, none of the above solutions allow immediate, secure, authenticated and non-repudiable prepay top up of the customers pre paid value via the customer's wireless telephone or similar device. Because of this, current pre-paid solutions are not as successful as anticipated.

It is thus an objective of the present invention to mitigate some of the above disadvantages.

SUMMARY OF THE INVENTION

One objective of the present invention is to enable authenticated credit transactions and real time payment for top-up of prepaid cellular phones, which uses existing interfaces at both the cell phone carrier network and at the financial institution effecting the top up payment.

In accordance with this invention there is provided a method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, the method comprising the steps of receiving at an application server first information indicative of the transaction device authentication; receiving at the application server second information for verification of the user; and using both the first and second information to authorize top-up payment of the prepaid service

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 349 of 1360

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the preferred embodiments of the invention will become more apparent in the following detailed description in which reference is made to the appended drawings wherein:

Figure 1 is schematic diagram of a payment system according to the present invention;

Figure 2 is a schematic diagram of a payment system according to one embodiment of the invention;

Figure 3 is a schematic diagram of a payment system according to another embodiment of the invention;

Figures 4, 5, 6 and 7 show ladder diagrams for use-case scenarios of the system of figure 3.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following description like numerals refer to like structures in the drawings. For convenience, the definitions, acronyms, and abbreviations used in the description are listed in table 1

Table I

Acronym/ Abbreviation	Expansion
TGS	Transaction Gateway Server
AS	Application Server
RTP	Real Time Payment
MWS	Merchant Wallet Server
VTS	Virtual Terminal Server
IVR	Interactive Voice Response
MT	Mobile Terminal
CDPD	Cellular Digital Packet Data

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 350 of 1360

Acronym/ Abbreviation	Expansion
ASCII	American Standard Code for Information Interchange

Referring now to Figure 1, there is shown a block diagram of the main components in a system 100 for facilitating prepaid-type transactions according to an embodiment of the present invention. This system includes an application server (AS) 120 for processing transaction requests from at least one wireless device 122, such as a cellular telephone, the application server 120 is also capable of forwarding transactions to an acquiring financial institution 124a or an issuing financial institution depending on whether the transaction is, respectively, a credit card transaction or a real time payment (RTP) transaction. A real time payment transaction refers to a payment mechanism where funds from the purchaser's bank account are debited in near real time. The system 100 also includes a merchant wallet server (MWS) 126, which acts as a proxy between a Virtual Terminal Server (VTS) and one or more electronic wallets (e-Wallets) 130 containing user credit card numbers, bank ATM card numbers or bank account numbers, stored value account numbers, billing addresses and shipping addresses stored in a carrier subscriber database 132. The MWS is able to extract information from the e-wallets130 and present them in a form that can be used by the VTS. In effect, the MWS acts as a front end to the VTS, enabling the support of m-commerce.

Credit card and RTP transactions may also be sent through a transaction gateway server (TGS) 134 to the acquiring bank's 124a interface.

The system 100 may also include carrier's IVR server 136, which transmits payment information to the AS. Payment information captured by a carrier's IVR system is sent to the AS in the same manner as that of a WAP enabled phone. Information entered by the IVR system is combined with information stored at the carrier's subscriber database. Credit card and RTP transactions are then routed to a TGS. The

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 351 of 1360

TGS is an optional intermediary in communication with the various financial institutions.

The prepaid transactions of the present invention are facilitated by payment applications (PA) running on the AS. The AS is a multi-application server, which allows for a variety of different payment methods and tender types. The payment applications have support for tender types such as credit card, cash, cheque, and e-Wallets. The e-Wallets themselves may contain references to credit cards, bank accounts, and stored value accounts. In addition, the payment application has an Enterprise Reporting feature allowing reports on usage per subscriber. An important feature of the AS is the ability to route the prepay transactions to the appropriate processing interface based on the payment type. In the case of WAP enabled digital phones, the owner of the prepaid mobile device communicates with the AS via the payment application residing on the AS. Information entered by the user, along with information kept within the carrier's prepaid database / e-Wallet is aggregated in the AS. The AS handles payment types as described below.

The payment types supported by the system 100 are generally credit card transactions and RTP transactions. With each of these payment types, there are different levels of device 122 and user authentication, different interface requirements, and differences in response mechanisms. The transaction types implemented will require mutual resolution and agreement between the parties.

Non-Face-To-Face Transactions Using Credit Cards

In a credit card transaction, only the credit card number of the prepaid user is stored in a subscriber e-Wallet 130. This is what is currently used to effect Internet based payment. There is no authentication for the card or account, no authentication of the owner of the card or account and no authentication of the owner's intent to complete the transaction as is evidenced in a card present credit card transaction when the card is swiped and the owner signs the receipt or as is evidenced in an on-line debit transaction when the card is swiped and the owner of a debit card enters a secret PIN

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 352 of 1360

associated with the debit card. Rather, this type of transaction is typically called a Mail Order Telephone Order (MOTO) transaction. This does not fulfill general requirements of a go-to-market strategy for m-Commerce as these types of transactions can be easily repudiated and hence are highly subject to fraud. This invention enables m-commerce transactions that can generally not be repudiated. This invention meets the general requirements for non-repudiation of ensuring that the transaction process itself requires something that only the consumer has in possession and that the consumer intended to complete the transaction by requiring consumer to securely disclose to the system, something that only the consumer knows. The challenge of m-Commerce to achieve this is made even more difficult as often, the consumer and the merchant are not face-to-face as is the case with a an on-line credit card or an on-line debit card transaction.

Credit Card with Subscriber Device Authentication

Subscriber handset identities (SID) are commonly used within cellular networks to authenticate user phones. In this case, a credit card number is associated with the phone's secure identity to satisfy the concept of a virtual card. Currently, to effect a card present transaction, the card must be physically swiped and the data (called track2 data) on the magstripe of the card must be captured. If a trust relationship is set up between the carrier and the financial institution, the combination of the phone's secure identity and credit card number represents an equivalent risk to a card present transaction. This may be referred to as a "virtual card present transaction".

Credit Card with Subscriber Device & Password Authentication

Building on the virtual credit card transaction, a password can be associated with the subscriber's e-Wallet. The password is used to authenticate the owner of the e-Wallet (i.e. the subscriber), allowing access to the associated virtual credit card contained in the e-Wallet. User authentication lowers the risk of fraud involved in using a virtual credit card. By agreement between the owner of the e-Wallet and the e-Wallet service provider, the use of a password to authenticate the subscriber can be considered as a replacement for a signed receipt for purposes of non-repudiation.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 353 of 1360

RTP through EFT

The AS can route RTP transactions via the TGS to an Electronic Funds Transfer (EFT) interface of banks. This mechanism transfers money from the subscriber's bank account to the merchant's bank account overnight. The attractiveness of EFT is the ability to handle transactions for all banks through one interface. The EFT backend deals with the transfer of funds between the individual banks. A limitation of the EFT interface is that payment transfers are typically delayed up to 24 hours, and are not immediate. Responses are typically batched into one file and extracted from the EFT interface, when the file is available. Therefore, prepay top up transactions may take up to 24 hours before receiving a response from the bank, hence failing to meet a real time acknowledgement requirement.

This delay is addressed in one of several ways. A first option is that the financial institution processes and acknowledges an EFT transaction in real time in a scenario where the merchant (i.e. carrier) account and subscriber account is within its own domain. A second option is that a notification is sent to the subscriber some time in advance when the number of minutes still remaining in the subscriber's prepay account is below a certain level so that the 24-hour delay is inconsequential.

RTP through Real Time Payment Gateway

The AS can route RTP transactions via the TGS to evolving bank interfaces. The goal of these interfaces is to process funds transfer transactions in real time. Transactions belonging to the bank, hosting the interface, may be processed in real time. These interfaces, often based on XML standards such as OFX, provide a real time confirmation for a given transaction, unlike an EFT interface. Real time responses allow a subscriber to issue a payment transaction online and wait for the acknowledgement. Within this scenario the financial institution can only process and acknowledge transactions in real time when the subscriber holds an account at that bank.

Debit Transactions

With Debit transactions networks such as the Interac™ network the underlying principles of authentication can be satisfied with today's cellular security and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 354 of 1360

authentication technologies, hence making debit transactions acceptable, most especially in the closed environment of prepay.

As described earlier, the MWS acts as a proxy between the VTS and e-Wallets that hold subscriber credentials. The MWS combines information from e-Wallets and information entered from either the carrier's IVR system or the WAP based prepay application. The information is used to construct a credit or RTP transaction. Once a successful response message is received, the MWS is responsible for notifying both the user of the mobile device, and the carrier's prepay subscriber database. The response can be sent to the WAP based prepay application or the carrier's IVR system. In the case that the subscriber database held at the carrier receives a successful response, the appropriate amount is added to the user's prepaid account.

Another feature of the MWS is the ability for a merchant to be authenticated as part of the transaction. Merchant credentials can be securely stored within the MWS and can be included in the transaction details, if the bank requires. This is a major step towards having the ability to authenticate both the subscriber and the merchant in a financial transaction. Optionally, if a PKI-enabled MWS is used, merchant credentials can be encrypted and digitally signed before sending the authentication to the bank. There are three e-Wallet configurations that the MWS supports.

Bank Hosted Wallet Server 140

The bank may choose to hold all of the subscriber's credentials within their own e-Wallet. The carrier's subscriber database is used as an authentication mechanism to enable payment through the bank e-Wallet. One authentication scheme involves the use of a token, which is stored at the subscriber database held at the carrier, and that token is used to extract subscriber credentials within the bank e-Wallet. This token can take the form of a PKI public key or certificate. If the prepay user has multiple e-Wallets with different banks, the carrier's subscriber database facilitates an authentication mechanism for each of the e-Wallets.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 355 of 1360

Carrier Hosted Wallet Server 130

The MWS can operate in an environment where a carrier hosts an e-Wallet. User information, along with credit card numbers and bank account numbers is held within the carrier's e-Wallet. This information is sent to the MWS, when a prepay top up transaction is being constructed. There is also a method for the MWS to update the user prepay account information at the carrier's subscriber database. In this scenario, the carrier subscriber database is proxied by the e-Wallet server. Therefore, once a response from a top up transaction is received, the MWS passes the details of the response to the e-Wallet server. The e-Wallet server, in turn, updates the users prepay account information held within the subscriber database.

Carrier and Bank Jointly Hosts the Wallet Server

The bank may choose to hold some of the e-Wallet credentials such as bank account information. They may also choose to hold only those credentials pertaining to the particular bank. This is an example of a multiple e-Wallet implementation. The MWS is capable of supporting connections to multiple e-Wallet servers whether they are hosted at the carrier or the bank.

While the overall system components, and payment types handle by the system have been describe above, the security mechanism implemented by the system 100 is now described.

Device Authentication

A device can be authenticated before any interactions with a financial institution. Carriers use subscriber identity authentication mechanisms and other security measures to safeguard the security and identity of a cellular phone. This technology, especially in the digital space has proven effective in authentication of mobile phones. The MWS solution builds on the carrier's authentication mechanisms. A devices authenticated identity is associated with a credit card number creating the notion of a virtual credit card. In actuality, the carrier's authentication procedure will enable the first step in granting access to a subscriber's e-Wallet that contains a subscriber's virtual credit cards. A password is used to authenticate the owner of the e-Wallet and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 356 of 1360

forms the second step in granting access to transact with the virtual credit cards in the e-Wallet.

User Authentication

To enable a prepay transaction, the carrier may choose to authenticate the user before accepting the transaction. There may be one or more passwords depending on the payment method. Typically, an e-Wallet password will be required to initiate a top up transaction. A second password may be needed to affect an RTP transaction. This is similar to an online bill payment scenario, where typically a username and password is required. The subscriber handset identity (SID) is used in place of the username. By agreement between the owner of the e-Wallet and the e-Wallet service provider, the use of a password to authenticate the subscriber can be considered as a replacement for a signed receipt for purposes of non-repudiation. PKI technologies will be implemented as these technologies mature within cellular devices.

Communication between Infrastructure Components

Standard Secure Sockets Layer (SSL) communications protocols are implemented on wide-area communications.

Referring to figure 2, there is shown another embodiment of the system 200 of the present invention. The system 200 comprises four interfaces into the AS, namely a carrier IVR system, carrier WAP gateway, carrier subscriber database via the e-Wallet, and the financial institution's acquiring interface via the TGS. It is noted that the carrier subscriber database is represented as an entity that accepts transaction responses and exception codes.

This implementation builds on the existing carrier infrastructure and requires only changes to the carrier's IVR system interface so that the IVR system communicates with the AS. All other four interfaces stay intact.

Prepay top up transactions can originate from either the carrier's IVR system or a WAP enabled phone. The IVR system communicates via an IP based connection into the AS business logic. XML based communications protocols may be used.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 357 of 1360

Whereas, the WAP enabled phone will access a prepay application hosted at the AS. Although, both mechanisms use different input strategies, the backend processing does not change.

The e-Wallet function has been split up into two components. The first component is an implementation of a simple e-Wallet for storage of subscriber payment information. The second component is the subscriber database that is currently in use at the carriers. When a top up transaction is created, user credentials are retrieved from the e-Wallet. This information is combined with the information entered by the user to affect the transaction. Once a transaction response has been received, an account update request is sent from the MWS to the subscriber database via the e-Wallet server. Both types of payment types are supported: credit card, and RTP.

Referring to figure 3, there is shown a further embodiment of an implementation of the system 100. In this scenario, the subscriber prepay database function has been separated from the client e-Wallet server. Once a transaction response has been received, an account update request is sent from the MWS directly to the subscriber database. Transaction details may be sent to the e-Wallet server to provide the subscriber with a transaction history.

Referring to figure 4, there is shown a ladder diagram describing a first use case for the embodiment of figure 3. This use-case describes a subscriber initiated prepay via WAP Phone scenario.

This scenario is a two-step transaction. The subscriber is involved in two phone sessions, where the second session is used as a further subscriber authentication step. The first session involves the subscriber affecting a prepay application. The prepay application may be accessible from either the WAP browser's default menu or by typing the URL of the application. The second session involves pushing an alert back to the subscriber. The second step removes the possibility that the original prepay transaction was not initiated by the intended subscriber. The subscriber ID of the

mobile device held within the e-Wallet defines the destination device of the push alert.

Each of the steps in the ladder diagram of figure 4 may be described as follows:

1. The subscriber enters the URL of WAP prepay application.
2. The carrier network validations ESN and MIN of subscriber phone.
3. Secure session is initiated with WAP gateway and prepay application host – the subscriber ID (SID) of the phone is passed to the application in the request header.
4. The subscriber is prompted by the prepay application for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.
5. Prepay application builds an XML based message and sends the message to the MWS. The request will minimally contain the SID for device authentication and optionally a password for subscriber authentication.
6. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.
7. Based on the SID, the subscriber's credentials are extracted from the e-Wallet. Optionally, if a password has been specified, the SID and password pair is authenticated against the SID and password held in the e-Wallet.
8. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.
9. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 359 of 1360

transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the SID extracted from the e-Wallet is sent to enable the WAP push mechanism in the next step.

10. The web server generates a WAP push message out to the subscriber device. The destination device can be determined by the SID. The push message can take the form of a real WAP push message through the WAP browser, or an indirect WAP push through the SMS messaging mechanism of the phone. In either case, the push message will contain a URL for triggering the prepay transaction. To complete the authentication loop, the URL will consist partly of the transaction ID of the temporary prepay transaction held at the MWS.

11. The subscriber authorizes the prepay transaction by selecting the URL and confirming the transaction.

12. The prepay web server sends a second XML based request to the MWS, which is an authorization request (confirmation) of the original prepay transaction.

13. The MWS sends the payment request to the VTS using an XML based protocol.

14. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

15. The TGS processes the transaction through the financial payment gateway.

16. The TGS receives a transaction response from the financial payment gateway.

17. The transaction response is routed back from the TGS to the VTS.

18. The transaction result is passed from the VTS to the MWS.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 360 of 1360

19. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the subscriber device. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

20. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.

21. To update the subscriber's device, the prepay result is sent from the MWS to the payment application.

22. The payment application generates a WAP push on the subscriber's device notifying the subscriber the prepay transaction has been processed.

Referring to figure 5, there is shown a ladder diagram describing a second use case for the embodiment of figure 3. This use case describes a System Initiated Prepay Via WAP Phone scenario.

This scenario is a one-step transaction. Unlike the subscriber initiated prepay, described with reference to figure 4, we are certain that the push alert will arrive at the intended subscriber device. A process continuously monitors the prepay database. If a subscriber's prepay amount falls below a certain threshold, a push alert is generated from the system. The subscriber acts on this push alert to affect a prepay transaction.

Each of the steps in the ladder diagram of figure 5 may be described as follows:

1. A database trigger is setup within the prepaid database. Once a subscriber's prepay amount falls below a certain threshold, an event is

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 361 of 1360

generated and a request is made to the MWS to initiate a prepay transaction. The request will also contain a reference to the subscriber record within the e-Wallet.

2. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.

3. The subscriber's credentials are extracted from the e-Wallet. Since the system is initiating a prepay request, the password held at the e-Wallet does not need to be validated.

4. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.

5. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the SID extracted from the e-Wallet is sent to enable the WAP push mechanism in the next step.

6. The web server generates a WAP push message out to the subscriber device. The destination device can be determined by the SID. The push message can take the form of a real WAP push message through the WAP browser, or an indirect WAP push through the SMS messaging mechanism of the phone. In either case, the push message will contain a URL for triggering the prepay transaction. To complete the authentication loop, the URL will consist partly of the transaction ID of the temporary prepay transaction held at the MWS.

7. The subscriber authorizes the prepay transaction by selecting the URL and confirming the transaction. The subscriber is also prompted for

additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.

8. The prepay web server sends an XML based request to the MWS, which is an authorization (confirmation) of the prepay transaction.

9. The MWS sends the payment request to the VTS using an XML based protocol.

10. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

11. The TGS processes the transaction through the financial payment gateway.

12. The TGS receives a transaction response from the financial payment gateway.

13. The transaction response is routed back from the TGS to the VTS.

14. The transaction result is passed from the VTS to the MWS.

15. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the subscriber device. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

16. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.

17. To update the subscriber's device, the prepay result is sent from the MWS to the payment application.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 363 of 1360

18. The payment application generates a WAP push on the subscriber's device notifying the subscriber the prepay transaction has been processed.

Referring to figure 6, there is shown a ladder diagram describing a third use case for the embodiment of figure 3. This use case describes a Subscriber Initiated Prepay Via IVR System scenario.

This scenario is a two-step transaction. The subscriber is involved in two IVR sessions, where the second session is used as a further subscriber authentication step. The first session involves the subscriber affecting a prepay application. The second session involves pushing an alert back to the subscriber. The push alert takes the form of a phone call to the subscriber device. The second step removes the possibility that the original prepay transaction was not initiated by the intended subscriber. The phone number (Mobile Identity Number, MIN) held within the e-Wallet defines the destination device of the push alert.

Each of the steps in the ladder diagram of figure 6 may be described as follows:

1. The subscriber dials the IVR system through the subscriber's device. The prepay application is selected from the list of options.
2. The carriers network validations ESN and MIN of subscriber phone.
3. The subscriber is prompted by the IVR system for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.
4. The IVR system builds the appropriate XML based message and sends the message to the MWS. The request will minimally contain the MIN for device authentication and optionally a DTMF password for subscriber authentication. The assumption is that caller ID is activated for the subscriber's device; therefore, the IVR system receives and passes through the MIN of the phone.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 364 of 1360

5. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.

6. Based on the MIN, the subscriber's credentials are extracted from the e-Wallet. Optionally, if a password has been specified, the SID and password pair is authenticated against the SID and password held in the e-Wallet.

7. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.

8. An XML based response message is sent back to the IVR system. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the MIN extracted from the e-Wallet is sent to enable the IVR callback in the next.

9. An IVR callback to the subscriber phone is performed using the MIN sent from the MWS. The IVR system outlines the transaction details to the subscriber. To complete the authentication loop, the IVR system will temporarily hold the transaction ID of the temporary prepay transaction held at the MWS.

10. The subscriber authorizes the prepay transaction through the IVR system.

11. The IVR system sends a second XML based request to the MWS, which is an authorization (confirmation) request of the original prepay transaction.

12. The MWS sends the payment request to the VTS using an XML based protocol.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 365 of 1360

13. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

14. The TGS processes the transaction through the financial payment gateway.

15. The TGS receives a transaction response from the financial payment gateway.

16. The transaction response is routed back from the TGS to the VTS.

17. The transaction result is passed from the VTS to the MWS.

18. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the IVR system. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

19. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.

20. To update the subscriber device, the prepay result is sent from the MWS to the IVR system.

21. The IVR system calls the subscriber's device notifying the subscriber the prepay transaction has been processed.

Referring to figure 7, there is shown a ladder diagram describing a third use case for the embodiment of figure 3. This use case describes a System Initiated Prepay Via IVR System scenario.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 366 of 1360

This scenario is a one-step transaction. Unlike the subscriber initiated prepay, we are certain that the IVR callback mechanism will arrive at the intended subscriber device. A process continuously monitors the prepay database. If a subscriber's prepay amount falls below a certain threshold, an IVR phone call is generated from the system. The subscriber confirms through the IVR system to affect a prepay transaction.

Each of the steps in the ladder diagram of figure 7 may be described as follows:

1. A database trigger is setup within the prepaid database. Once a subscriber's prepay amount falls below a certain threshold, an event is generated and a request is made to the MWS to initiate a prepay transaction. The request will also contain a reference to the subscriber record within the e-Wallet.
2. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.
3. The subscriber's credentials are extracted from the e-Wallet. Since the system is initiating a prepay request, the password held at the e-Wallet does not need to be validated.
4. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.
5. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the MIN extracted from the e-Wallet is sent to enable the IVR callback mechanism in the next step.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 367 of 1360

6. The IVR system outlines the transaction details to the subscriber. To complete the authentication loop, the IVR system will temporarily hold the transaction ID of the temporary prepay transaction held at the MWS.

7. The subscriber authorizes the prepay transaction through the IVR system. The subscriber is also prompted for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.

8. The prepay web server sends an XML based request to the MWS, which is an authorization (confirmation) of the prepay transaction.

9. The MWS sends the payment request to the VTS using an XML based protocol.

10. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

11. The TGS processes the transaction through the financial payment gateway.

12. The TGS receives a transaction response from the financial payment gateway.

13. The transaction response is routed back from the TGS to the VTS.

14. The transaction result is passed from the VTS to the MWS.

15. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the IVR system. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

16. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 368 of 1360

optionally be viewable from the online customer care website as a prepay transaction history.

17. To update the subscriber device, the prepay result is sent from the MWS to the IVR system.

18. The IVR system calls the subscriber's device notifying the subscriber the prepay transaction has been processed.

Accordingly it may be seen that the system of the present invention provides a secure real-time top-up service that can be implemented in existing payment infrastructures.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 369 of 1360

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, said method comprising the steps of:

(a) receiving at an application server first information indicative of the transaction device authentication;

(b) receiving at said application server second information for verification of said user; and

(c) using both said first and second information to authorize top-up payment of said prepaid service from said financial institution.

2. A method as defined in claim 1, said prepaid service being a prepaid cellular phone.

3. A method as defined in claim 2, said first information being a hardware identification of said cellular telephone.

4. A method as defined in claim 2, said second information being a personal identification number (PIN) of said user.

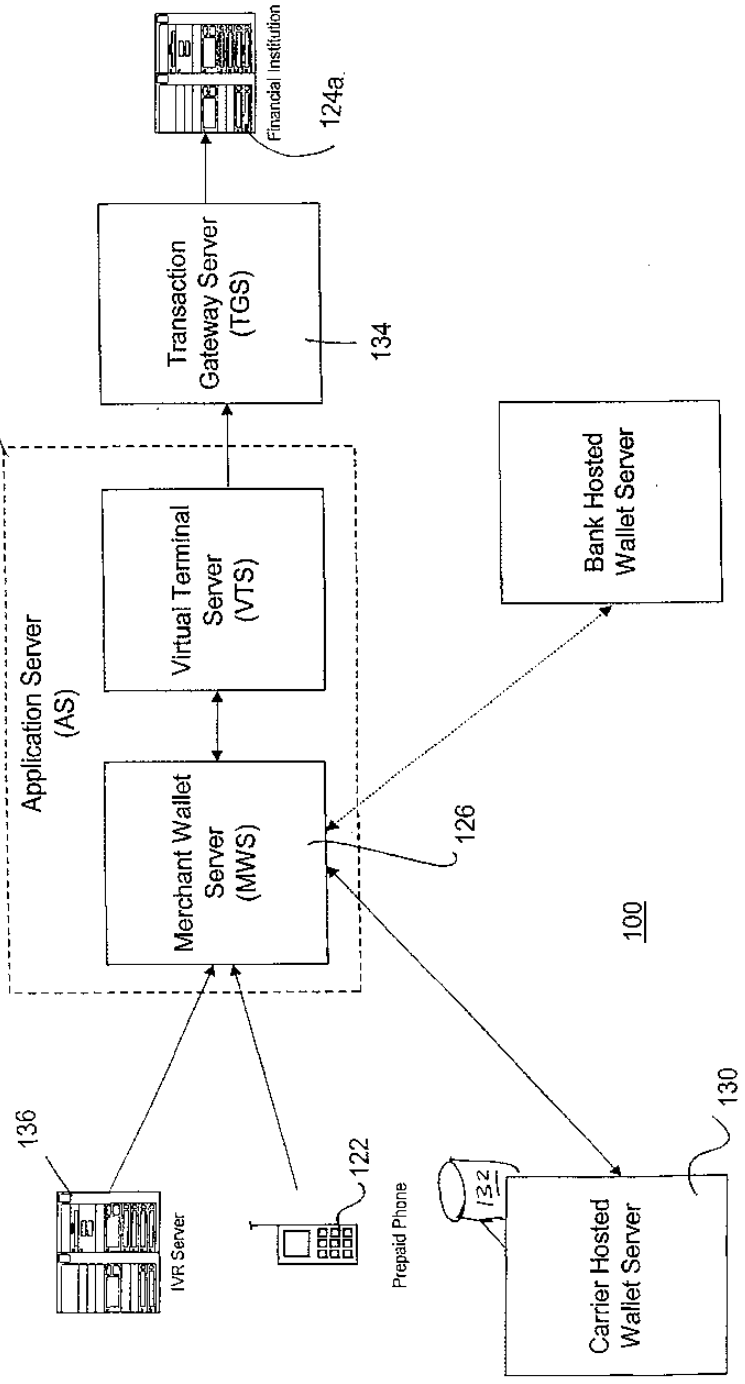


Figure 1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 371 of 1360

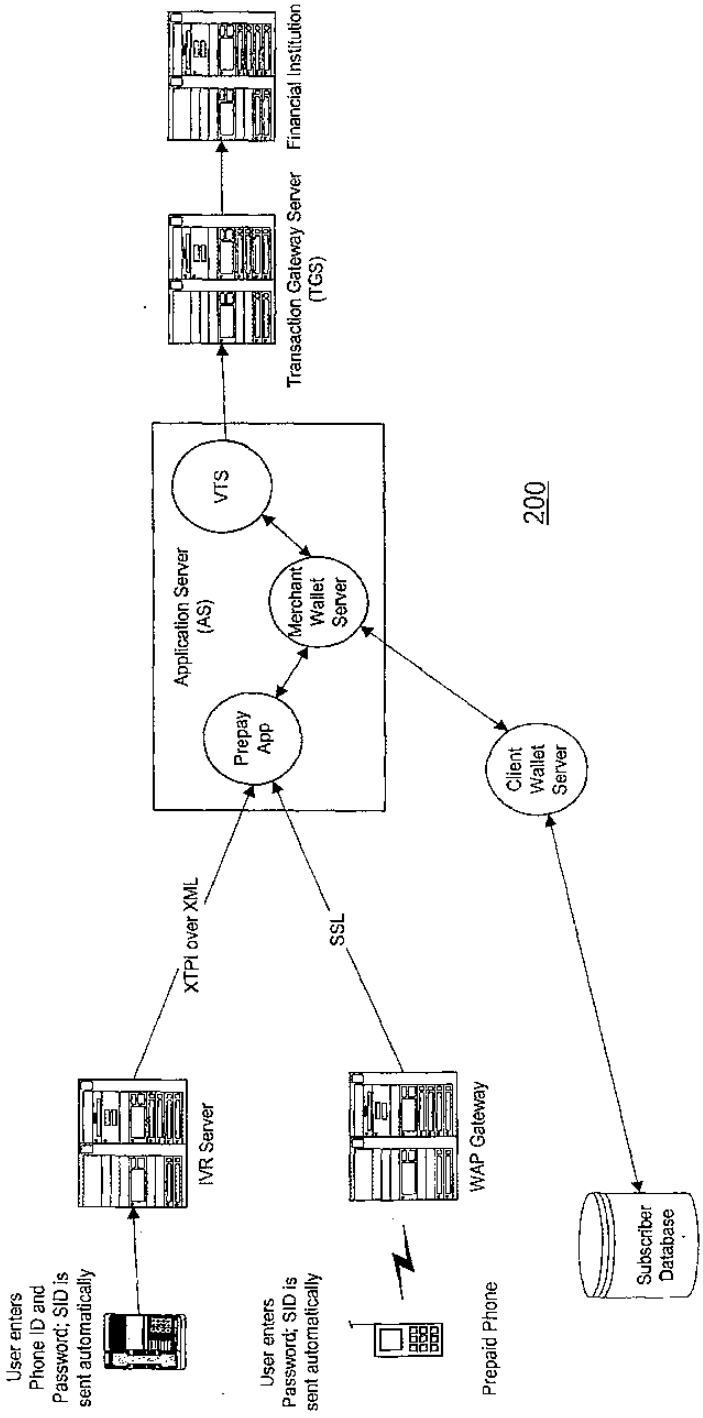


Figure 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 372 of 1360

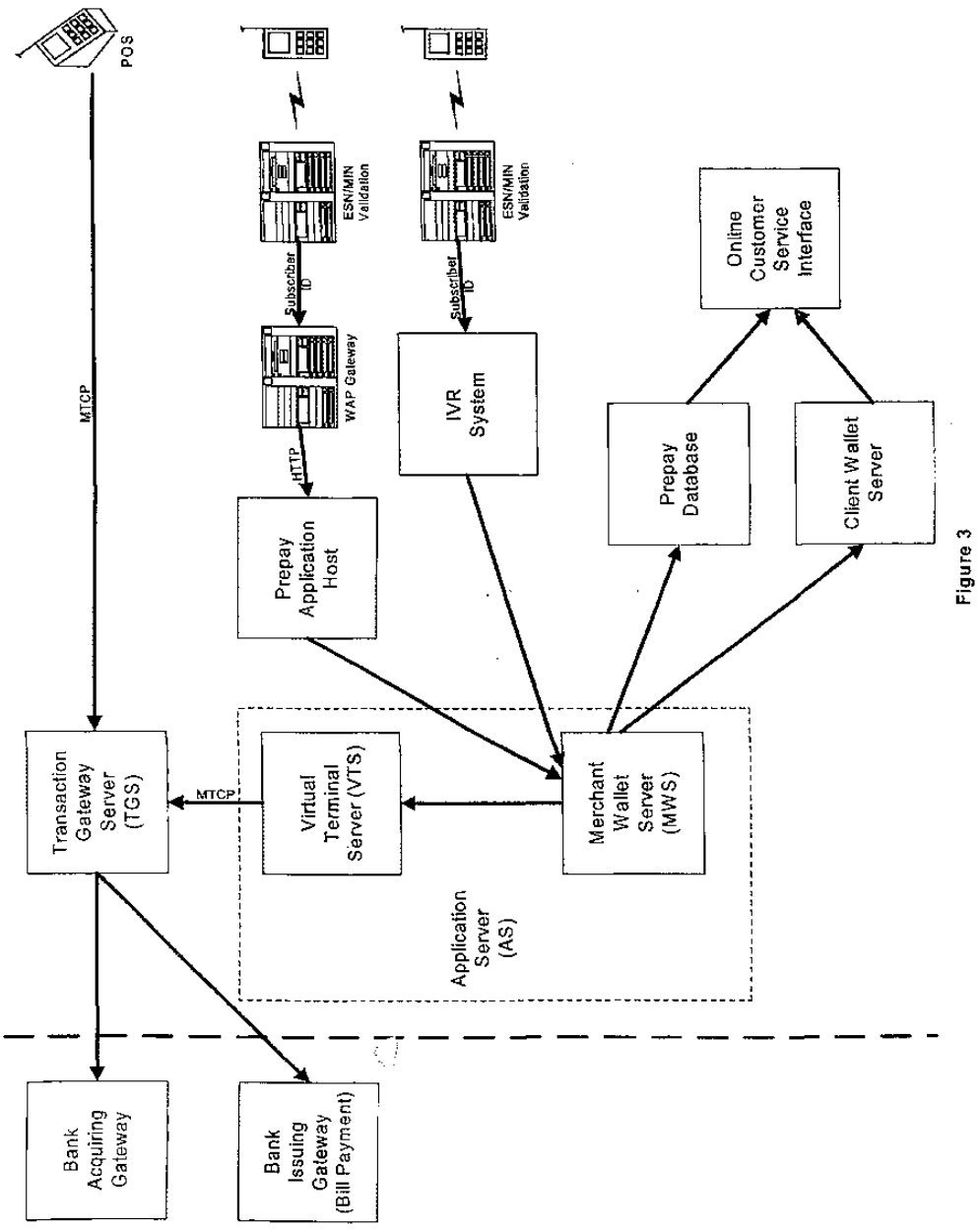


Figure 3

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 373 of 1360

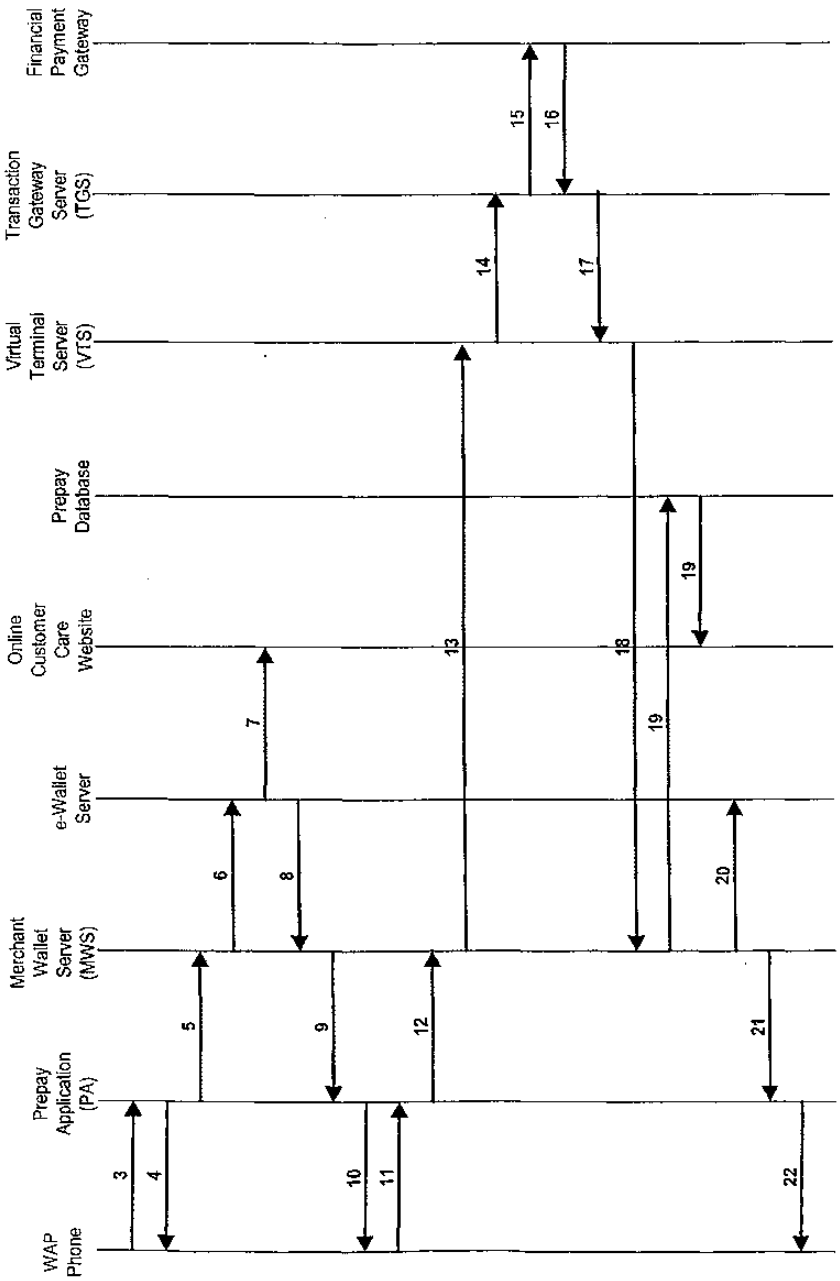


Figure 4

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 374 of 1360

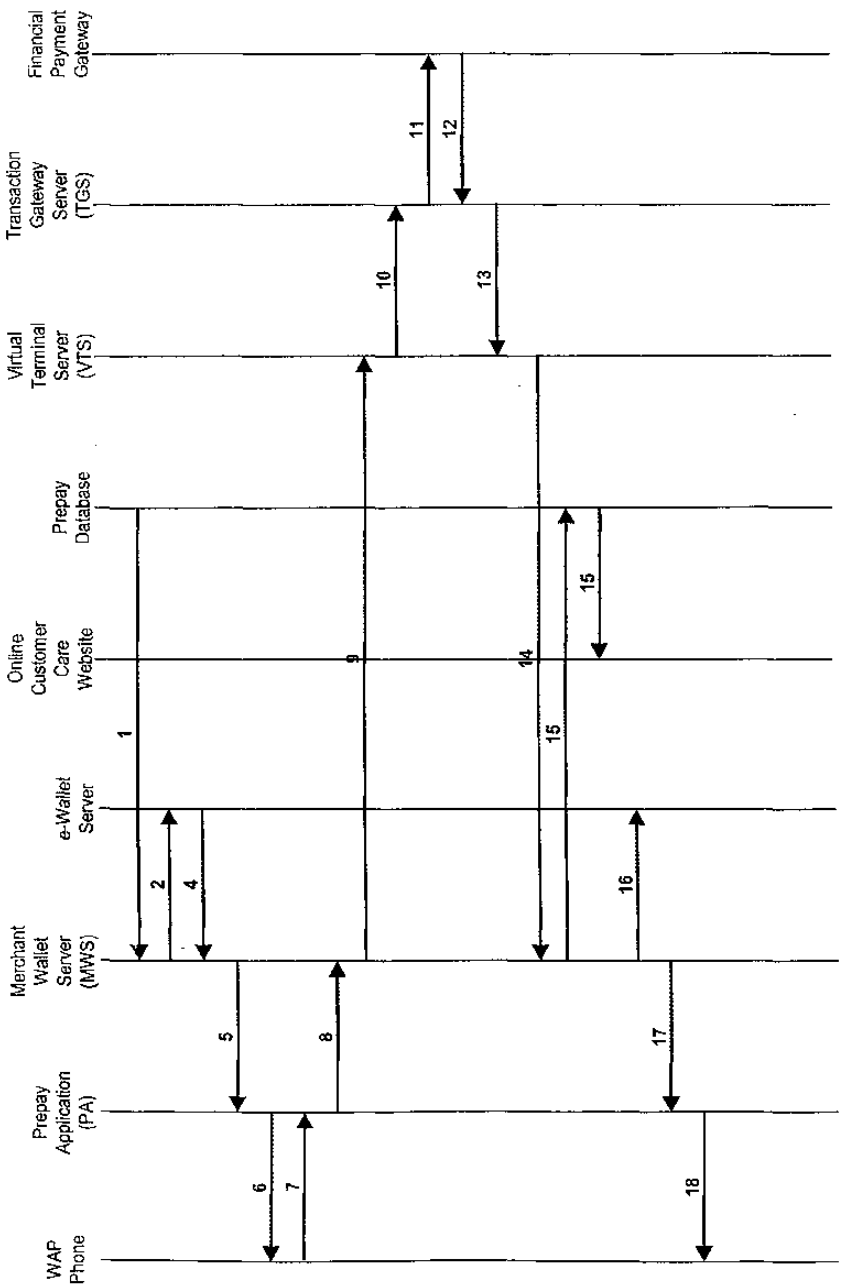


Figure 5

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 375 of 1360

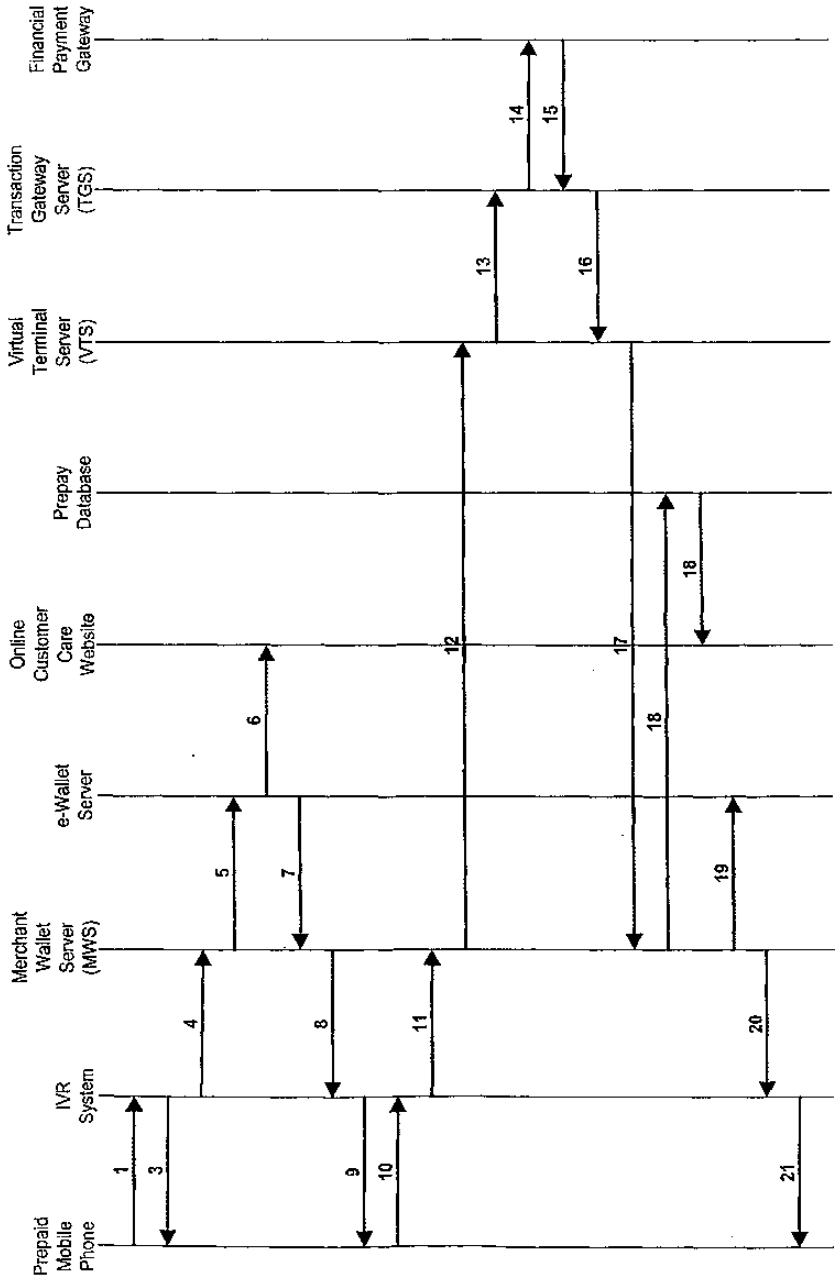


Figure 6

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 376 of 1360

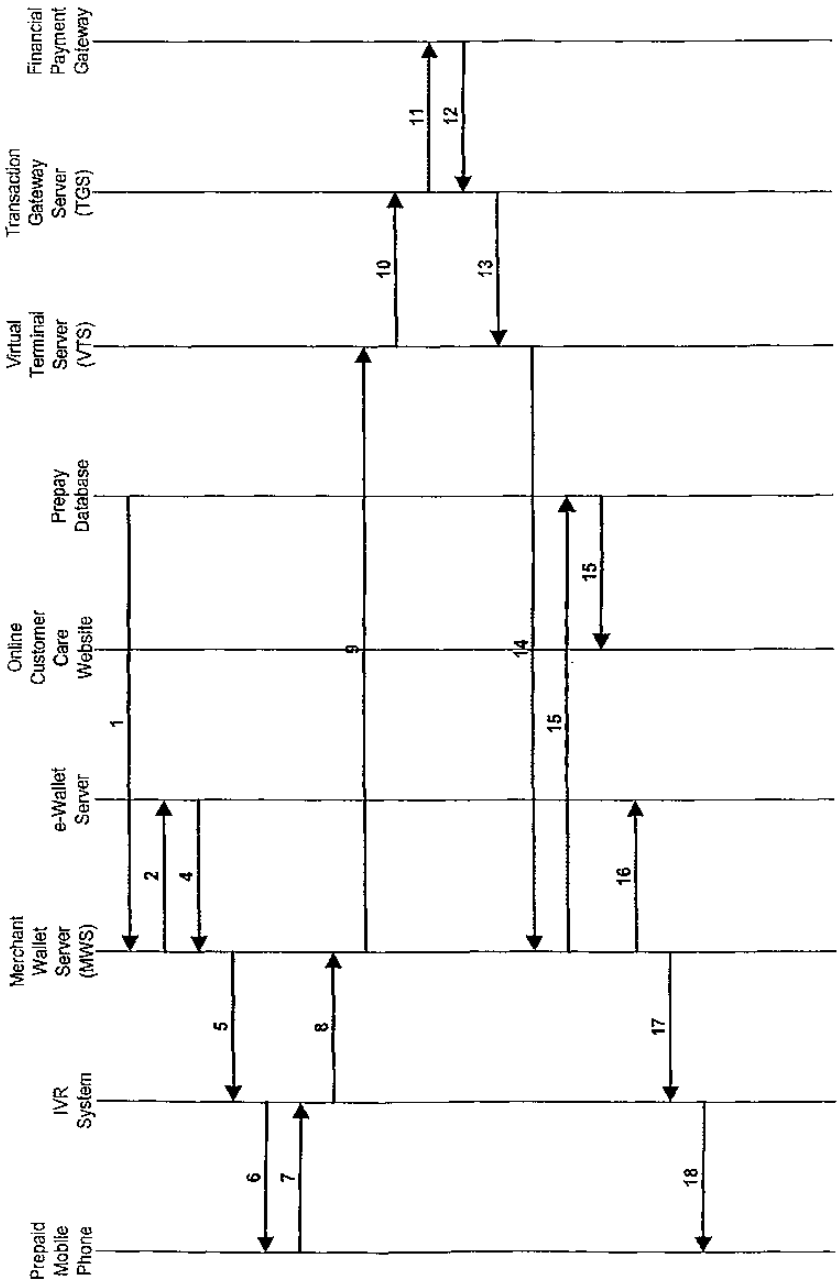


Figure 7

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 377 of 1360

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年12 月20 日 (20.12.2001)

PCT

(10) 国際公開番号
WO 01/97118 A1

(51) 国際特許分類7: G06F 17/60, 19/00

(21) 国際出願番号: PCT/JP01/05039

(22) 国際出願日: 2001 年6 月13 日 (13.06.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-178188 2000 年6 月14 日 (14.06.2000) JP
特願2000-221240 2000 年7 月21 日 (21.07.2000) JP
特願2000-402918
2000 年12 月28 日 (28.12.2000) JP

(71) 出願人 および
(72) 発明者: 浄弘貴子 (JOGU, Takako) [JP/JP]; 〒631-0036 奈良県奈良市学園北1丁目8番4号 Nara (JP). 與　貞行 (ATAE, Sadayuki) [JP/JP]; 〒815-0071 福岡県福岡市南区平和2-4-10-402 Fukuoka (JP).

(74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 三井住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

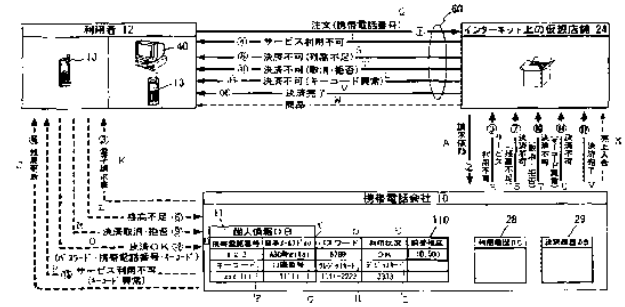
(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
国際調査報告書

[続葉有]

(54) Title: SETTLING METHOD USING MOBILE PHONE AND MOBILE PHONE

(54) 発明の名称: 携帯電話機を用いた決済方法および携帯電話機



12...USER
A...ORDER (MOBILE PHONE NUMBER)
B...SERVICE USE NOT PERMITTED
S...SETTLEMENT NOT PERMITTED (BALANCE IN THE RED)
T...SETTLEMENT NOT PERMITTED (CANCELLED, REJECTED)
U...SETTLEMENT NOT PERMITTED (ABNORMAL KEYCODE)
V...SETTLEMENT COMPLETED
W...COMMODITY
24...VIRTUAL STORE ON INTERNET
A...BILLING REQUEST
X...SALES PAYMENT CREDITED
28...PERSONAL INFORMATION DB
10...MOBILE PHONE FIRM
M...MOBILE PHONE NUMBER
C...E-MAIL ADDRESS
D...PASSWORD
E...USAGE STATUS
110...ADVANCE PAYMENT BALANCE
26...USAGE HISTORY DB
29...SETTLEMENT HISTORY DB
F...KEYCODE
G...ACCOUNT NUMBER
N...CREDIT CARD
I...DEBIT CARD
J...BALANCE UPDATING
K...ELECTRONIC BILLING
L...BALANCE IN THE RED
M...SETTLEMENT CANCELLED/REJECTED
O...SETTLEMENT ON (PASSWORD/MOBILE PHONE NUMBER/KEYCODE)
P...SERVICE USE NOT PERMITTED (ABNORMAL KEYCODE)

(57) Abstract: A virtual account (110) is opened in a mobile phone firm (10) for each user (12) of a mobile phone (13). A user (12) deposits advance payment in a virtual account (110) using a mobile phone (13). Advance payment is paid in combination with telephone charges or by means of a credit card or a debit card. A balance of a virtual account is stored in

[続葉有]

WO 01/97118 A1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 378 of 1360

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

a mobile phone (13). When shopping at a virtual store on the Internet, the phone number of a mobile phone (13) is transmitted, and , when shopping at a real store, the phone number is sent to a POS terminal. Each store bills a settlement amount to a mobile phone firm. Therefore, settlement can be made with high security and simplicity by using a mobile phone.

(57) 要約:

携帯電話機（１３）の利用者（１２）ごとに携帯電話会社（１０）内に仮想口座（１１０）を設ける。利用者（１２）は携帯電話機（１３）を用いて仮想口座（１１０）に前払金を入金しておく。前払金は、通話料と合せて支払ったり、クレジットカードやデビットカードで支払う。携帯電話機（１３）には仮想口座（１１０）の残高が記憶されている。インターネット上の仮想店舗で買物をする場合は携帯電話機（１３）の電話番号を送信し、実在店舗で買物をする場合は電話番号をＰＯＳ端末に送信する。各店舗は、携帯電話会社（１０）に決済金額を請求する。したがって、高いセキュリティで簡単に携帯電話機を用いて決済することができる。

明細書

携帯電話機を用いた決済方法および携帯電話機

技術分野

この発明は、携帯電話機およびその携帯電話機を用いた決済方法に関し、さらに詳しくは、インターネット上の仮想店舗や実在店舗における決済を仲介するサービスに関する。

背景技術

現在、携帯電話機を用いた種々の決済方法が提案されている。日経エレクトロニクス「携帯で決済」第７６９号, 日経ＢＰ社(２０００年５月８日) 発行, １０９～１２９頁には、ＩＣカードを搭載した携帯電話機が記載されている。この携帯電話機では、ＩＣカードにクレジットカード番号をセキュアな状態で予め記録しておき、決済時にクレジットカード番号を暗号化して送信するようにしている。また、非接触型ＩＣカード用のリーダ／ライタを搭載した携帯電話機も記載されている。この携帯電話機では、プリペイドカードの度数のような電子バリューをダウンロードし、これをリーダ／ライタにより非接触型ＩＣカードに無線経由で転送するようにしている。利用者はこの非接触型ＩＣカードを使って決済を行なう。

上記ＩＣカードを搭載した携帯電話機ではクレジットカード番号を暗号化しているが、クレジットカード番号を送信していることに変わりはないので、インターネット上の電子商取引では十分なセキュリティとは言えない。

一方、上記リーダ／ライタを搭載した携帯電話機では、利用者は携帯電話機とともに非接触型ＩＣカードを持ち歩かなければならない。また、リーダ／ライタはサイズが大きく、コストも高いなど、問題も多い。

この他、携帯電話機を用いた種々の決済方法が提案されているが、いずれも決済時に与信照会が必要であったり、決済データの送信が必要なため、決済時に電波を飛ばす必要があり、電波圏外では使用することができず、また、決済に時間

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 380 of 1360

がかかるという問題がある。

発明の開示

この発明は、上記のような問題を解決するためになされたもので、セキュリティが高く使い勝手のよい携帯電話機およびその携帯電話機を用いた決済方法を提供することを目的とする。

この発明による携帯電話機を用いた決済方法は、売り主と携帯電話機の利用者たる買い主との間の決済を仲介する方法であって、利用者の金銭を蓄積するための口座を利用者ごとに設けたサーバコンピュータにおいて、携帯電話機から送信された金額を受信するステップと、受信した金額を利用者の口座に入金してその口座の残高を更新するステップと、更新した口座の残高を携帯電話機に送信するステップと、決済金額を受信するステップと、受信した決済金額を口座の残高から減じるステップと、受信した決済金額を売り主に支払うステップとを含む。ここでのサーバコンピュータは、携帯電話局（会社）、金融機関（会社）、決済機関（会社）などに設置され得るが、その位置は特に限定されない。

一方、この発明による携帯電話機は、売り主と携帯電話機の利用者たる買い主との間の決済に用いられる携帯電話機であって、利用者の金銭を蓄積するための口座がサーバコンピュータに利用者ごとに設けられ、利用者の操作に応じて口座に入金される所望の金額を入力する手段と、入力された金額を携帯電話局のコンピュータに送信し、サーバコンピュータから送信された仮想口座の残高を受信する送受信手段と、受信した口座の残高を記憶する手段とを備える。

この決済方法または携帯電話機によれば、利用者は携帯電話機を用いて所望の金額を携帯電話局または携帯電話局を通じて金融機関もしくは決済機関に送信する。携帯電話局、金融機関または決済機関は、携帯電話機から送信された金額を受信し、その金額を利用者の口座に入金してその口座の残高を更新して携帯電話機に送信する。携帯電話機は、携帯電話局から送信された口座の残高を受信して記憶する。したがって、利用者は携帯電話機を財布のように使って決済を行なうことができる。ここでは、クレジット番号などを送信する必要がないので、セキュリティが高い。また、ＩＣカードなどを持ち歩く必要もないので、使い勝手が

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 381 of 1360

よい。

図面の簡単な説明

図１は、この発明の第１の実施の形態に従って仮想口座に入金する前払金額を通話料と併せて支払う場合の資金移動を示す概略図である。

図２は、この発明の第１の実施の形態に従って仮想口座に入金する前払金額をクレジットカードで支払う場合の資金移動を示す概略図である。

図３は、この発明の第１の実施の形態に従って仮想口座に入金する前払金額をデビットカードで支払う場合の資金移動を示す概略図である。

図４は、この発明の第１の実施の形態に従って仮想口座に入金する前払金額を銀行口座から自動引落しする場合の資金移動を示す概略図である。

図５は、この発明の第１の実施の形態に従って携帯電話機を用いてインターネット上の仮想店舗で決済する方法を示す概略図である。

図６は、この発明の第１の実施の形態に従って携帯電話機を用いて実在店舗で決済する方法を示す概略図である。

図７は、図１～図４に示したように仮想口座に前払金を入金するために用いられる、携帯電話機および携帯電話会社のサーバのハードウェア構成を示すブロック図である。

図８は、図１に示した場合における、図７に示した携帯電話機および携帯電話会社のサーバの動作を示すフローチャートである。

図９は、図８に示した携帯電話機の動作中に表示される画面の遷移図である。

図１０は、図２に示した場合における、図７に示した携帯電話機および携帯電話会社のサーバの動作を示すフローチャートである。

図１１は、図１０に示した携帯電話機の動作中に表示される画面の遷移図である。

図１２は、図３に示した場合における、図７に示した携帯電話機および携帯電話会社のサーバの動作を示すフローチャートである。

図１３は、図１２に示した携帯電話機の動作中に表示される画面の遷移図である。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 382 of 1360

図１４は、図４に示した場合における、図７に示した携帯電話機および携帯電話会社のサーバの動作を示すフローチャートである。

図１５は、図１４に示した携帯電話の動作中に表示される画面の遷移図である。

図１６は、この発明の第１の実施の形態に従ってインターネット上の仮想店舗で携帯電話機を用いて決済する場合に用いられる、携帯電話機、携帯電話会社のサーバ、パーソナルコンピュータ、および仮想店舗のサーバのハードウェア構成を示すブロック図である。

図１７は、図５に示した場合における図１６に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

図１８は、図１７に続くフローチャートである。

図１９は、図１７および図１８に示した携帯電話機の動作中に表示される画面の遷移図である。

図２０は、図６に示した場合に用いられる、携帯電話機、携帯電話会社のサーバ、および実在店舗のＰＯＳ端末のハードウェア構成を示すブロック図である。

図２１は、図２０に示した携帯電話機、実在店舗のＰＯＳ端末、および携帯電話会社のサーバの動作を示すフローチャートである。

図２２は、図２１に続くフローチャートである。

図２３は、図２１および図２２に示した携帯電話機の動作中に表示される画面の遷移図である。

図２４は、携帯電話機のＲＡＭおよびＲＯＭに記憶される情報を示す図である。

図２５は、この発明の第２の実施の形態に従って実在口座から仮想口座に振替える場合の資金移動を示す概略図である。

図２６は、図２５に示したように実在口座から仮想口座への振替に用いられる携帯電話機、携帯電話会社のサーバおよび金融機関のサーバのハードウェア構成を示すブロック図である。

図２７は、図２５に示した場合における、図２６に示した携帯電話機、携帯電話会社のサーバ、および金融機関のサーバの動作を示すフローチャートである。

図２８は、図２７に続くフローチャートである。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 383 of 1360

図２９は、図２７および図２８に示した携帯電話機の動作中に表示される画面の遷移図である。

図３０は、この発明の第２の実施例に従って携帯電話機を用いてインターネット上の仮想店舗で決済する方法を示す概略図である。

図３１は、図３０に示した場合に用いられるパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、金融機関のサーバ、決済機関のサーバ、および仮想店舗のサーバのハードウェア構成を示すブロック図である。

図３２は、図３０に示した場合における、図３１に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、仮想店舗のサーバ、および金融機関サーバの動作を示すフローチャートである。

図３３は、図３２に続くフローチャートである。

図３４は、図３３に続くフローチャートである。

図３５は、図３２～図３４に示した携帯電話機の動作中に表示される画面の遷移図である。

図３６は、この発明の第２の実施の形態に従って携帯電話機を用いて実在店舗で決済する方法を示す概略図である。

図３７は、図３６に示した場合に用いられる、携帯電話機、実在店舗のＰＯＳ端末、携帯電話会社のサーバ、金融機関のサーバ、および決済機関のサーバのハードウェア構成を示すブロック図である。

図３８は、図３６に示した場合における、図３７に示した携帯電話機、ＰＯＳ端末、携帯電話会社のサーバ、金融機関のサーバの動作を示すフローチャートである。

図３９は、図３８に続くフローチャートである。

図４０は、図３９に続くフローチャートである。

図４１は、この発明の第３の実施の形態に従ってサービスの利用者情報を登録する方法を示す概略図である。

図４２は、この発明の第３の実施の形態に従って仮想口座に前払金額を入金する場合の資金移動を示す概略図である。

図４３は、この発明の第３の実施の形態に従って携帯電話機を用いてインター

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 384 of 1360

ネット上の仮想店舗で決済する方法を示す概略図である。

図４４は、この発明の第３の実施の形態に従って携帯電話機を用いて実在店舗で決済する方法を示す概略図である。

図４５は、この発明の第３の実施の形態に従って決済機関が利用者に対して携帯電話機に蓄積されている未通知データを要求する方法を示す概略図である。

図４６は、この発明の第３の実施の形態に従って携帯電話機を用いてインターネット上の仮想店舗で決済する場合において決済機関が金融機関に対する請求を代行する方法を示す概略図である。

図４７は、図４１に示した利用登録に用いられる、携帯電話機、携帯電話会社のサーバおよび決済機関のサーバのハードウェア構成を示すブロック図である。

図４８は、図４１に示した場合における、図４７に示した携帯電話機、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

図４９は、図４２に示した仮想口座への資金移動に用いられる、携帯電話機、携帯電話会社のサーバ、決済機関のサーバおよび金融機関のサーバのハードウェア構成を示すブロック図である。

図５０は、図４２に示した場合における、図４９に示した携帯電話機、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

図５１は、図５０に続くフローチャートである。

図５２は、図５１に続くフローチャートである。

図５３は、図４３に示した仮想店舗での決済に用いられる、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバおよび仮想店舗のサーバのハードウェア構成を示すブロック図である。

図５４は、図４３に示した場合における、図５３に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバおよび仮想店舗のサーバの動作を示すフローチャートである。

図５５は、図５４に続くフローチャートである。

図５６は、図５５に続くフローチャートである。

図５７は、図４４に示した実在店舗での決済に用いられる、携帯電話機、ＰＯＳ端末、携帯電話会社のサーバおよび決済機関のサーバのハードウェア構成を示

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 385 of 1360

すブロック図である。

図５８は、図４４に示した場合における、図５７に示した携帯電話機、ＰＯＳ端末、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

図５９は、図５８に続くフローチャートである。

図６０は、図５９に続くフローチャートである。

図６１は、図４５に示した未通知データの要求の場合における、携帯電話機、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

図６２は、図４６に示した請求代行に用いられる、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、金融機関のサーバおよび仮想店舗のサーバのハードウェア構成を示すブロック図である。

図６３は、図４６に示した場合における、図６２に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、金融機関のサーバおよび仮想店舗のサーバの動作を示すフローチャートである。

図６４は、図６３に続くフローチャートである。

図６５は、この発明の第４の実施の形態に従う前払方法を示す概略図である。

図６６は、図６５に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

図６７は、図６６に続くフローチャートである。

図６８は、この発明の第４の実施の形態に従う第１の送金方法を示す概念図である。

図６９は、図６８に示した場合における、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

図７０は、図６９に続くフローチャートである。

図７１は、この発明の第４の実施の形態に従う第２の送金方法を示す概念図です。

図７２は、図７１に示した場合における、パーソナルコンピュータ、携帯電話

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 386 of 1360

機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

図７３は、図７２に続くフローチャートである。

図７４は、この発明の第４の実施の形態に従って、小口決済履歴がない場合におけるワンタイムＩＤの発行方法を示す概念図である。

図７５は、この発明の第４の実施の形態に従って、小口決済履歴がある場合におけるワンタイムＩＤの発行方法を示す概念図である。

図７６は、図７４および図７５に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

図７７は、図７６に続くフローチャートである。

図７８は、この発明の第４の実施の形態に従い、ワンタイムＩＤを使用して実在店舗で決済する方法を示す概念図である。

図７９は、図７８に示した場合における、携帯電話機、実在店舗のＰＯＳ端末、および決済機関のサーバの動作を示すフローチャートである。

発明を実施するための最良の形態

以下、この発明の実施の形態を図面を参照して詳しく説明する。図中同一または相当部分には同一符号を付してその説明は繰返さない。

［第１の実施の形態］

１．サービスの概要

この発明の実施の形態は、携帯電話会社が提供する新規サービス（「お財布サービス」と呼び、以下単に「本サービス」という）を実現するためのコンピュータシステムに関するものである。本サービスは、携帯電話機を財布のように使用できるようにするものである。以下、本サービスの概要を説明する。

携帯電話機購入の際、通話料金を引落す銀行口座以外に、クレジットカード番号やキャッシュカード番号などを携帯電話会社に登録する。携帯電話会社は、携帯電話機の利用者ごとに仮想口座を設ける。利用者は、決済の前に、仮想口座に前払金を入金するように、携帯電話機を用いて携帯電話会社に要請する。携帯電話会社は、予め登録されている銀行口座、クレジットカード番号、キャッシュカ

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 387 of 1360

ード番号などを用い、利用者に対して前払金の請求を行なう。前払金の支払方法は、利用者が選択することができる。前払金の請求後、携帯電話会社は、仮想口座に前払金を入金したうえで仮想口座の残高を携帯電話機に送信する。携帯電話機は、送信された仮想口座の残高を記憶する。利用者は、この携帯電話機を財布代わりに使ってインターネット上の仮想店舗や実在店舗で決済を行なう。店舗は、携帯電話会社に対して請求を行なう。

２．前払金の支払方法

次に、４通りの前払金の支払方法について説明する。

２－１．通話料と併せて支払う場合

図１は、前払金を通話料と併せて支払う場合の資金移動を示す概略図である。図１に示すように、携帯電話会社（携帯電話局）１０には、個人情報データベース１１が設けられている。個人情報データベース１１には、各利用者１２の個人情報が登録されている。具体的には、前払金（携帯電話会社にとっては前受金）を蓄積するための仮想口座１１０が設けられ、携帯電話機１３の電話番号の他、電子メールアドレス、パスワード、利用状況、キーコード、口座番号、クレジットカード番号、デビットカード番号などが予め登録されている。

まず、利用者１２は携帯電話機１３を用いて所望の前払金額とその支払方法（ここでは「通話料に加算」）とを携帯電話会社１０に送信する。このとき、携帯電話機１３の電話番号も併せて送信する。

携帯電話会社１０は、送信された携帯電話番号に基づいて個人情報データベース１１を検索し、利用者１２の仮想口座１１０の利用状況を照会する。利用者１２に問題がなければ（利用状況が「ＯＫ」であれば）、携帯電話会社１０は送信された前払金額を仮想口座１１０の前受残高に加算し、更新した最新の前受残高を送信する。一方、利用者１２の支払いが滞っていたり、本サービスの利用が停止されている場合、利用状況は「ＮＧ」となっている。この場合、携帯電話会社１０は携帯電話機１３を通じて本サービスを利用できない旨を利用者１２に通知する。

上記のように利用者１２が支払方法として「通話料に加算」を選択した場合、携帯電話会社１０は、基本料金と通話料金の請求書１４と併せて本サービスの利

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 388 of 1360

用明細書１５を利用者１２に送付する。

携帯電話会社１０は、個人情報データベース１１に登録されている口座番号に基づいて利用者１２の取引銀行１７に利用料金の引落しを依頼する。これに応じて銀行１７は、利用者１２の口座１６から、銀行１８に開設されている携帯電話会社１０の口座１９に資金を振替える。

２－２．クレジットカードで支払う場合

図２は、前払金をクレジットカードで支払う場合の資金移動を示す概略図である。この場合、図２に示すように、利用者１２は携帯電話機１３を用いて前払金額とその支払方法（ここでは「クレジットカード」）とを携帯電話会社１０に送信する。

携帯電話会社１０は、利用者１２の利用状況に問題がなければ、予め登録されているクレジットカード番号に基づいて信販会社２０に承認を依頼する。信販会社２０は、承認できる場合はその旨を携帯電話会社１０に通知する。これに応じて、携帯電話会社１０は仮想口座１１０の前受残高を更新し、その最新の前受残高を携帯電話機１３に送信する。一方、承認できない場合は、信販会社２０はその旨を携帯電話会社１０に通知する。これに応じて、携帯電話会社１０は前受残高を更新することなく、クレジットカードによる支払いができない旨を利用者１２に通知する。

支払いを承認した場合、信販会社２０は、利用者１２が所望した前払金額を携帯電話会社１０の口座１９に振込む。次いで信販会社２０は、銀行１７に対して利用者１２の口座１６から前払金額を引落すように依頼する。これに応じて銀行１７は、利用者１２の口座１６から信販会社２０に資金を振替える。

２－３．デビットカードで支払う場合

図３は、前払金をデビットカードで支払う場合の資金移動を示す概略図である。この場合、図３に示すように、利用者１２は携帯電話機１３を用いて前払金額とその決済方法（ここでは「デビットカード」）とを携帯電話会社１０に送信する。

携帯電話会社１０は、利用者１２の利用状況に問題がなければ、予め登録されているデビットカード番号に基づいてそのデビットカードを発行した銀行１７に資金の振替えを依頼する。振替え依頼を承認した場合、銀行１７はその振替えデ

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 389 of 1360

ータをクリアリングセンター２１に送信するとともに、振替えの完了を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、前受残高を更新し、その最新の前受残高を携帯電話機１３に送信する。一方、銀行１７が振替え依頼を承認しない場合、振替えできない旨を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、前受残高を更新することなく、デビットカードで支払いできない旨を利用者１２に通知する。

クリアリングセンター２１は、銀行１７の他、多数の銀行から送信された振替えデータに基づいて振替えの相殺および集計を行ない、銀行間の決済尻データを決済銀行２２に送信する。これに応じて決済銀行２２は、銀行１７から加盟店銀行２３に資金を振替える。これに応じて加盟店銀行２３は、その資金を携帯電話会社１０の口座１９に入金する。

２－４．自動引落しで支払う場合

図４は、前受金を銀行口座から自動引落しで支払う場合の資金移動を示す概略図である。この場合、図４に示すように、利用者１２は携帯電話機１３を用いて前払金額とその支払方法（ここでは「自動引落」）とを携帯電話会社１０に送信する。携帯電話会社１０は、利用者１２の利用状況に問題がなければ、予め登録されている口座番号に基づいて銀行１７に資金の引落しを依頼する。引落しが可能な場合、銀行１７はその旨を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、前受残高を更新し、最新の前受残高を携帯電話機１３に送信する。引落しが不可能な場合、銀行１７はその旨を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、支払いできない旨を利用者１２に通知する。携帯電話会社１０から引落し依頼を受けた銀行１７は直ちに、利用者１２の口座１６から携帯電話会社１０の口座１９に資金を振替える。これとは別に、利用明細書１５は請求書１４と併せて利用者１２に送付される。

３．決済

次に、携帯電話機１３を使って上述した前払金で決済を行なう方法について説明する。

３－１．インターネット上の仮想店舗での決済

図５は、インターネット上の仮想店舗で携帯電話機を使って決済する方法を示

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 390 of 1360

す概略図である。図５に示すように、まず、利用者１２は携帯電話機１３またはパーソナルコンピュータ４０でインターネット上の仮想店舗２４に商品やサービスを注文し、その決済方法（ここでは「携帯電話決済」）を選択する。パーソナルコンピュータ４０を用いる場合、利用者１２は携帯電話機１３の電話番号をパーソナルコンピュータ４０に手で入力し、インターネット６０を通じて仮想店舗２４に送信する。

注文を受けた仮想店舗２４は、送信された携帯電話番号に基づいて携帯電話会社１０に決済金額の請求を依頼する。

請求依頼を受けた携帯電話会社１０は、利用者１２の利用状況に問題があれば本サービスが利用できない旨を仮想店舗２４に通知する。これに応じて仮想店舗２４は、本サービスが利用できない旨を利用者１２に通知する。利用者１２の利用状況に問題がなければ、携帯電話会社１０は予め登録されている利用者１２の電子メールアドレスに基づいて利用者１２の携帯電話機１３に電子メールで電子請求書を送信する。電子請求書は、仮想口座１１０からの支払いを利用者１２に確認するためのものである。

また、電子請求書を受取った利用者１２は、その決済を承認するか否かを選択する。利用者１２が決済を承認した場合、電子請求書を受信した携帯電話機１３は、前払残高を検証し、前払残高が決済金額を下回っている場合、携帯電話機１３は残高不足として決済ができない旨を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、残高が不足しているから決済できない旨を仮想店舗２４を通じて利用者１２に通知する。利用者１２が決済を取消しまたは拒否した場合、決済取消しまたは決済拒否を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、決済が取消しまたは拒否されたから決済できない旨を仮想店舗２４に通知する。これに応じて仮想店舗２４は、決済できない旨を利用者１２に通知する。

また、利用者１２が決済を承認した場合において、前払残高の検証の結果、決済金額が前払残高以内のとき、その決済を了承する旨を携帯電話会社１０に通知する。このとき、予め携帯電話会社１０に登録されているパスワード、携帯電話番号、キーコードなどを併せて送信する。携帯電話会社１０は、送信された携帯

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 391 of 1360

電話番号に基づいて個人情報データベース１１を検索し、送信されたパスワードおよびキーコードが予め登録されているパスワードおよびキーコードとそれぞれ一致するか否かを判別する。キーコードが一致しない場合、携帯電話会社１０はキーコードが異常であるから本サービスを利用できない旨を利用者１２に通知するとともに、決済できない旨を仮想店舗２４を通じて利用者１２に通知する。両者とも一致する場合、携帯電話会社１０は仮想口座１１０の前受残高から決済金額を減算して前受残高を更新するとともに、その更新した前受残高を携帯電話機１３に送信する。これに応じて携帯電話機１３は内部の前受残高を更新する。また、携帯電話会社１０は決済完了を仮想店舗２４に通知する。これに応じて仮想店舗２４は決済完了を利用者１２に通知する。

その後、仮想店舗２４は注文を受けた商品を利用者１２に届けたり、注文を受けたサービスを利用者１２に提供する。携帯電話会社１０は、上記決済金額を仮想店舗２４に入金する。仮想店舗２４は、本サービスを利用した手数料を携帯電話会社１０に支払う。

３－２．実在店舗での決済

図６は、実在店舗で携帯電話機を使って決済する方法を示す概略図である。図６に示すように、実在店舗において、利用者１２は携帯電話機１３をＰＯＳ端末２７に接続された読取装置２７０にセットする。店員は商品の金額をＰＯＳ端末２７に打ち込み、決済金額を計算する。この決済金額はＰＯＳ端末２７から読取装置２７０を通じて携帯電話機１３に送信される。携帯電話機１３は、内部に記憶されている残高と決済金額とを比較し、決済が不可能であればエラーをＰＯＳ端末２７に送信する。一方、決済が可能であれば、携帯電話機１３は携帯電話番号とキーコードとをＰＯＳ端末２７に送信する。携帯電話番号は、ＰＯＳ端末２７に手で直接入力することはできない。

携帯電話番号とキーコードとを受信したＰＯＳ端末２７は決済を完了して、その旨を携帯電話機１３に通知する。決済完了を受けて、携帯電話機１３はその決済金額を内部メモリに記憶し、決済モードがオフになる。その後、利用者１２は携帯電話機１３を読取装置２７０から取り除く。

次に、決済金額とともに携帯電話番号およびキーコードを携帯電話会社１０に

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 392 of 1360

送信する。これに応じて携帯電話会社１０は、仮想口座１１０の前受残高から決済金額を減算して前受残高を更新するとともに、決済完了をＰＯＳ端末２７に通知する。

４．ハードウェア構成

図７は、携帯電話機１３、および携帯電話会社１０に設置されるサーバコンピュータ（以下、単にサーバという）３０のハードウェア構成を示すブロック図である。

図７に示すように、携帯電話機１３は、ＣＰＵからなるデータ処理部１３１と、ＲＡＭ１３２と、ＥＥＰＲＯＭのようなＲＯＭ１３３と、アンテナ１３４と、送受信部１３５と、テンキーやカーソルキーのような入力装置１３６と、液晶ディスプレイのような表示装置１３７と、バッテリ１３８と、インターフェイス（Ｉ／Ｆ）部１３９とを備える。この携帯電話機１３は電源アダプタ１４０に装着され、電源アダプタ１４０からＩ／Ｆ部１３９を通じてバッテリ１３８に電流が供給され、バッテリ１３８が充電される。データ処理部１３１は、ＲＡＭ１３２、ＲＯＭ１３３、送受信部１３５、入力装置１３６、表示装置１３７およびＩ／Ｆ部１３９を用いて通常の携帯電話機能を実行する他、後述する決済機能を実行する。

携帯電話会社１０に設置されているサーバ３０は、ＣＰＵからなるデータ処理部３０１と、データベース３０２とを備える。データベース３０２は、個人情報データベース１１と、利用履歴データベース２８と、決済履歴データベース２９とを含む。データ処理部３０１はデータベース３０２を用いて後述する決済機能を実行する。データ処理部３０１は無線基地局３０３に接続されている。無線基地局３０３のアンテナ３０４と携帯電話機１３のアンテナ１３４との間で電波が送受信される。利用履歴データベース２８は、携帯電話機１３とのデータの取引内容を記録するためのログファイルである。具体的には、仮想口座１１０の入出金日時、入出金額、残高などが記録される。決済履歴データベース２９は、店舗とのデータの取引内容を記録するためのログファイルである。具体的には、決済日時、決済金額などが記録される。

５．前払い時の処理動作

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 393 of 1360

５－１．通話料と併せて支払う場合

図８は、図１に示した前払金を通話料と併せて支払う場合における携帯電話機１３およびサーバ３０の動作を示すフローチャートである。図９は、この場合に携帯電話機１３の表示装置１３７に表示される表示画面の遷移図である。

まず、携帯電話機１３のデータ処理部１３１は、表示装置１３７上に図９に示した画面Ｄ１を表示し、利用者１２に対してパスワードの入力を促す。利用者１２が入力装置１３６を操作してパスワードを入力すると、入力装置１３６はその入力されたパスワードをデータ処理部１３１に与える（Ｓ１０１）。

続いて、データ処理部１３１はその入力されたパスワードをＲＡＭ１３２またはＲＯＭ１３３に予め登録されているパスワードと比較することにより入力されたパスワードの検証を行なう（Ｓ１０２）。入力されたパスワードが誤っている場合、データ処理部１３１は表示装置１３７上に図９に示した画面Ｄ２を表示する（Ｓ１０３）。一方、入力されたパスワードが正しい場合、データ処理部１３１は表示装置１３７上に図９にした画面Ｄ３を表示し、利用者１２に対し、「①お金を払う」、「②お財布の中を見る」、「③お財布にお金を入れる」の中から１つを選択するよう促す。利用者１２が入力装置１３６を操作し、「③お財布にお金を入れる」を選択すると、データ処理部１３１は表示装置１３７上に画面Ｄ４を表示し、利用者１２に対して前払金額の入力を促す。このとき、未通知データ（詳細は後述する）がない場合はＲＡＭ１３２に記憶されている前払残高を現在の残高として表示し、未通知データがある場合はＲＡＭ１３２に記憶されている前払残高から未通知の決済金額を減算して真の前払残高を計算し、それを現在の残高として表示する。利用者１２が入力装置１３６を操作して所望の前払金額を入力すると、入力装置１３６がその入力された前払金額をデータ処理部１３１に与える（Ｓ１０４）。

続いて、データ処理部１３１は表示装置１３７上に画面Ｄ５を表示し、利用者１２に対して前払金額の支払方法を選択するよう促す。利用者１２が入力装置１３６を操作すると、「通話料に加算」という支払方法の他、「クレジット」、「デビットカード」、「自動引落」といういくつかの支払方法が表示される。ここでは利用者１２が「通話料に加算」という支払方法を選択するものとする。こ

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 394 of 1360

れに応じて、入力装置１３６は「通話料に加算」という支払方法の選択をデータ処理部１３１に与える（Ｓ１０５）。

続いて、データ処理部１３１は選択された支払方法および入力された前払金額を送受信部１３５に与え、送受信部１３５はこれらを携帯電話会社１０に送信する（Ｓ１０６）。このとき、ＲＯＭ１３３に予め記憶されている利用者１２に固有の携帯電話番号と、ＲＯＭ１３３に予め記憶されている携帯電話機１３に固有のキーコードと、ＲＡＭ１３２に記憶されている未通知データとを併せて送信する。携帯電話番号は、携帯電話会社１０が携帯電話機１３を販売する際にＥＥＰＲＯＭのようなＲＯＭ１３３に予めプログラムする。キーコードは、携帯電話機メーカが携帯電話機を製造する際に製造番号や各携帯電話機固有の管理番号（サブスクライバＩＤ（識別子）、機体ＩＤ、端末ＩＤなどと呼ばれる）などをＥＥＰＲＯＭのようなＲＯＭ１３３に予めプログラムする。したがって、携帯電話番号は利用者１２に固有のもので、携帯電話機１３を買い換えた場合でも同じ携帯電話番号を登録することができる。ただし、利用者１２自身は携帯電話番号を書き換えることはできず、利用者１２の依頼に応じて携帯電話会社１０が書き換えることになる。これに対し、キーコードは携帯電話機１３に固有のものである。キーコードに製造番号を用いた場合、利用者１２はもちろん、携帯電話会社１０さえも書き換えることができない。キーコードに上述したサブスクライバＩＤのような管理番号を用いた場合、携帯電話会社１０は書き換えることができるが、利用者１２は書き換えることができない。

続いて、データ処理部１３１はこれまでの処理が正常に終了したか否かを判別し（Ｓ１０７）、正常に終了していない場合はその旨を表示装置１３７に表示し（Ｓ１０８）、接続を切断する（Ｓ１０９）。一方、正常に終了した場合は異常終了の表示をすることなく接続を一旦切断する（Ｓ１０９）。

一方、携帯電話会社１０に設置されているサーバ３０において、データ処理部３０１は、携帯電話機１３から送信された前払金額、支払方法、携帯電話番号およびキーコードを無線基地局３０３を通じて受信する（Ｓ２０１）。

続いて、データ処理部３０１は受信した携帯電話番号に基づいて個人情報データベース１１を検索する（Ｓ２０２）。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 395 of 1360

続いて、データ処理部３０１は受信したキーコードを検索した個人情報データベース１１のキーコードと比較し、キーコードが一致するか否か確認する（Ｓ２０３）。キーコードが一致した場合、データ処理部３０１は個人情報データベース１１の利用状況を確認し、問題があるか否か判別する（Ｓ２０４）。上記ステップＳ２０２でキーコードが一致しない場合、またはこのステップＳ２０４で利用状況に問題がある場合、データ処理部３０１は本サービス利用不可の情報を携帯電話機１３に送信する（Ｓ２０５）。

携帯電話機１３においては、送受信部１３５が携帯電話機１３から送信された本サービス利用不可能の情報を受信する（Ｓ１１０）

続いて、データ処理部１３１は図９に示した画面Ｄ６を表示装置１３７上に表示し、本サービスを利用できない旨を利用者１２に通知する（Ｓ１１１）。そして、データ処理部１３１は表示装置１３７上に異常に終了した旨を表示する（Ｓ１１２）。

一方、上記ステップＳ２０４で利用状況に問題がなければ、利用履歴データベース２８を更新する（Ｓ２０６）。具体的には、現在の日時と、今回の前受金額（利用者１２にとっては前払金額）と、現在の前受残高と、未通知データ（未通知の決済金額）とを利用履歴データベース２８に記録する。

続いて、データ処理部３０１は現在の前受残高を携帯電話機１３に送信する（Ｓ２０７）。

続いて、データ処理部３０１はこの前受金額について請求データを作成する（Ｓ２０８）。

続いて、データ処理部３０１は作成した請求データを毎月一括して通話料に加算し、図１に示すように請求書１４とともに本サービスの利用明細書１５を発行する。

以降の処理は既存の処理と同じで、利用者１２の個人情報データベース１１に登録されている口座番号に基づき利用者１２の取引銀行１７に対して料金の引落しを依頼する（Ｓ２０９）。これに応じて、本サービスの利用料金が通話料と併せて利用者の口座１６から携帯電話会社の口座１９に振替えられる。

携帯電話機１３においては、上記ステップＳ２０７でサーバ３０から送信され

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 396 of 1360

た前受残高を送受信部１３５が受信する（Ｓ１１３）。

続いて、データ処理部１３１は受信した前受残高を前払残高としてＲＡＭ１３２に格納し、これにより前受残高を更新する（Ｓ１１６）。

続いて、データ処理部１３１は図９に示した画面Ｄ７を表示装置１３７に表示する（Ｓ１１７）。具体的には、これまでの前払処理が完了した旨と現在の前払残高とを表示する。

５－２．クレジットカードで支払う場合

図１０は、図２に示した前払金額をクレジットカードで支払う場合における携帯電話機１３およびサーバ３０の動作を示すフローチャートである。図１１は、この場合に携帯電話機１３の表示装置１３７に表示される画面の遷移図である。

上記と異なり前払金額をクレジットカードで支払う場合は、図１１に示した画面Ｄ５で利用者１２は「クレジット（一括）」を選択する。これに応じて、入力装置１３６はクレジットカードによる支払いという支払方法の選択をデータ処理部１３１に与える（図１０，Ｓ１０５）。

また、携帯電話会社１０のサーバ３０においては、利用状況に問題がない場合、個人情報データベース１１に予め登録されているクレジットカード番号に基づいて信販会社２０に利用者１２の与信照会を行なう（Ｓ２１０）。

続いて、データ処理部３０１は信販会社２０からの返信に基づいて信販会社２０がクレジットカードによる支払いを承認したか否かを判別する（Ｓ２１１）。

非承認の場合、データ処理部３０１は支払できない旨を携帯電話機１３に送信する（Ｓ２１２）。承認の場合は、利用履歴データベース２８を更新する（Ｓ２０５）。

一方、携帯電話機１３においては、送受信部１３５がサーバ３０からクレジットカードによる支払いは不可能な旨を受信した場合、図１２に示した画面Ｄ８を表示装置１３７に表示し、クレジットカードによる支払いが不可能な旨を利用者１２に通知する（Ｓ１２０）。

５－３．デビットカードで支払う場合

図１２は、前払金額をデビットカードで支払う場合の携帯電話機１３およびサーバ３０の動作を示すフローチャートである。図１３は、この場合に携帯電話機

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 397 of 1360

１３の表示装置１３７に表示される画面の遷移図である。

上記と異なり前払金額をデビットカードで支払う場合、図１３に示した表示画面Ｄ５において利用者１２は「デビットカード」を選択する。これに応じて、入力装置１３６はその選択情報をデータ処理部１３１に与える（Ｓ１０５）。

一方、携帯電話会社１０のサーバ３０においては、利用状況に問題がない場合、データ処理部３０１は個人情報データベース１１に予め登録されているデビットカード番号に基づいてそのデビットカードの発行銀行１７に引落し（承認）依頼を送信する（Ｓ２２０）。これに応じて、既存のデビットカード処理が実行される（Ｓ２２１）。

続いて、データ処理部３０１はデビットカードの発行銀行１７から送信された振替え結果に基づいて振替えが完了したか否かを判別する（Ｓ２２２）。振替えができなかった場合、データ処理部３０１はその旨を携帯電話機１３に送信する（Ｓ２１２）。

これに応じて携帯電話機１３のデータ処理部１３１は、図１３に示した画面Ｄ９を表示装置１３７に表示し（Ｓ１２０）、デビットカードによる支払いができない旨を利用者１２に通知する。

５－４．自動引落で即時支払う場合

図１４は、図４に示した前払金額を利用者の口座１６から自動的に引落す場合における携帯電話機１３およびサーバ３０の動作を示すフローチャートである。図１５は、この場合に携帯電話機１３の表示装置１３７に表示される画面の遷移図である。

上記と異なり自動引落しの場合、図１５に示した画面Ｄ５で利用者１２は「自動引落」を選択し、この利用者１２の操作に応じて入力装置１３６はデータ処理部１３１にその選択情報を与える（Ｓ１０５）。

一方、サーバ３０においては、利用状況に問題がない場合、データ処理部３０１は受信した前払金額が引落し可能か否かを利用者１２の取引銀行１７に照会する（Ｓ２３０）。

続いて、データ処理部３０１は銀行１７から返信された照会結果に基づいて引落しが可能か否かを判別する（Ｓ２３１）。引落しが不可能な場合、データ処理

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 398 of 1360

部３０１はその旨を携帯電話機１３に送信する（Ｓ２３２）。

これに応じて携帯電話機１３のデータ処理部１３１は、図１５に示した画面Ｄ１０を表示し（Ｓ１２０）、利用者の口座１６からは所望の前払金額を引落すことができない旨を利用者１２に通知する。

一方、引落しが可能な場合、携帯電話会社１０は既存の方法で銀行１７に引落しを依頼する（Ｓ２２３）。

６．決済時の処理動作

次に、携帯電話機１３を用いてインターネット上の仮想店舗および実在店舗で決済を行なう場合の動作について説明する。

６－１．仮想店舗で決済する場合

図１６は、仮想店舗で決済を行なう場合に用いられる利用者のパーソナルコンピュータ（ＰＣ）４０および携帯電話機１３、携帯電話会社のサーバ３０、ならびに仮想店舗のサーバコンピュータ（以下、単にサーバという）５０のハードウェア構成を示すブロック図である。

図１６に示すように、利用者１２のパーソナルコンピュータ４０は、ＣＰＵのようなデータ処理部４０１と、ＲＯＭやＲＡＭのようなメモリ４０２と、ハードディスク（ＨＤ）４０３と、モデム４０４と、キーボードやマウスのような入力装置４０５と、ＣＲＴディスプレイや液晶ディスプレイのような表示装置４０６とを備える。仮想店舗２４のサーバ５０も同様に、データ処理部５０１と、メモリ５０２と、ハードディスク５０３と、モデム５０４と、入力装置５０５と、表示装置５０６とを備える。パーソナルコンピュータ４０はモデム４０４を通じてインターネット６０に接続される。サーバ５０もモデム５０４を通じてインターネット６０に接続される。携帯電話会社１０のサーバ３０もモデム３０３を通じてインターネット６０に接続される。

図１７および図１８は、図１６に示したパーソナルコンピュータ４０、携帯電話機１３、サーバ３０および５０の動作を示すフローチャートである。

利用者１２はパーソナルコンピュータ４０の入力装置４０５を操作して仮想店舗２４に商品やサービスの注文を行ない、その決済方法として携帯電話決済を選択する。これに応じて、パーソナルコンピュータ４０のデータ処理部４０１は入

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 399 of 1360

力された注文情報および携帯電話番号をインターネット６０を通じて仮想店舗２４のサーバ５０に送信する（Ｓ３０１）。

サーバ５０のデータ処理部５０１は、送信された注文情報および携帯電話番号を受信する（Ｓ６０１）。

続いて、データ処理部５０１は、店舗名、決済金額、携帯電話番号などの請求情報をインターネット６０を通じて携帯電話会社１０のサーバ３０に送信することにより、携帯電話会社１０に利用者１２の決済金額を請求する（Ｓ６０２）。

サーバ３０のデータ処理部３０１は、送信された請求情報を受信する（Ｓ５０１）。

続いて、データ処理部３０１は受信した携帯電話番号に基づいて個人情報データベース１１を検索する（Ｓ５０２）。

続いて、データ処理部３０１は検索した利用者１２の個人情報の中から利用状況を照会し、問題がないか否か確認する（Ｓ５０３）。問題がある場合、データ処理部３０１は本サービス利用不可の情報をサーバ５０に送信する。これにより、本サービスを利用できない旨を仮想店舗２４に通知する（Ｓ５０４）。一方、利用状況に問題がない場合、データ処理部３０１は検索した個人情報の中から利用者１２の電子メールアドレスを特定し、電子メールで請求データを携帯電話機１３に送信する（Ｓ５０５）。これは、携帯電話会社１０が仮想店舗２４に代わって利用者１２に請求書を発行することを意味する。利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０のサーバ３０から送信された請求データを受信する（Ｓ４０１）。

利用者１２が携帯電話機１３の入力装置１３６を操作して「受信メール一覧」を選択すると、携帯電話機１３のデータ処理部１３１は図１９に示した画面Ｄ１１を表示装置１３７上に表示する。利用者１２が入力装置１３６を操作して請求データの電子メールを選択すると、データ処理部１３１は画面Ｄ１２を表示装置１３７上に表示する。これは電子請求書であり、注文日、注文者（通常は利用者１２と同じ）、請求者（通常は仮想店舗２４と同じ）、請求額（通常は決済金額と同じ）が表示されている。

利用者１２が請求内容を確認し、同意できれば「支払」を選択し、同意できな

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 400 of 1360

ければ「拒否」を選択する。携帯電話機１３の入力装置１３６はこのような利用者１２の操作に応じて選択情報をデータ処理部１３１に入力する。データ処理部１３１は入力された選択情報に基づいて決済が承認されたか否かを判別する（Ｓ４０２）。決済が承認されなかった場合、送受信部１３５は決済取消・拒否の情報を携帯電話機１０のサーバ３０に送信する（Ｓ４０３）。この場合、データ処理部１３１は、図１９に示した画面Ｄ１３を表示装置１３７上に表示する（Ｓ４０４）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された決済取消・拒否の情報を受信し（Ｓ５０６）、さらにその情報を仮想店舗２４のサーバ５０に送信する（Ｓ５０７）。

仮想店舗２４のサーバ５０においては、データ処理部５０１が携帯電話会社１０のサーバ３０から送信された決済取消・拒否の情報を受信する（Ｓ６０５）。

続いて、データ処理部５０１は受信した決済取消・拒否の情報をインターネット６０を通じて利用者１２のパーソナルコンピュータ４０に送信し、これにより仮想店舗２４は利用者１２に決済が取消しまたは拒否された旨を利用者１２に通知する（Ｓ６０６）。

利用者１２のパーソナルコンピュータ４０においては、データ処理部４０１が仮想店舗２４のサーバ５０から送信された決済取消・拒否の情報を受信し（Ｓ３０４）、決済が取消しまたは拒否された旨を表示装置４０６上に表示する。

上記ステップＳ４０２で決済が承認された場合、携帯電話機１３のデータ処理部１３１は、ＲＡＭ１３２内に未通知データ（電波圏外の店舗で決済したために携帯電話会社１０に未だ通知できていない決済日時、決済金額などで、その詳細は後述する。）が存在しないか否かを判別する（Ｓ４０５）。未通知データがある場合、データ処理部１３１は未通知の決済金額を合計して累計未通知金額を計算し（Ｓ４０６）、続いてＲＡＭ１３２に記憶されている前払残高から累計未通知金額を減算して現時点における真の前払金額を計算する（Ｓ４０７）。

上記ステップＳ４０５で未通知データがない場合、または上記ステップＳ４０７の後、データ処理部１３１は前払残高を検証し、決済金額が前受残高以内か否かを判別する（Ｓ４０８）。決済金額が前受残高を超えている場合、データ処理

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 401 of 1360

部１３１は図１９に示した画面Ｄ１４を表示装置１３７上に表示して残高不足を利用者１２に通知し（Ｓ４０９）、続いて残高不足の情報を電波で携帯電話会社１０のサーバ３０に送信する（Ｓ４１０）。

これに応じて携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された残高不足の情報を受信し（Ｓ５０８）、続いてこの残高不足の情報をインターネット６０を通じて仮想店舗２４のサーバ５０に送信する（Ｓ５０９）。

仮想店舗２４のサーバ５０においては、データ処理部５０１が携帯電話会社１０のサーバ３０から送信された残高不足の情報を受信し（Ｓ６０７）、続いてこの残高不足の情報をインターネット６０を通じて利用者１２のパーソナルコンピュータ４０に送信する（Ｓ６０８）。利用者１２のパーソナルコンピュータ４０はこの残高不足の情報を受信し、その旨を表示装置４０６上に表示する（Ｓ３０５）。

一方、携帯電話機１３において、上記ステップＳ４０８で決済金額が前払残高以内の場合、データ処理部１３１は図１９に示した画面Ｄ１を表示し、利用者１２にパスワードの入力を促す。利用者１２がパスワードを入力すると、入力装置１３６は入力されたパスワードをデータ処理部１３１に与える（Ｓ４１１）。

続いて、送受信部１３５は、決済承認の情報および未通知データを携帯電話会社１０のサーバ３０に電波で送信する（Ｓ４１２）。具体的には、携帯電話機１３の電話番号、ＲＯＭ１３３に予めハード的に登録されているキーコード、上記ステップＳ４１１で入力されたパスワード、未通知の決済金額を送信する。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された決済承認の情報を受信する（Ｓ５１０）。

続いて、データ処理部３０１は個人情報データベース１１を検索し、受信した携帯電話番号に基づいて利用者１２の個人情報を特定する。データ処理部３０１はさらに、受信したキーコードを利用者１２の個人情報として予め登録されているキーコードと比較し、キーコードが一致するか否かを判別する（Ｓ５１１）。キーコードが一致した場合、データ処理部３０１は、受信したパスワードを利用者１２の個人情報として予め登録されているパスワードと比較し、パスワードが

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 402 of 1360

一致するか否かを判別する（Ｓ５１２）。

キーコードが一致しない場合、またはパスワードが一致しない場合、データ処理部３０１は本サービス利用不可の情報を携帯電話機１３に電波で送信し、これにより携帯電話会社１０は利用者１２に本サービスが利用できない旨を通知する（Ｓ５１３）。

利用者の携帯電話機１３においては、送受信部１３５が携帯電話会社１０のサーバ３０から送信された本サービス利用不可の情報を受信する（Ｓ４１３）。

続いて、データ処理部１３１は本サービスが利用できない旨を表示装置１３７上に表示する（Ｓ４１４）。

続いて、データ処理部１３１は本サービス手続が異常に終了した旨を表示装置１３７上に表示する（Ｓ４１５）。

一方、携帯電話会社１０の携帯電話機１３において、データ処理部３０１は決済不可の情報をインターネット６０を通じて仮想店舗２４のサーバ５０に送信する（Ｓ５１４）。

仮想店舗２４のサーバ５０においては、データ処理部５０１が携帯電話会社１０のサーバ３０から送信された決済不可の情報を受信する（Ｓ６０９）。

これに応じて、データ処理部５０１は決済不可の情報をインターネット６０を通じて利用者１２のパーソナルコンピュータ４０に送信し、これにより仮想店舗２４は利用者１２に決済ができない旨を通知する（Ｓ６１０）。

利用者１２のパーソナルコンピュータ４０においては、データ処理部４０１が仮想店舗２１のサーバ５０から送信された決済不可の情報を受信し（Ｓ３０６）、決済ができない旨を表示装置４０６上に表示する。

一方、携帯電話会社１０のサーバ３０においては、上記ステップＳ５１２でパスワードが一致した場合、データ処理部３０１は利用履歴データベース２８を更新し、利用者１２の仮想口座１１０の前受残高を更新する（Ｓ５１５）。利用履歴データベース２８には具体的には、決済日時、決済金額などを記録する。

続いて、データ処理部３０１は更新した前受残高を電波で携帯電話機１３に送信する（Ｓ５１６）。

携帯電話機１３においては、データ処理部１３１が携帯電話会社１０のサーバ

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 403 of 1360

３０から送信された仮想口座１１０の前受残高を受信する（Ｓ４１６）。

続いて、データ処理部１３１は受信した仮想口座の前受残高と同じになるようにＲＡＭ１３２に記憶されている前払残高を更新し、さらにＲＡＭ１３２に記憶されている未通知データをクリアする（Ｓ４１７）。これにより、携帯電話機１３内の前払残高と携帯電話会社内の仮想口座１１０の前受残高とが同期する。

そして、データ処理部１３１は図１９に示した画面Ｄ１５を表示装置１３７上に表示し、決済が完了した旨を利用者１２に通知する。

携帯電話会社１０のサーバ３０においては、上記ステップＳ５１６の後、決済完了の情報をインターネット６０を通じて仮想店舗２４のサーバ５０に送信し、これにより携帯電話会社１０は決済が完了した旨を仮想店舗２４に通知する（Ｓ５１７）。そして、携帯電話会社１０は既存の方法で仮想店舗２４に決済金額を支払う（Ｓ５１８）。

一方、仮想店舗２４のサーバ５０においては、データ処理部５０１は携帯電話会社１０のサーバ３０から送信された決済完了の情報を受信する（Ｓ６１１）。

続いて、データ処理部５０１は受注明細および決済完了の情報をインターネット６０を通じて利用者１２のパーソナルコンピュータ４０に送信する（Ｓ６１２）。

利用者１２のパーソナルコンピュータ４０においては、データ処理部４０１が仮想店舗２４のサーバ５０から送信された受注明細および決済完了の情報を受信する（Ｓ３０７）。

６－２．実在店舗で決済する場合

図２０は、実在店舗で決済する場合に用いられる携帯電話機１３、ＰＯＳ端末３７およびサーバ３０のハードウェア構成を示すブロック図である。

図２０に示すように、ＰＯＳ端末２７も同様に、データ処理部２７１と、ＲＡＭ２７２と、ハードディスク２７３と、入力装置２７４と、表示装置２７５と、インターフェイス（Ｉ／Ｆ）部２７６とを備える。決済時に携帯電話機１３がセットされる読取装置２７０はインターフェイス２７６に接続される。商品バーコードを読取るためのスキャナもインターフェイス部２７６に接続される。現金引出し部２７８もインターフェイス部２７６に接続される。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 404 of 1360

図２１および図２２は、図６に示したように実在店舗で決済する場合における携帯電話機１３、ＰＯＳ端末２７およびサーバ３０の動作を示すフローチャートである。

まず利用者１２は実在店舗２６で買物する前に、図２３に示した画面Ｄ１で携帯電話機１３の入力装置１３６を操作してパスワードを入力し、これに応じて入力装置１３６は入力されたパスワードをデータ処理部１３１に与える（Ｓ７０１）。

続いて、データ処理部１３１は入力されたパスワードを、図２４に示すようにＲＡＭ１３２に予め登録されているパスワードと比較し、パスワードの検証を行なう（Ｓ７０２）。パスワードが一致しない場合、データ処理部１３１は図２３に示した画面Ｄ２を表示装置１３７上に表示する（Ｓ７０３）。

一方、パスワードが一致した場合、データ処理部１３１は図２３に示したメニュー画面Ｄ３を表示する。利用者１２が「①お金を払う」を選択すると、データ処理部１３１は未通知データがあるか否かを判別する（Ｓ７０４）。未通知データは、電波圏外の店舗で決済した場合に、その決済金額、決済日時、決済店舗などが図２４に示すようにＲＡＭ１３２に累積的に格納されたものである。未通知データがある場合、データ処理部１３１は電波圏内か否かを判別し（Ｓ７０５）、電波圏内の場合、送受信部１３５は電波で携帯電話会社１０のサーバ３０に未通知データを図２４に示すようにＲＯＭ１３３に予め登録されたキーコードとともに送信する（Ｓ７０６）。電波圏外の場合、ＲＡＭ１３２に記憶されている未通知の決済金額を合計して累計未通知金額を計算し（Ｓ７０７）、続いてＲＡＭ１３２に記憶されている前払残高からその累計未通知金額を減算し、現在の真の前払残高を計算する（Ｓ７０８）。携帯電話機１３内の前払残高は、携帯電話会社１０から仮想口座１１０の前受残高が送信されて来ない限り更新されない。したがって、電波圏外の実在店舗で連続して携帯電話機１３で決済を行なった場合などは、その各決済金額を未通知データとしてＲＡＭ１３２に記憶しておく。

一方、携帯電話会社１０のサーバ３０においては、上記ステップＳ７０６で利用者１２の携帯電話機１３から送信された未通知データをデータ処理部３０１が受信する（Ｓ９０１）。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 405 of 1360

続いて、データ処理部３０１は、携帯電話機１３から送信されたキーコードを、個人情報データベース１１に予め登録されているキーコードと比較し、キーコードが一致するか否かを確認する（Ｓ９０２）。キーコードが一致しない場合、データ処理部３０１は本サービス利用不可の情報を携帯電話機１３に電波で送信し、これにより携帯電話会社１０は利用者１２に本サービスが利用できない旨を通知する（Ｓ９０３）。キーコードが一致する場合、データ処理部３０１は受信した未通知データに基づいて利用履歴データベース２８を更新し、仮想口座１１０の前受残高を更新する（Ｓ９０４）。続いて、データ処理部３０１は更新した最新の前受残高を携帯端末機１３に送信する（Ｓ９０５）。

携帯電話機１３においては、上記ステップＳ９０３で携帯電話会社１０のサーバ３０から送信された本サービス利用不可の情報を送受信部１３５が受信する（Ｓ７０９）。続いて、データ処理部１３１は本サービスが利用できない旨を表示装置１３７上に表示し（Ｓ７１０）、さらに本サービス手続が異常に終了した旨を表示装置１３７上に表示する（Ｓ７１１）。

また、上記ステップＳ９０５で携帯電話会社１０のサーバ３０から送信された前受残高を送受信部１３５が受信する（Ｓ７１２）。続いて、データ処理部１３１は受信した前受残高と同じになるようにＲＡＭ１３２に記憶されている前払残高を更新し、さらに未通知データをクリアする（Ｓ７１３）。

上記ステップＳ７０４で未通知データがない場合、または上記ステップＳ７０８もしくはＳ７１３の後、データ処理部１０３は図２３に示した画面Ｄ１６のように現在利用可能な残高を表示する（Ｓ７１４）。

続いて、携帯電話機１３の決済モードがオンになり、データ処理部１３１は図２３に示した画面Ｄ１７を表示装置１３７上に表示する（Ｓ７１５）。

続いて、利用者１２は携帯電話機１３を読取装置２７０にセットする（Ｓ７１６）。これにより、データ処理部１３１は図２３に示した画面Ｄ１８を表示装置１３７上に表示する。このとき、実在店舗のＰＯＳ端末２７においては、データ処理部２７１が読取装置２８を通じて携帯電話機１３に決済金額を送信する（Ｓ８０１）。

携帯電話機１３においては、データ処理部１３１はＰＯＳ端末２７から送信さ

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 406 of 1360

れた決済金額を受信する（Ｓ７１７）。

続いて、データ処理部１３１は受信した決済金額が現在の残高内か否かを判別する（Ｓ７１８）。決済金額が残高を超えている場合、データ処理部１３１は図２３に示した画面Ｄ１９を表示装置１３７上に表示し、残高不足を利用者１２に通知する（Ｓ７１９）。

決済金額が残高内の場合、データ処理部１３１は携帯電話機１３の電話番号およびＲＯＭ１３３に予めハード的に登録されているキーコードを読取装置２８を通じてＰＯＳ端末２７に送信する（Ｓ７２０）。

ＰＯＳ端末２７においては、データ処理部２７１が携帯端末機１３から送信された携帯電話番号およびキーコードを受信する（Ｓ８０２）。

続いて、データ処理部２７１は受信した携帯電話番号およびキーコードならびに決済内容をハードディスク２７３に記録する（Ｓ８０３）。

続いて、データ処理部２７１は決済完了の情報を読取装置２７０を通じて携帯電話機１３に送信する（Ｓ８０４）。

携帯電話機１３においては、データ処理部１３１がＰＯＳ端末２７から送信された決済完了の情報を受信し、取引完了を確認する（Ｓ７２１）。

続いて、データ処理部１３１はこのときの決済金額などを含む決済内容を未通知データとしてＲＡＭ１３２に記憶する（Ｓ７２２）。

上記ステップＳ７１６～Ｓ７２２の間、データ処理部１３１は図２３に示した画面Ｄ１８を表示装置１３７上に表示する。また、携帯電話機１３が途中で読取装置２７０から取外された場合は異常終了となる。上記ステップＳ７２２で決済内容をＲＡＭ１３２に記憶した後、データ処理部１３１は図２３に示した画面Ｄ２０を表示装置１３７上に表示する。そして、上記決済モードはオフになる（Ｓ７２３）。

続いて、データ処理部１３１は電波圏内か否かを判別し（Ｓ７２４）、電波圏内の場合、ＲＡＭ１３２に蓄積されている未通知データをＲＯＭ１３３にプログラムされているキーコードとともに携帯電話会社１０のサーバ３０に送信する（Ｓ７２５）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 407 of 1360

１３から送信された未通知データをキーコードとともに受信する（Ｓ９０９）。

続いて、データ処理部３０１は、携帯電話機１３から送信されたキーコードを、個人情報データベース１１に予め登録されているキーコードと比較し、キーコードが一致するか否かを確認する（Ｓ９１０）。キーコードが一致しない場合、データ処理部３０１は本サービス利用不可の情報を携帯電話機１３に電波で送信する（Ｓ９１１）。携帯電話機１３は、この情報を受信し（Ｓ７２６）、続いて本サービスが利用できない旨を表示装置１３７上に表示し（Ｓ７２７）、そして本サービス手続が異常に終了した旨を表示装置１３７上に表示する（Ｓ７２８）。

上記ステップＳ９１０でキーコードが一致する場合、データ処理部３０１は受信した未通知データに基づいて利用履歴データベース２８を更新し、仮想口座１１０の前受残高を更新する（Ｓ９１２）。

続いて、データ処理部３０１は最新の前受残高を携帯電話機１３に送信する（Ｓ９１３）。

携帯電話機１３においては、携帯電話会社１０のサーバ３０から送信された前受残高を受信し、この受信した前受残高と同じになるようにＲＡＭ１３２に記憶されている前払残高を更新し、さらに未通知データをクリアする（Ｓ７２９）。

一方、実在店舗２６のＰＯＳ端末２７においては、データ処理部２７１が上記決済内容を携帯電話会社１０のサーバ３０に送信する（Ｓ８０５）。決済内容の送信は取引ごと、つまりリアルタイムで行なうのが望ましいが、営業終了後に一括してバッチ処理で行なってもよい。

携帯電話会社１０のサーバ３０においては、データ処理部３０１はＰＯＳ端末２７から送信された決済内容を受信する（Ｓ９０６）。

続いて、データ処理部３０１は決済完了の情報をＰＯＳ端末２７に送信する（Ｓ９０７）。そして、携帯電話会社１０は決済内容に基づいて実在店舗２６に対して支払処理を行なう（Ｓ９０８）。

ＰＯＳ端末２７においては、データ処理部２７１が携帯電話会社１０のサーバ３０から送信された決済完了の情報を受信する（Ｓ８０６）。

上記第１の実施の形態ではＰＯＳ端末２７から決済金額を携帯電話機１３に送信し、携帯電話機１３が決済の可否を判定しているが、携帯電話機１３から仮想

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 408 of 1360

口座の残高をＰＯＳ端末２７に送信し、ＰＯＳ端末２７が決済の可否を判定するようにしてもよい。また、上記第１の実施の形態では携帯電話機１３を読取装置２７０を用いてＰＯＳ端末２７に電気的に接続しているが、近距離無線（たとえばブルートゥース(Bluetooth)）、無線ＬＡＮ(Local Area Network)またはＩｒＤＡ(Infrared Data Association)で接続したり、あるいはバーコードリーダを用いて光学的に接続してもよい。バーコードリーダを用いる場合、携帯電話機１３からＰＯＳ端末２７に送信するデータをバーコードで表示装置１３７に表示し、これをバーコードリーダで読取るようにすればよい。これらの変更は後述する実施の形態でも適用可能である。

７．本サービスの利点

７－１．クレジットカード番号、キャッシュカード番号、口座番号がインターネット上に流れない。

クレジットによる決済の場合、クレジットカード番号さえあれば決済可能な場合があり、特にインターネット上の決済においては、利用者はクレジットカード番号を入力することに強い不安と抵抗を感じることになり、事実、第三者にクレジットカード番号を知られると決済されてしまう危険性や、店頭においてもカード番号が盗まれる危険性は否定できない。しかしながら、この実施の形態ではインターネット上に流れる決済取引データにクレジットカード番号は含まれておらず、携帯電話番号がその役目を果たすものである。また、携帯電話番号はその利用目的上、広く第三者に知られているが、第三者が他人の携帯電話番号のみを知っていても携帯電話機そのものを持っていないと、実在店舗でもインターネット上の仮想店舗でも決済を完了できないうえ、決済限度額が仮想口座内の残高に限定されるため、安全性は高い。

７－２．決済の際に信用照会および承認が不要である。

利用者が携帯電話会社の仮想口座に資金を預ける（前払）する際に、その支払方法ごとに必要とされる信用照会および承認が行なわれるので、利用者がインターネット上の仮想店舗や実在店頭で決済するときには、決済金額が前払残高以内であるか否かを確認するだけでよい。現在、店頭決済時に必要とされている承認番号の取得や本人の署名などの手続が不要となる。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 409 of 1360

７－３．店頭決済時に電波を飛ばす必要がない（電波圏外でもよい）。

この実施の形態では、店頭決済時に携帯電話機から必ずしも電波を飛ばす必要はない。したがって、店頭決済を行なう場所が電波圏内であるかどうかを意識する必要がない。よって、電波圏外の多い都市圏の地下街やビル内部、地下鉄構内、地下に設置されている自動販売機や券売機などでも決済することが可能である。携帯電話機が電波圏外にあり、決済金額が携帯電話会社に未通知状態になっていても、携帯電話機の内部メモリに未通知金額が記憶された状態で残り、次回取引発生時には未通知データが必ず送信され、仮想口座の残高が携帯電話機と携帯電話会社との間で同期がとれている状態になってから次の決済処理に入る。

７－４．２４時間仮想口座への振替が可能である。

インターネット上の仮想店舗または実在店舗での決済時に仮想口座の残高が不足しても、原則としてその場で２４時間いつでも仮想口座への資金の振替（前払）をすることが可能であるので、時間を問わず買物ができる。

７－５．決済の際に与信枠や残高を意識する必要がない。

従来、店頭でクレジットカードによる決済をする際に利用限度額を超過するため、クレジットカードによる決済を拒否されることがあり、現金の持ち合せが十分でないときには決済そのものが不可能になることもある。そのため、複数のクレジットカードを使い分けている利用者も多く、かといって利用者が各社クレジットカードごとにその限度額を認識しておくことは現実的には困難である。これに対し、この実施の形態では利用者がいつでも携帯電話会社内の仮想口座に振替済である金額、つまり前払残高を携帯電話機で確認することが可能であり、その上その残高内であれば常に決済可能であることが保証されている。

７－６．利用者は、クレジットカードやデビットカードなどの既存決済手段を提供している売り手から提供されている各サービスプログラムを継続して利用可能である。

利用者は、クレジットカードなどの既存決済手段等を利用して携帯電話会社の仮想口座に資金を振込むことで、信販会社などが提供しているサービスを継続して受けることができる。

７－７．クレジットカードを持てない世代でも後払が可能である。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 410 of 1360

利用者が携帯電話会社内の仮想口座に「通話料に加算」という支払方法で資金の振替を指定する場合、実際に利用者の口座から資金が引落されるのは通話料金の引落し時点である。よって、クレジットカードを持てない世代でも通話料の引落し時に口座に資金があればよいことになり、クレジットカードのような「擬似翌月一括払」が可能となる。

７－８．宅配業者が提供する「代金引換え」において利用可能となれば、利用者は予め現金を準備しておく必要がなくなる。

宅配業者は、商品配達時に代金を回収する手段として、携帯電話機による決済を導入することにより、利用者は現金を予め用意する必要がなくなり、宅配業者は配達員に釣銭を持たせる必要が軽減する。店頭のＰＯＳ端末のように携帯電話会社のサーバと決済ごとにデータの送受信を行なわず、一括してその日の業務終了後に送信する方法や、その都度無線で送受信する方法等が考えられる。また、こういった移動先での決済を可能とする端末は、小規模店舗等でも流用可能であるうえ、導入が容易である。

７－９．銀行振込やコンビニエンスストアでの決済と比較して手数料が割安である。

携帯電話会社内の仮想口座への資金の振替を「通話料に加算」という支払方法で行なう場合、利用者は１００円～２００円程度の月額使用料を支払う。少額決済を同じ月内に繰返し行なう場合等は、銀行振込みやコンビニエンスストアでの決済を利用する場合よりも利用者が負担する手数料が安く済むことになる。

７－１０．手数料負担が公平である。

現行のクレジットカードやデビットカードによる決済では、手数料を加盟店が負担しており、その課金方法では少額決済では売上利益を圧迫するため、クレジットカードやデビットカードによる決済を採用していない（加盟していない）店舗がある。一方、この実施の形態では携帯電話会社への資金振込みの際にクレジットカードやデビットカードを利用する場合、極端な少額を振替える例は少ないと想定され、必要に応じて携帯電話会社が資金振替の際の最低金額やその単位を予め設定することにより、携帯電話会社が負担する信販会社等に支払う手数料と収入金額のバランスを取ることが可能である。一方、携帯電話会社から加盟店へ

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 411 of 1360

資金を振替える際には、その振替金額の一定期間中の合計に対して手数料が計算され、課金される。つまり、利用者が決済するごとに、その決済金額に対して手数料が加盟店に課金される現状のクレジットカードやデビットカードによる決済方法とは違い、加盟店は携帯電話会社からその合計金額に対する手数料を課金されることになり、少額決済の多い店舗（企業）であっても導入しやすく、個々の取引決済金額の大小にかかわらず、手数料負担が公平である。つまり、従来の決済システムでは、少額決済が大半を占める店舗、企業（たとえばコンビニエンスストア）でも、利益率を圧迫されることがない。

７－１１．少額取引に適した決済システムである。

上記７－１０のとおり、手数料負担が公平であることから、少額決済が大半を占める店舗や企業（たとえばコンビニエンスストア）でも、売上利益を圧迫されることはない。また、クレジットカードやデビットカードによる決済方法を導入している店舗や企業でも、負担する手数料の売上金額に対する割合を考慮し、利用可能な最低決済金額（たとえば３０００円以上）が設けられていることが多いが、この実施の形態では手数料は一定期間中の合計決済金額に対して課金されるので、限度額設定の必要がない。

７－１２．携帯電話機に金銭的な価値を付加するものではない。

現在、進行中の電子マネー計画では携帯電話機に金銭情報そのものをダウンロードして利用することを目的としているが、この実施の形態では仮想口座から振込を実現するための道具として携帯電話機を使用するものであり、電子マネーを仮想口座に振込む資金として利用することも可能である。商取引に携帯電話会社および決済サイトを介在させることにより、その安全性と利便性を高めることが目的であり、携帯電話機に金銭価値を付加するものではない。したがって、電子マネーは紛失したら現金を紛失することと同じであるが、この実施の形態では携帯電話機を落としても金銭的価値が消失するものではない。

７－１３．端末の不正使用に対する安全性

紛失や盗難の際も携帯電話会社にサービス停止を依頼することが可能であり、サービス停止になるまでに店頭で悪用されたとしても、利用できる金額は仮想口座内の残高内である。また、本人が携帯電話機を所有しているにもかかわらず、

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 412 of 1360

その携帯電話番号がインターネット上で第三者に悪用された場合でも、他の決済手段では決済が完了するまでまたは利用明細書が届くまで本人が認識することが困難であるのに対し、この実施の形態では決済確認がすべて携帯電話機に送信されることから、決済が完了する前に本人が認識し、未然に防ぐことが可能である。なお、携帯電話機の利用契約者が本サービスの停止を携帯電話会社に申告している場合は、インターネット上での決済の場合は携帯電話機の利用状況の確認の際に、実在店舗での決済の場合は決済モードをオンにする際にサービスの利用不可として通知される。

７－１４．携帯電話機と携帯電話会社のサーバ間での取引の安全性が高い。

携帯電話機から携帯電話会社のサーバには携帯電話番号とキーコードとがペアで送信され、携帯電話会社はこの両者を用いて認証を行なっている。携帯電話番号は利用者に固有で、キーコードは携帯電話機に固有であるから、利用者１２の携帯電話番号を知っている第三者であっても、利用者１２自身の携帯電話機１３以外の携帯電話機を使って上述した取引を行なうことはできない。

７－１５．短時間で決済が完了する。

上記７－２のとおり、与信照会は前払い時に行ない、決済時には行なう必要がないので、決済にかかる時間は短い。この時間は、現在実在店舗で行なわれているクレジットカードやデビッドカードによる決済にかかる時間よりも短い。

［第２の実施の形態］

以上、本発明の実施の形態を説明したが、本発明はその他の形態でも実施可能なものである。たとえば上記実施の形態では携帯電話会社に仮想口座を設けているが、銀行のような金融機関に仮想口座を設けてもよく、要するに携帯電話機と直接または間接的に通信可能なサーバに仮想口座を設ければよい。以下、本発明の第２の実施の形態を上記第１の実施の形態との相違点を中心に説明する。

１．資金移動

図２５は、この発明の第２の実施の形態における資金移動を示す概略図である。図１に示した第１の実施の形態と異なり、この第２の実施の形態では図２５に示すように、利用者１２の仮想口座１１０が銀行などの金融機関７０のサーバコンピュータに設けられる。この仮想口座１１０には残高の他、実在口座番号、仮想

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 413 of 1360

口座番号、携帯電話会社、および携帯電話番号が記憶される。実在口座番号としては、利用者１２が金融機関７０に実際に開設している口座の番号が登録される。仮想口座番号としては、この仮想口座１１０を特定するための番号が登録される。携帯電話会社としては、利用者１２が契約している携帯電話会社１０の名称が登録される。携帯電話番号としては、利用者１２の携帯電話機１３の携帯電話番号が登録される。

金融機関７０には仮想口座１１０の他、利用者１２の実在口座７１０、仮想口座１１０の入出金履歴データベース７１２、および仮想口座１１０の決済履歴データベース７１４が設けられる。利用者１２の実在口座７１０には、実在口座番号および口座残高が記憶される。入出金履歴データベース７１２には、仮想口座１１０の口座番号と、仮想口座１１０の入出金の日付と、その入出金額とが記憶される。決済履歴データベース７１４には、仮想口座１１０の口座番号と、仮想口座１１０の入出金の日付と、決済金額と、携帯電話機１３にその時点での仮想口座残高を携帯電話機１３に通知したか否かを示す状態とが記憶される。一方、携帯電話会社１０のサーバコンピュータにおける個人情報データベース１１には利用者１２が取引している金融機関７０の名称が記憶される。

図２６は、資金移動に用いられる携帯電話機、携帯電話会社のサーバ、および金融機関のサーバのハードウェア構成を示すブロック図である。上記図７に示した第１の実施の形態と異なり、この第２の実施の形態では図２６に示すように携帯電話会社１０のサーバ３０のデータベース３０２には前受け履歴や決済履歴は記録されない。また、この個人情報データベース１１には仮想口座情報は記録されない。その代わり、金融機関７０のサーバ７２にはデータベース７０２が設けられ、このデータベース７０２に仮想口座情報１１０、仮想口座入出金履歴７１２、および仮想口座決済履歴７１４が記録される。サーバ７２のデータ処理部７０１はサーバ３０のデータ処理部３０１と通信し、データベース７０２を用いて決済処理を行なう。

図２７および図２８は、金融機関７０の仮想口座１１０に資金を振替える場合における携帯電話機１３、携帯電話会社のサーバ３０、および金融機関のサーバ７２の動作を示すフローチャートである。図２９は、この場合に携帯電話機１３

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 414 of 1360

に表示される画面の遷移図である。

図２７に示すようにこの第２の実施の形態では、ステップＳ１０４において、利用者１２は携帯電話機１３の入力装置１３６を操作して所望の振替金額を入力する。これにより、入力装置１３６はその入力された振替金額をデータ処理部１３１に与える。

続いて、携帯電話機１３の送受信部１３５は、携帯電話番号、キーコードおよび未通知データとともに、その入力された振替金額を携帯電話会社１０のサーバ３０に送信する。

携帯電話会社１０のサーバ３０においては、上記第１の実施の形態と同様に、受信した携帯電話番号およびキーコードを用いて認証を行なった後（Ｓ２０２，Ｓ２０３）、図２８に示すように利用者１２の取引銀行へ振替依頼を送信する（Ｓ２４０）。具体的には、利用者１２の個人情報データベース１１から利用者１２の取引銀行の名称（ここではＢ銀行）を読出し、Ｂ銀行のサーバ７２に利用者１２の携帯電話番号および振替金額を送信し、これにより利用者１２の実在口座７１０から仮想口座１１０にその送信した金額を振替えるよう依頼する。

金融機関７０のサーバ７２においては、データ処理部７０１が携帯電話会社１０から送信された上記振替依頼を受信する（Ｓ１０００）。

続いて、データ処理部７０１は利用者１２の実在口座７１０を参照して振替が可能か否かを判定する（Ｓ１００１）。依頼のあった振替金額が実在口座７１０の残高を超えている場合、データ処理部７０１は振替不可の情報を携帯電話会社１０のサーバ３０に送信する（Ｓ１００２）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７０から送信された振替不可の情報を受信し（Ｓ２４１）、引続きこれを利用者１２の携帯電話機１３に送信する（Ｓ２４２）。

利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された振替不可の情報を受信する（Ｓ１４０）。

続いて、データ処理部１３１は表示装置１３７上に図２９に示した画面Ｄ２１を表示し（Ｓ１４１）、残高不足のために振替ができない旨を利用者１２に通知する。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 415 of 1360

続いて、データ処理部１３１は表示装置１３７上に異常終了を表示する（Ｓ１４２）。

上記ステップＳ１００１において依頼のあった振替金額が実在口座７１０の残高以内の場合、データ処理部７０１はその依頼のあった金額を実在口座７１０から仮想口座１１０に振替える（Ｓ１００４）。

続いて、データ処理部７０１は上記振替金額に基づいて入出金履歴データベース７１２を更新する（Ｓ１００５）。

続いて、上記ステップＳ１０００で受信した情報の中に未通知データがあるか否かをデータ処理部７０１が判別する（Ｓ１００５）。上記ステップＳ７０４で未通知データが存在し、上記ステップＳ１０６で携帯電話機１３から携帯電話会社１０に未通知データを送信し、さらに上記ステップＳ２４０で携帯電話会社１０から金融機関７０に未通知データを送信している場合、データ処理部７０１はその未通知データに基づいて決済履歴データベース７１４を更新する（Ｓ１００６）。未通知データが存在しない場合、データ処理部７０１は仮想口座１１０の残高を携帯電話会社１０に送信する（Ｓ１００７）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７０から送信された仮想口座１１０の残高を受信し（Ｓ２４３）、引続きこれを利用者１２の携帯電話機１３に送信する（Ｓ２０７）。

携帯電話機１３においては、上記第１の実施の形態と同様に送受信部１３５が携帯電話会社１０から送信された仮想口座１１０の残高を受信し（Ｓ１１３）、データ処理部１３１がＲＡＭ１３２に記録されている仮想口座の残高を更新し（Ｓ１１４）、最後に表示装置１３７上に振替が完了した旨を表示する（Ｓ１１５）。ここで、未通知データが存在する場合はその未通知データをクリアする（Ｓ１４３）。

２．仮想店舗での決済

図３０は、この発明の第２の実施の形態による仮想店舗での決済を示す概略図である。図３０に示すように、ここではインターネット上の仮想店舗２４と金融機関７０との間に決済機関８０が設けられる。決済機関８０は本サービスが利用される度に決済情報８１０を蓄積し、蓄積した多数の決済情報８１０に基づいて

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 416 of 1360

仮想店舗２４に対して利用代金を一括して支払う。決済情報８１０には、銀行名として金融機関７０の名称、支払者名として利用者１２の氏名または名称、振替金額、仮想口座１１０の仮想口座番号、および支払先としてインターネット上の仮想店舗２４の名称が含まれている。

図３１は、仮想店舗での決済に用いられるパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、金融機関７０のサーバ７２、決済機関８０のサーバ８２、および仮想店舗２４のサーバ５０のハードウェア構成を示すブロック図である。図３１に示すように、決済機関８０のサーバ８２には、データ処理部８０１と、データベース８０２とが設けられる。データベース８０２には決済情報８１０が蓄積される。データ処理部８０１はサーバ７２のデータ処理部７０１と通信し、データベース８０２に蓄積した決済情報８１０に従って仮想店舗２４に対して支払処理を行なう。

図３２～図３４は、仮想店舗２４で決済を行なう場合におけるパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、仮想店舗２４のサーバ５０、および金融機関７０のサーバ７２の動作を示すフローチャートである。ここでは説明を簡単にするために、決済機関８０のサーバ８２の動作を省略する。

図１７に示した第１の実施の形態と同様に、携帯電話会社１０のサーバ３０は仮想店舗２４からの請求データを携帯電話機１３に送信する（Ｓ５０５）。

携帯電話機１３においては、送受信部１３５がその請求データを受信する（Ｓ４０１）。

続いて、その電子メールで送られてきた電子請求書を開封する（Ｓ４２０）。

続いて、上記第１の実施の形態と同様に未通知データを処理した後（Ｓ４０５～Ｓ４０７）、データ処理部１３１が表示装置１３７上に請求内容および利用可能残高（たとえば図３５に示した画面Ｄ２２またはＤ２３）を表示する（Ｓ４２１）。

続いて、データ処理部１３１は請求額が利用可能残高以内か否かを検証する（Ｓ４２２）。請求額が利用可能残高以内の場合、図３５の画面Ｄ２２のように「支払」のボタンが表示される。請求額が利用可能残高を超えている場合、図３

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 417 of 1360

５の画面Ｄ２３のように「お財布にお金を入れる」のボタンが表示される。

請求額が利用可能残高を超えている場合、データ処理部１３１は利用者１２の操作に応じて追加資金を振替えるか否かを判別する（Ｓ４２３）。追加資金を振替える場合は上述した資金振替を行ない（Ｓ４２４）、追加資金を振替えない場合はステップＳ４０３に移る。

上記ステップＳ４２２で請求額が利用可能残高以内の場合、上記第１の実施の形態と同様に利用者１２が決済を承認したか否かを判別する（Ｓ４０２）。

また、携帯電話会社１０のサーバ３０において、パスワードを確認した後（Ｓ５１２）、データ処理部３０１は金融機関７０に対して決済依頼の情報を送信するとともに、未通知データが存在する場合はその未通知データを送信する（Ｓ５２０）。

金融機関７０のサーバ７２においては、データ処理部７０１が携帯電話会社１０から送信された決済依頼の情報を受信する（Ｓ１１００）。

続いて、データ処理部７０１は受信した決済金額を利用者１２の仮想口座１１０から振替える（Ｓ１１０１）。未通知データを受信している場合、その未通知の決済金額も利用者１２の仮想口座１１０から振替える。ここでは、仮想店舗２４への決済金額の振替を決済機関８０に依頼する。決済機関８０は依頼のたびにその決済金額を仮想店舗２４に支払うのではなく、たとえば所定の月度単位で複数の決済金額をまとめて仮想店舗２４に支払う。このような決済機関８０は必ずしも必要なく、金融機関７０が決済金額を直接仮想店舗２４に支払うようにしてもよい。ただし、決済機関８０を設けた方が振替の度に発生する手数料を抑えることができる。

続いて、データ処理部７０１はその決済金額に基づいて入出金履歴データベース７１２を更新する。（Ｓ１１０２）。

続いて、データ処理部７０１はその決済金額に基づいて決済履歴データベース７１４を更新する。（Ｓ１１０３）。

続いて、データ処理部７０１は仮想口座１１０の残高を読出して携帯電話会社１０に送信する（Ｓ１１０４）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 418 of 1360

０から送信された仮想口座残高を受信し（Ｓ５２１）、引続きこれを利用者１２の携帯電話機１３に送信する（Ｓ５１６）。

３．実在店舗での決済

図３６は、この発明の第２の実施の形態による実在店舗での決済を示す概略図である。図３６に示すように、実在店舗で決済する場合も決済機関８０が金融機関７０からの振替依頼を一括して実在店舗２６に対して支払を行なう。

図３７は、実在店舗での決済に設けられる携帯電話機１３、ＰＯＳ端末２７、携帯電話会社１０のサーバ３０、金融機関７０のサーバ７２、および決済機関８０のサーバ８２のハードウェア構成を示すブロック図である。

図３７に示すように、決済機関８０のサーバ８２におけるデータ処理部８０１はサーバ７２のデータ処理部７０１と通信し、決済情報８１０に従って実在店舗２６に対する支払を行なう。

図３８～図４０は、実在店舗で決済する場合における携帯電話機１３、ＰＯＳ端末２７、携帯電話会社１０のサーバ３０、および金融機関７０のサーバ７２の動作を示すフローチャートである。

上記図２１に示した第１の実施の形態と異なり、この第２の実施の形態では図３８に示したステップＳ７０７において、携帯電話機１３のデータ処理部１３１はＲＡＭ１３２に記録されている仮想口座残高からステップＳ７０７で計算した累計未通知金額を減算する。

また、携帯電話会社１０のサーバ３０において、ステップＳ９０２でキーコードの一致を確認した場合、データ処理部３０１は未通知データを金融機関７０のサーバ７２に送信する（Ｓ９２０）。

金融機関７０のサーバ７２においては、データ処理部７０１が携帯電話会社１０から送信された未通知データを受信する（Ｓ１２００）。

続いて、データ処理部７０１は受信した未通知データに基づいて決済履歴データベース７１４を更新する（Ｓ１２０１）。

続いて、データ処理部７０１は仮想口座１１０の仮想口座残高を携帯電話会社１０のサーバ３０に送信する（Ｓ１２０２）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 419 of 1360

０から送信された仮想口座残高を受信し（Ｓ９２１）、引続きこれを利用者１２の携帯電話機１３に送信する（Ｓ１０５）。

携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された仮想口座残高を受信し（Ｓ７１２）、さらにデータ処理部１３１はその受信した仮想口座残高に基づいてＲＡＭ１３２に記録されている仮想口座残高を更新しかつ未通知データをクリアする（Ｓ７１３）。

また、携帯電話会社１０のサーバ３０においては、ステップＳ９０６で実在店舗２６から送信された決済内容を受信した後、データ処理部３０１がその受信した決済内容を金融機関７０のサーバ７２に送信する（Ｓ９２２）。金融機関７０のサーバ７２においては、データ処理部７０１が携帯電話会社１０から送信された決済内容を受信する（Ｓ１２０３）。

続いて、データ処理部７０１はその受信した決済内容に基づいて決済履歴データベース７１４を更新する（Ｓ１２０４）。

続いて、データ処理部７０１は決済完了の情報を携帯電話会社１０のサーバ３０に送信する（Ｓ１２０５）。そして、金融機関７０は上記仮想店舗の場合と同様に決済機関８０を通じて実在店舗２６に対する支払処理を行なう（Ｓ１２０６）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７０から送信された決済完了の情報を受信し（Ｓ９２３）、引続きこれを実在店舗２６のＰＯＳ端末２７に送信する（Ｓ９０７）。

また、携帯電話会社１０のサーバ３０においては、ステップＳ９０９でキーコードの一致を確認した場合、データ処理部３０１はステップＳ９０９で受信した未通知データを金融機関７０のサーバ７２に送信する（Ｓ９２４）。

金融機関７０のサーバ７２においては、データ処理部７０１が携帯電話会社１０から送信された未通知データを受信しする（Ｓ１２０７）。

続いて、データ処理部７０１はその受信した未通知データに基づいて決済履歴データベース７１４を更新する（Ｓ１２０８）

続いて、データ処理部７０１は仮想口座１１０の仮想口座残高を読出して携帯電話会社１０のサーバ３０に送信する（Ｓ１２０９）。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 420 of 1360

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７０から送信された仮想口座残高を受信し（Ｓ９２５）、引続きこれを利用者１２の携帯電話機１３に送信する（Ｓ９１３）。

利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された仮想口座残高を受信し（Ｓ７３０）、さらにその受信した仮想口座残高に基づいてＲＡＭ１３２に記録されている仮想口座残高を更新しかつ未通知データをクリアする（Ｓ７２９）。

以上のようにこの発明の第２の実施の形態によれば、仮想口座１１０を金融機関７０に設けているため、仮想口座１１０への資金移動が上記第１の実施の形態に比べて簡単になる。

上記第２の実施の形態では金融機関７０に実在口座７１０とは別に仮想口座１１０を設けているが、実在口座７１０をそのまま仮想口座１１０として取扱うようにしてもよい。この場合、実在口座７１０から仮想口座１１０への資金移動が不要となるため、処理手続はさらに簡単になる。

上記実施の形態のインターネット上の仮想店舗での決済では利用者はパーソナルコンピュータを用いて注文をしているが、携帯電話機を用いて注文をする場合もある。この場合、携帯電話機がパーソナルコンピュータの代わりの機能を果たす。

［第３の実施の形態］

仮想口座を上記第１の実施の形態では携帯電話会社に設け、上記第２の実施の形態では金融機関に設けているが、以下に述べる第３の実施の形態では携帯電話会社や金融機関とは別個の決済機関に仮想口座を設ける。

１．サービスの概要

この第３の実施の形態によるサービスの利用を希望する利用者は、仮想口座に前払金を入金するために必要な銀行の口座番号や信販会社のクレジットカード番号などを決済機関に予め登録しておく。利用者は、決済の前に、仮想口座に前払金を入金するように、携帯電話機を用いて携帯電話会社を通じて決済機関に要請する。決済機関は、予め登録されている銀行の口座番号や信販会社のクレジットカード番号などを用い、利用者に対して前払金の請求を行なう。決済機関は、前

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 421 of 1360

払金の請求後、前払金を仮想口座に入金した上で仮想口座の残高を携帯電話会社を介して携帯電話機に送信する。仮想店舗や実在店舗は、上記第１および第２の実施の形態のように携帯電話会社や金融機関ではなく、決済機関に対して請求を行なう。

１－１．利用登録

図４１は、携帯電話機１３の利用者１２が本サービスの利用を希望する場合に最初に行なう利用登録の方法を示す概略図である。図４１に示すように、本サービスの利用を希望する利用者１２は、加入している携帯電話会社、携帯電話番号、および前払金を引落すための銀行の口座番号や信販会社のクレジットカード番号といった決済情報を所定の引落口座登録用紙２５に記入して決済機関９０に郵送する。決済機関９０は、引落口座登録用紙２５に基づいて利用者情報９１０をデータベースに登録する。

続いて、決済機関９０は、利用者１２に付与した会員番号（利用者情報９１０中の顧客番号）を携帯電話会社１０を通じて利用者１２に通知する。利用者１２はその通知内容を確認し、問題がなければ携帯電話会社１０を通じて決済機関９０に対して本サービスの申込を承認する。これに応じて決済機関９０は、仮想口座１１０を開設するとともに、仮想口座の入出金履歴９１２や決済履歴９１４を記録するための領域をデータベース内に開設する。

なお、決済機関９０のデータベースには、本サービスの利用が可能な加盟店（仮想店舗および実在店舗を含む）とその加盟店における利用金額を振込むための振込口座などの加盟店情報９１６が登録されている。

続いて、決済機関９０は、本サービスの開始を携帯電話会社１０を通じて利用者１２の携帯電話機１３に通知する。このとき、携帯電話会社１０は個人情報１１の利用状況を「未登録」から「利用可」に変更する。利用者１２の携帯電話機１３が携帯電話会社１０から本サービス開始の通知を受けると、携帯電話機１３の利用状況を「利用不可」から「利用可」に変更する。

上記手続により、利用者１２は本サービスの利用が可能となる。

１－２．仮想口座への資金移動

図４２は、決済機関９０に設けた仮想口座１１０に入金する前払金を金融機関

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 422 of 1360

の口座から引落しする場合の資金移動を示す概略図である。図４２に示すように、利用者１２は携帯電話機１３を用い、携帯電話会社１０を通じて決済機関９０に対して所望の前払金を仮想口座１１０に入金するよう要請する。ここでは仮想口座１１０に５０００円を入金する場合を例示している。決済機関９０は仮想口座１１０への前払の要請を受けると、利用者情報９１０に基づき、利用者１２の口座１６０が開設されている銀行や信販会社のような金融機関１７０に対して前払金の引落しを依頼する。引落し依頼を受けた金融機関１７０は引落しが可能か否かを確認し、可能な場合は振替データを決済機関９０に送り、前払金を決済機関９０に支払う。引落しが不可能な場合はその旨決済機関９０に通知する。決済機関９０は金融機関１７０から振替データを受けると、入出金履歴９１２を更新し、さらに仮想口座１１０を更新する。続いて、決済機関９０はその更新した仮想口座１１０の残高を携帯電話会社１０に通知する。携帯電話会社１０では、携帯電話番号や仮想口座残高などの送信データ１０２が作成される。携帯電話会社１０はこの送信データ１０２に基づいて利用者１２に仮想口座残高を通知する。この通知に応じて利用者１２の携帯電話機１３は仮想口座残高を更新する。携帯電話会社１０から利用者１２の携帯電話機１３への送信データ１０２の送信が完了すると、送信データ１０２はクリアされる。利用者１２が電波圏外にいる場合など、送信データ１０２の送信が不可能な場合、送信データ１０２はクリアされずにそのまま保持される。

１－３．仮想店舗での決済

図４３は、携帯電話機１３を用いてインターネット上の仮想店舗２４で決済する方法を示す概略図である。図４３に示すように、利用者１２は携帯電話機１３またはパーソナルコンピュータ４０を用いて仮想店舗２４に対して注文を出す。注文を受けた仮想店舗２４は、利用者１２の顧客番号や請求内容などを記載した電子請求書を決済機関９０および携帯電話会社１０を通じて利用者１２の携帯電話機１３に送信する。利用者１２はその送信された電子請求書を携帯電話機１３で確認し、その請求内容が自らの注文内容と一致する場合は決済の承認を携帯電話会社１０を通じて決済機関９０に通知する。決済機関９０は決済の承認を得ると、その請求内容に応じて入出金履歴９１２および決済履歴９１４を更新すると

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 423 of 1360

ともに、仮想口座１１０の残高も更新する。ここではB店という仮想店舗２４で３０００円の商品を購入した場合を例示している。

続いて、決済機関９０はその更新した仮想口座残高を携帯電話会社１０に通知する。携帯電話会社１０はその仮想口座残高を送信データ１０２とし、さらに利用者１２の携帯電話機１３に送信する。これに応じて携帯電話機１３の仮想口座残高が更新される。携帯電話会社１０から利用者１２への仮想口座残高の送信が完了すると、送信データ１０２はクリアされる。

一方、決済機関９０は仮想口座残高の更新を終えると、決済の完了を仮想店舗２４を通じて利用者１２に通知する。また、決済機関９０は加盟店情報９１６に基づいてその決済金額を加盟店の振込口座に入金する。

１－４．実在店舗での決済

図４４は、携帯電話機１３を用いて実在店舗２６で決済する方法を示す概略図である。図４４に示すように、実在店舗２６に設置されているＰＯＳ端末２７に携帯電話機１３が装着されると、ＰＯＳ端末２７は決済金額を携帯電話機１３に送信する。決済金額が仮想口座残高以内の場合、携帯電話機１３は決済内容を未通知データに記録するとともに、携帯電話番号、キーコードおよびパスワードをＰＯＳ端末２７に送信する。これに応じて、ＰＯＳ端末２７は決済の完了を携帯電話機１３に通知する。

その後、ＰＯＳ端末２７は、携帯電話番号、キーコードおよびパスワードとともに決済内容を決済機関９０に通知する。決済機関９０は、受信した携帯電話番号、キーコードおよびパスワードを携帯電話会社１０に送信することにより認証を依頼する。認証依頼を受けた携帯電話会社１０は、個人情報１１の未通知を「無」から「有」に変更する。受信した携帯電話番号、キーコードおよびパスワードが個人情報１１として登録されている携帯電話番号、キーコードおよびパスワードと一致しない場合、携帯電話会社１０は個人情報１１の利用状況を「認証異常」に変更し、その旨を利用者１２および決済機関９０に通知する。この通知に応じて、携帯電話機１３は利用状況を「認証異常」に変更する。

一方、受信した携帯電話番号、キーコードおよびパスワードが個人情報１１として登録されている携帯電話番号、キーコードおよびパスワードと一致した場合、

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 424 of 1360

携帯電話会社１０は認証が正常に完了した旨を決済機関９０に通知する。この通知に応じて、決済機関９０は入出金履歴９１２および決済履歴９１４を更新する。決済機関９０はさらに、仮想口座１１０の残高を更新するとともに、未通知を「無」から「有」に変更する。ここでは、Ｄ店という実在店舗２６で１０００円の商品を購入した場合を例示している。

続いて、決済機関９０は決済が完了した旨を実在店舗２６に通知する。また、決済機関９０は加盟店情報９１６に基づいて加盟店の振込口座にその決済金額を入金する。

１－５．未通知データの要求

図４５は、利用者１２が実在店舗２６で決済をしたために携帯電話機１３内に未通知データが発生して携帯電話機１３の仮想口座残高が決済機関９０の仮想口座残高と一致しなくなった場合に決済機関９０が仮想口座残高の同期をとるために携帯電話機１３に対して未通知データの送信を要求する方法を示す概略図である。図４５に示すように、決済機関９０は携帯電話会社１０を通じて利用者１２の携帯電話機１３に未通知データを要求する。これに応じて、携帯電話機１３は携帯電話会社１０を通じて未通知データを決済機関９０に送信する。決済機関９０は、受信した未通知データに基づいて決済履歴９１４のうち該当の決済の状態を「未通知」から「通知済」に変更する。

続いて、決済機関９０は仮想口座１１０の残高を携帯電話会社１０に送信する。携帯電話会社１０は受信した仮想口座残高を送信データ１０２とするとともに、個人情報１１中の未通知を「有」から「無」に変更する。携帯電話会社１０は仮想口座残高を携帯電話機１３に送信する。これに応じて、携帯電話機１３は仮想口座残高を更新するとともに、未通知データをクリアする。携帯電話会社１０は仮想口座残高の送信を完了すると、送信データ１０２をクリアする。

１－６．請求代行

図４６は、仮想店舗２４に代わって決済機関９０が利用者１２による仮想店舗２４での決済金額を信販会社２０に請求する方法を示す概略図である。この請求代行は、決済機関９０に設けた仮想口座１１０を利用するものではなく、利用者情報９１０として登録されている銀行の口座番号や信販会社のクレジットカード

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 425 of 1360

番号を利用してデビット決済やカード決済を行なうものである。

図４６に示すように、利用者１２が携帯電話機１３またはパーソナルコンピュータ４０を用いて仮想店舗２４に対して注文をすると、仮想店舗２４は顧客番号や請求内容などからなる電子請求書を決済機関９０および携帯電話会社１０を通じて利用者１２に発行する。利用者１２は携帯電話機１３に送信された電子請求書を確認し、決済を承認する場合はその旨を携帯電話会社１０を通じて決済機関９０に通知する。その際に、予め登録している決済方法の中から１つを選択する。ここでは、信販会社Ｅ社のクレジットカードによる決済を選択した場合を例示している。

決済機関９０は決済の承認を仮想店舗２４に通知するとともに、利用者情報９１０を用いてクレジットカード番号や決済金額などの決済内容を信販会社２０に通知する。これに応じて信販会社２０は仮想店舗２４に対して決済金額の支払処理を行ない、決済が完了した旨を仮想店舗２４に通知する。

利用者１２が決済方法としてデビットカードによる決済を選択した場合、決済機関９０は利用者情報９１０を用いて口座番号や決済金額などの決済内容を銀行１７に通知する。銀行１７はその決済金額を利用者１２の口座から引落し、さらに仮想店舗２４に対してその決済金額の支払処理を行なう。

上記請求代行サービスでは、銀行の口座番号や信販会社のクレジットカード番号といった重要な決済情報は予め決済機関９０に登録されており、携帯電話機１３やパーソナルコンピュータ４０から送信されることはない。認証は携帯電話番号、キーコードおよびパスワードを用いて携帯電話会社１０で行なわれ、認証が得られた場合だけ予め登録されている口座番号やクレジットカード番号が決済機関９０から金融機関１７０や信販会社２０に通知される。したがって、高い安全性を確保することができる。

２．システム構成およびその動作

次に、上記サービスを実現するためのシステム構成およびその動作について説明する。

２－１．利用登録

図４７は、図４１に示した利用登録のためのハードウェア構成を示すブロック

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 426 of 1360

図である。上記第１および第２の実施の形態と異なり、この第３の実施の形態では、携帯電話会社１０のサーバ３０には、送信データ１０２を記憶するためのメモリ３０３が設けられる。また、決済機関９０のサーバ９２には、データ処理部９２１と、データベース９２２とが設けられる。データベース９２２には、利用者情報９１０、仮想口座の入出金履歴９１２、仮想口座の決済履歴９１４および加盟店情報９１６が蓄積される。データ処理部９２１は、携帯電話会社１０に設置されているサーバ３０のデータ処理部３０１と接続され、データベース９２２に対して所定のデータ処理を行なう。

図４８は、利用登録を行なう場合における利用者１２の携帯電話機１３、携帯電話会社１０のサーバ３０および決済機関９０のサーバ９２の動作を示すフローチャートである。

まず、利用者１２は携帯電話機１３の入力装置１３６を操作して本サービスの利用申込を携帯電話機１３から携帯電話会社１０に送信する（Ｓ１１）。携帯電話会社１０のサーバ３０においては、データ処理部 301 が携帯電話機１３から送信された利用申込を受信し（Ｓ２１）、これを決済機関９０に送信する（Ｓ２２）。決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された利用申込を受信する（Ｓ１３０１）。これに応じて、決済会社９２は所定の申込用紙を利用者１２に発送する（Ｓ１３０２）。利用者１２は申込用紙に引落しを希望する銀行の口座番号や信販会社のクレジットカード番号などを記入した後、決済機関９０に返送する。決済機関９０は利用者１２から返送された申込用紙を受取る（Ｓ１３０２）。この申込用紙に記入された事項に基づいて、データ処理部３０１は利用者情報９１０をデータベース９２２に登録する（Ｓ１３０３）。具体的には、利用者１２の会員番号、携帯電話番号、携帯電話会社、銀行の口座番号、信販会社のクレジットカード番号などを登録する。続いて、データ処理部９２１は会員番号を携帯電話会社１０に通知する（Ｓ１３０４）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０から送信された会員番号を受信し（Ｓ２３）、これを利用者１２に通知する（Ｓ２４）。利用者１２の携帯電話機１３においては、送受信部１３５が携帯電

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 427 of 1360

話会社１０から送信された会員番号を受信し（Ｓ１２）、利用者１２がその申込を承認した場合はその旨を携帯電話会社１０に通知する（Ｓ１３）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された申込承認の通知を受信し（Ｓ２５）、これを決済機関９０に通知する（Ｓ２６）。

決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された申込承認の通知を受信し(Ｓ１３０５）、仮想口座１１０を開設し（Ｓ１３０６）、本サービスの開始を携帯電話会社１０に通知する（Ｓ１３０７）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０から送信されたサービス開始の通知を受信し（Ｓ２７）、個人情報１１の利用状況を「未登録」から「利用可」に更新する（Ｓ２８）。続いて、データ処理部３０１は本サービスの開始を利用者１２に通知する（Ｓ２９）。利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信されたサービス開始の通知を受信し（Ｓ１４）、利用状況を「利用不可」から「利用可」に更新する（Ｓ１５）。

２－２．仮想口座への資金移動

図４９は、図４２に示した資金移動に用いられる利用者１２の携帯電話機１３、携帯電話会社１０のサーバ３０、決済機関９０のサーバ９２、金融機関１７０のサーバ１７２のハードウェア構成を示すブロック図である。図４９に示すように、金融機関１７０に設置されるサーバ１７２は、データ処理部１７４と、データベース１７６とを備える。データ処理部１７４はデータベース１７６のデータを処理するとともに、携帯電話会社１０に設置されているサーバ３０のデータ処理部３０１に接続される。データベース１７６には、利用者の住所や氏名などの利用者情報１７７と、金融機関１７０に開設されている実在口座に関する実在口座情報１７８と、実在口座における入出金などの実在口座履歴１７９とが登録される。

図５０～図５２は、図４２に示したように金融機関１７０から決済機関９０の仮想口座１１０に資金を移動する場合における携帯電話機１３、携帯電話会社１０のサーバ３０および決済機関９０のサーバ９２の動作を示すフローチャートである。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 428 of 1360

ここでは、パスワードの入力（Ｓ１０１）前に、携帯電話機１３が利用状況を確認し、利用不可の場合はその旨を表示装置１３７に表示する（Ｓ１００）。利用可の場合は利用者１２に対してパスワードの入力を促す（Ｓ１０１）。また、パスワードの検証（Ｓ１０２）後、前払金額の入力（Ｓ１０４）前に、図２１と同様に未通知データを確認して利用可能残高を表示する（Ｓ７１４）。

続いて、携帯電話機１３の送受信部１３５はステップＳ１０４で入力された前払金額などを携帯電話会社１０に送信するが（Ｓ１０６）、ここではステップＳ１０１で入力されたパスワードも携帯電話会社１０に送信する。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が受信した携帯電話番号に基づいて個人情報１１を検索した後（Ｓ２０２）、受信したキーコードおよびパスワードを検証する（Ｓ２０３）。キーコードまたはパスワードが一致しない場合、個人情報１１の利用状況を「利用可」から「利用不可」に変更し（Ｓ２５０）、認証の異常を利用者１２に通知する（Ｓ２５１）。

利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から認証異常の通知を受信し（Ｓ１５０）、これに応じてデータ処理部１３１は携帯電話機１３の利用状況を「利用可」から「認証異常」に変更し（Ｓ１５１）、本サービスの利用停止を表示装置１３７に表示する（Ｓ１５２）。

一方、ステップＳ２０３でキーコードおよびパスワードの両方が一致した場合、データ処理部３０１は個人情報１１の利用状況を確認し（Ｓ２０４）、利用状況が「利用可」の場合は未通知データがあるか否かを判定する（Ｓ２５３）。未通知データがある場合、データ処理部３０１はステップＳ２０１で受信した前払金額とともに未通知データを決済機関９０に送信する（Ｓ２５４）。一方、未通知データがない場合、データ処理部３０１は前払金額のみを決済機関９０に送信する（Ｓ２５５）。このように携帯電話会社１０から決済機関９０に前払金額を送信する際には、利用者１２の携帯電話番号も送信する。

決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された携帯電話番号や前払金額などを受信し（Ｓ１３００）、その受信した情報およびデータベース９２２に登録されている利用者情報９１０に基づいて利用者１２が口座を開設している金融機関１７０に対する請求データを作成

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 429 of 1360

する（Ｓ１３０１）。決済機関９０はその請求データに従って金融機関１７０に前払金額の引落しを依頼する（Ｓ１３０２）。

金融機関１７０は、決済機関９０からの引落し依頼に応じて利用者１２の口座１６０から前払金額を引落す（Ｓ１４００）。続いて、データ処理部１７４は引落しが可能か否か、すなわち前払金額が口座残高以内か否かを判定する（Ｓ１４０１）。引落しが不可能な場合、データ処理部１７４は決済機関９０にその旨を通知する（Ｓ１４０２）。決済機関９０のサーバ９２においては、データ処理部９２１が金融機関１７０から引落し不可の通知を受信し（Ｓ１３０３）、これを利用者１２の携帯電話番号とともに携帯電話会社１０に通知する（Ｓ１３０４）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０から引落し不可の通知を受信し（Ｓ２５６）、これを利用者１２の携帯電話機１３に通知する（Ｓ２３２）。

一方、ステップＳ１４０１において引落しが可能な場合、サーバ１７２のデータ処理部１７４は振替データを決済機関９０に送信し（Ｓ１４０３）、利用者１２の口座１６０から決済機関９０の口座に前払金額を振替える支払処理を実行する（Ｓ１４０４）。

決済機関９０のサーバ９２においては、データ処理部９２１が金融機関１７０から送信された振替データを受信し（Ｓ１３０５）、続いて前払金額の入金をデータベース９２２に記録することにより入出金履歴９１２を更新する（Ｓ１３０６）。未通知データが送信されて来ている場合は、ここで決済金額をデータベース９２２に記録することにより決済履歴９１４を更新する（Ｓ１３０７）。続いて、データ処理部９２１は仮想口座１１０の残高に前払金額を加算することにより仮想口座残高を更新する（Ｓ１３０８）。未通知データがあった場合はこれを「無」に変更する。続いて、データ処理部９２１は仮想口座１１０の残高を携帯電話番号とともに携帯電話会社１０に送信する（Ｓ１３０９）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０から送信された仮想口座残高を受信し（Ｓ２５７）、その仮想口座残高を送信データ１０２としてメモリ３０３に記憶する（Ｓ２５８）。続いて、データ処理部３０１は未通知データを「無」に変更する（Ｓ２５９）。続いて、データ処理

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 430 of 1360

部３０１は、メモリ３０３に記憶された送信データ１０２を利用者１２の携帯電話機１３に送信する（Ｓ２６０）。続いて、上記送信が正常に終了したか否かを判定し（Ｓ２６１）、正常に終了した場合は送信データ１０２をクリアし（Ｓ２６２）、利用者１２が電波圏外にいたり携帯電話機１３の電源を切っていた場合など、送信データを携帯電話機１３に送信できず、送信が正常に終了しなかった場合は再送信処理を行なう（Ｓ２６３）。具体的には、所定期間経過後に送信データ１０２を再び携帯電話機１３に送信する。

２－３．仮想店舗での決済

図５３は、図４３に示した仮想店舗２４での決済に用いられるパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、決済機関９０のサーバ９２および仮想店舗２４のサーバ５０のハードウェア構成を示すブロック図である。図５３に示すように、決済機関９０に設置されたサーバ９２のデータ処理部９２１はインターネット６０に接続される。

図５４～図５６は、図４３に示したように仮想店舗２４で決済する場合におけるパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、決済機関９０のサーバ９２、および仮想店舗２４のサーバ５０の動作を示すフローチャートである。

ここでは、利用者１２のパーソナルコンピュータ４０または携帯電話機１３は注文内容とともに会員番号（顧客番号）を仮想店舗２４に送信する（Ｓ３０１）。仮想店舗２４のサーバはこれらを受信し（Ｓ６０１）、電子請求書を作成して会員番号とともに請求内容をインターネット６０を介して決済機関９０に送信する（Ｓ６０２）。

決済機関９０のサーバ９２においては、データ処理部９２１が仮想店舗２４から送信された電子請求書を受信し（Ｓ１３１０）、その受信した会員番号に基づいてデータベース９２２を検索して利用者情報９１０の中から利用者１２の携帯電話番号および携帯電話会社を特定する（Ｓ１３１１）。続いて、データ処理部９２１は受信した電子請求書を該当の携帯電話会社１０に携帯電話番号とともに送信する（Ｓ１３１２）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 431 of 1360

０から送信された電子請求書を携帯電話番号とともに受信する（Ｓ５０１）。データ処理部３０１は個人情報１１中の利用状況を確認し（Ｓ５０３）、利用状況が「利用不可」の場合はその旨を携帯電話番号とともに決済機関９０に通知する（Ｓ５０４）。

決済機関９０のサーバ９２においては、携帯電話会社１０から携帯電話番号とともに通知されたサービス利用不可の通知を受信し（Ｓ１３１３）、これをインターネット６０を介して仮想店舗２４に通知する（Ｓ１３１４）。

また、利用者１２は、携帯電話会社１０から送信され、携帯電話機１３で受信した電子請求書を開封し（Ｓ４１８）、携帯電話機１３のデータ処理部１３１は受信した電子請求書の請求内容および利用可能な仮想口座残高を表示装置１３７に表示する（Ｓ１５４）。

また、電子請求書の請求金額が利用可能残高を超えている場合、データ処理部１３１は表示装置１３７を通じて利用者１２に対して仮想口座１１０への追加振替を行なうか否かを問合せる（Ｓ１５５）。追加振替を行なう場合、データ処理部１３１は資金振替の処理を実行する（Ｓ１５６）。

また、決済を承認するか否かの判定（Ｓ４０２）は、利用可能残高の検証（Ｓ４０８）後に行なう。携帯電話会社１０のサーバ３０においては、データ処理部３０１が受信した決済の取消または拒否を携帯電話番号とともに決済機関９０に送信する（Ｓ５０７）。決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された決済の取消または拒否を受信し（Ｓ１３１５）、これをインターネット６０を介して仮想店舗２４に送信する（Ｓ１３１６）。決済の取消または拒否は上記実施の形態と同様に仮想店舗２４を介して利用者１２に返信される（Ｓ６０５，Ｓ６０６，Ｓ３０４）。利用者１２のパーソナルコンピュータ４０または携帯電話機１３においては、データ処理部４０１または１３１がその受信した決済の取消または拒否（受注取消）を表示装置４０６または１３７に表示する（Ｓ３０８）。

また、利用者１２の携帯電話機１３においては、パスワードの入力（Ｓ４１１）後に、データ処理部１３１がその入力されたパスワードの検証を行なう（Ｓ１５７）。パスワードが誤っている場合はデータ処理部１３１はその旨を表示装

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 432 of 1360

置１３７に表示し（Ｓ１５８）、パスワードが正しい場合は送受信部１３５は決済の承認を携帯電話会社１０に通知する（Ｓ４１２）。

また、携帯電話会社１０のサーバ３０においては、キーコードまたはパスワードが不一致の場合、データ処理部３０１は個人情報１１の利用状況を「利用可」から「認証異常」に変更し（Ｓ５２２）、その旨を利用者１２に通知し（Ｓ５２３）、さらに決済機関９０にも携帯電話番号とともに通知する（Ｓ５２４）。利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された認証異常の通知を受信し（Ｓ１５９）、データ処理部１３１は利用状況を「利用可」から「認証異常」に変更し、さらに本サービスの利用停止を表示装置１３７に表示する（Ｓ１６１）。一方、決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された認証異常の通知を受信し（Ｓ１３１７）、認証異常を理由に決済が不可能である旨をインターネット６０を介して仮想店舗２４に通知する（Ｓ１３１８）。仮想店舗２４のサーバ５０においては、モデム５０４が決済機関９０から送信された決済不可の通知を受信し（Ｓ６１３）、これに応じて受注の取消をインターネット６０を介して利用者１２のパーソナルコンピュータ４０または携帯電話機１３に送信する（Ｓ６１４）。利用者１２のパーソナルコンピュータ４０または携帯電話機１３においては、モデム４０４または送受信部１３５が仮想店舗２４から送信された受注の取消を受信し（Ｓ３０９）、データ処理部４０１または１３１がその旨を表示装置４０６または１３７に表示する（Ｓ３１０）。

ステップＳ５１１，Ｓ５１２においてキーコードおよびパスワードがともに一致した場合、データ処理部３０１は未通知が「有」か否かを判定し（Ｓ５２５）、未通知データがある場合は決済データおよび未通知データを携帯電話番号とともに決済機関９０に送信する（Ｓ５２６）。未通知データがない場合はデータ処理部３０１は決済データを携帯電話番号とともに決済機関９０に送信する（Ｓ５２７）。決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された決済データ（および未通知データがある場合は未通知データ）を受信し（Ｓ１３１９）、その受信した決済データ（および未通知データがある場合は未通知データ）に基づいて入出金履歴９１２を更新し（Ｓ１３２０）、

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 433 of 1360

決済履歴９１４を更新し（Ｓ１３２１）、さらに仮想口座１１０の残高を更新する（Ｓ１３２２）。ここで、データ処理部９２１は仮想口座１１０の未通知を「無」にする。

続いて、データ処理部９２１は更新した仮想口座１１０の残高を携帯電話番号とともに携帯電話会社１０に送信し（Ｓ１３２３）、決済の完了をインターネット６０を介して仮想店舗２４に通知し（Ｓ１３２４）、さらに仮想店舗２４への支払処理を行なう（Ｓ１３２５）。決済完了の通知は仮想店舗２４を介して利用者１２にも通知される（Ｓ６１２，Ｓ３０７）。利用者１２のパーソナルコンピュータ４０または携帯電話機１３においては、データ処理部４０１または１３１がその受信した決済の完了を表示装置４０６または１３７に表示する（Ｓ３１１）。

一方、携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０から送信された仮想口座残高を受信し（Ｓ５２８）、その残高を送信データ１０２としてメモリ３０３に記憶する（Ｓ５２９）。続いて、データ処理部３０１は個人情報１１の未通知を「無」にし（Ｓ５３０）、メモリ３０３に記憶された送信データ（仮想口座残高）１０２を利用者１２の携帯電話機１３に送信する（Ｓ５３１）。

続いて、データ処理部３０１は上記データの送信が正常に終了したか否かを判定し（Ｓ５３２）、正常に終了した場合はメモリ３０３に記憶された送信データ１０２をクリアし（Ｓ５３３）、正常に終了しなかった場合は再び送信処理を行なう（Ｓ５３４）。

利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された送信データ１０２を受信し（Ｓ１６２）、データ処理部１３１がその受信した送信データ１０２に基づいて仮想口座残高を更新する（Ｓ１６３）。続いて、データ処理部１３１は未通知データをクリアし（Ｓ１６４）、仮想口座残高とともに決済の完了を表示装置１３７に表示する（Ｓ１６５）。

２－４．実在店舗での決済

図５７は、図４４に示した実在店舗での決済に用いられる携帯電話機１３、ＰＯＳ端末２７、携帯電話会社１０のサーバ３０および決済機関９０のサーバ９２

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 434 of 1360

のハードウェア構成を示すブロック図である。ここでは図２０と異なり、決済機関９０のサーバ９２が実在店舗２６のＰＯＳ端末２７および携帯電話会社１０のサーバ３０に接続される。

図５８～図６０は、図５７に示した携帯電話機１３、ＰＯＳ端末２７、携帯電話会社１０のサーバ３０および決済機関９０のサーバ９２の動作を示すフローチャートである。

ここでは、携帯電話会社１０のサーバ３０において、ステップＳ５２５の判定の結果、未通知データがある場合、データ処理部３０１はその未通知データを携帯電話番号とともに決済機関９０に送信する（Ｓ５３５）。決済機関９０のサーバ９２においては、未通知データがある場合、データ処理部９２１は入出金履歴９１２を更新する（Ｓ１３３０）。続いて、データ処理部９２１は決済履歴９１４を更新し、該当する決済の状態を「通知済」とする（Ｓ１３３１）。続いて、データ処理部９２１は未通知データがある場合に仮想口座１１０の残高を更新し、未通知を「無」にする（Ｓ１３３２）。

また、ここでは図２２と異なり、利用者１２の携帯電話機１３において、残高の検証（Ｓ７１８）後に、データ処理部１３１は未通知データに決済内容を記憶し（Ｓ７２２）、その後、携帯電話番号、キーコード、パスワードといった携帯電話機１３の端末情報をＰＯＳ端末２７に送信する（Ｓ７２０）。ステップＳ８０２～Ｓ８０４，Ｓ７２１は図２２と同じである。ステップＳ７２１でＰＯＳ端末２７から決済完了の通知を受信した後、データ処理部１３１は決済モードをオフにし（Ｓ７２３）、決済の終了を表示装置１３７に表示する（Ｓ７３１）。

また、ＰＯＳ端末２７のデータ処理部２７１はステップＳ８０２で受信した携帯電話番号、キーコードおよびパスワードとともに、ステップＳ８０３で記録した決済内容を決済機関９０に送信する（Ｓ８０５）。決済機関９０のサーバ９２においては、データ処理部９２１がＰＯＳ端末２７から携帯電話番号などとともに送信された決済内容を受信し（Ｓ１３３３）、その受信した携帯電話番号に基づいてデータベース９２２に記憶された利用者情報９１０を検索する（Ｓ１３３４）。この検索結果に従って、データ処理部９２１は該当の携帯電話会社１０に認証を依頼するためにステップＳ１３３３で受信した携帯電話番号、キーコード

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 435 of 1360

およびパスワードを携帯電話会社１０に送信する（Ｓ１３３５）。

携帯電話会社１０のサーバ３０においては、図５５と同様にデータ処理部３０１が認証を行なう（Ｓ５１１，Ｓ５１２）。ただしここでは、キーコードまたはパスワードが不一致の場合、データ処理部３０１は個人情報１の利用状況を「利用不可」に変更し（Ｓ５２２）、本サービスの利用停止を利用者１２に通知する（Ｓ５２３）。利用者１２の携帯電話機１３においては、データ処理部１３１は利用状況を「利用不可」に変更する（Ｓ１６０）。

一方、キーコードおよびパスワードが一致した場合、データ処理部３０１は個人情報１１の未通知を「有」に変更し（Ｓ９２５）、認証の成功を決済機関９０に通知し、さらに後述する未通知データの要求処理を行なう（Ｓ９２７）。

決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された認証成功の通知を受信し（Ｓ１３３０）、入出金履歴９１２、決済履歴９１４および仮想口座１１０の残高をそれぞれ更新する（Ｓ１３２０～Ｓ１３２２）。ここでは、決済履歴９１４を更新したときその状態を「未通知」とする。続いて、データ処理部９２１は仮想口座１１０の未通知を「有」に変更する（Ｓ１３３１）。

また、データ処理部９２１が携帯電話会社１０から認証異常の通知を受信した場合も（Ｓ１３１７）、データ処理部９２１は実在店舗２６に対する決済金額の支払処理を行なう（Ｓ１３３２）。このような認証異常が起こる原因として利用者１２の不正が考えられるが、この場合も決済機関９０は実在店舗２６に対して支払を保証することになる。決済機関９０は不正使用による損害を負担することになるが、上記のように認証異常を検出した時点で本サービスの利用を停止しているので損害を最小限に抑えることができる。

２－５．未通知データの要求

図６１は、携帯電話会社１０が利用者１２に対して未通知データを要求する場合における携帯電話機１３、携帯電話会社１０のサーバ３０および決済機関９０のサーバ９２の動作を示すフローチャートである。なお、未通知データは図２４に示した第１の実施の形態と同様に携帯電話機１３のＲＡＭ１３２に記憶されている。また、未通知データの要求の際には図４７に示したハードウェア構成が用

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 436 of 1360

いられる。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が予め定められた時間間隔おきに利用者１２の携帯電話機１３に対して未通知データの送信を要求する（Ｓ５４０）。利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された未通知データの送信要求を受信し（Ｓ１７０）、これに応じてデータ処理部１３１がＲＡＭ１３２に記憶されている未通知データを携帯電話番号、キーコードおよびパスワードとともに携帯電話会社１０に送信する（Ｓ７０６）。以下、図５８および図５９と同様に携帯電話会社１０のサーバ３０は認証などを行ない、決済機関９０のサーバ９２は決済履歴９１４の更新などを行なう。

２－６．請求代行

図６２は、図４６に示した請求代行に用いられるパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、仮想店舗２４のサーバ５０、決済機関９０のサーバ９２、金融機関１７０のサーバ９４のハードウェア構成を示すブロック図である。図６２に示すように、金融機関のサーバ９４は、データ処理部９４１と、データベース９４２とを備える。データ処理部９４１は、インターネット６０と、決済機関９０に設置されているサーバ９２のデータ処理部９２１とに接続される。データベース９４２には、利用者情報９４３、加盟店情報９４４および利用者履歴９４５が蓄積される。利用者情報９４３は、利用者の住所、氏名、電話番号などの他、銀行の場合は口座番号、信販会社の場合はクレジットカード番号および引落銀行口座などである。加盟店情報９４４は、デビットカードやクレジットカードによる決済を受付ける加盟店の住所、名称などである。利用者履歴９４５は、デビットカードやクレジットカードによる決済金額、決済日、利用加盟店の名称などである。

図６３および図６４は、図６２に示したパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、決済機関９０のサーバ９２、金融機関のサーバ９４および仮想店舗２４のサーバ５０の動作を示すフローチャートである。

図６３および図６４に示した請求代行の処理は、図５４～図５６に示した仮想

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 437 of 1360

店舗での決済の処理に類似している。ただし、請求代行の際には利用者１２の携帯電話機１３において、ステップＳ４１８で電子請求書を開封した後直ちに、決済の承認を行なう（Ｓ４０２）。また、ステップＳ１５７でパスワードが一致した場合に、デビットカードによる決済かクレジットカードによる決済かという決済方法の選択を利用者１２に対して促す（Ｓ１７１）。続いて、携帯電話機１３の送受信部１３５は、決済の承認を携帯電話会社１０に通知する（Ｓ４１２）。このとき、携帯電話番号、キーコード、パスワード、決済内容の他、決済方法も合わせて携帯電話会社１０に送信する。

また、携帯電話会社１０のサーバ３０においては、ステップＳ５１１，Ｓ５１２でキーコードおよびパスワードが一致した場合に、データ処理部３０１はステップＳ５１０で受信した決済の承認を携帯電話番号とともに決済機関９０に送信する。決済機関９０のサーバ９２においては、データ処理部９２１がこの決済の承認をインターネット６０を介して仮想店舗２４に通知し（Ｓ１３３５）、仮想店舗２４のサーバ５０においてはモデム５０４がこの通知を受信する（Ｓ６１５）。

続いて、データ処理部９２１は金融機関に決済内容を通知する（Ｓ１３３６）。金融機関のサーバ９４においては、データ処理部９４１が決済機関９０から送信された決済内容を受信し（Ｓ１５００）、所定の決済処理を行なう（Ｓ１５０１）。続いて、データ処理部９４１は決済の可否を仮想店舗２４に通知する（Ｓ１５０２）。仮想店舗２４のサーバ５０においては、モデム５０４が金融機関から送信された決済可否の通知を受信し（Ｓ６１６）、決済が可能か否かを判定し（Ｓ６１７）、決済が不可能な場合は受注の取消を利用者１２のパーソナルコンピュータ４０または携帯電話機１３に送信する（Ｓ６１８）。利用者１２のパーソナルコンピュータ４０または携帯電話機１３においては、モデム４０４または送受信部１３５が仮想店舗２４から送信された受注取消を受信し（Ｓ３１５）、その旨を表示装置４０６または１３７に表示する（Ｓ３１６）。

上記第３の実施の形態は仮想口座１１０を決済機関９０に設けている点で上記第１および第２の実施の形態と大きく相違するが、その他の点でも相違している。これらの相違点は上記第１および第２の実施の形態でも採用することは可能であ

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 438 of 1360

る。

〔第４の実施の形態〕

上記第３の実施の形態では携帯電話会社１０に設けた個人情報１１に基づいて利用者１２の認証を行なっているが、以下に述べる第４の実施の形態では決済機関９０に設けた利用者情報９１０に基づいて利用者１２の認証を行なう。この第４の実施の形態のためのハードウエア構成は、図４７、図４９、図５３、図５７および図６２に示したものと同じであるから、その説明は繰返さない。以下、第４の実施の形態を上記第３の実施の形態との相違点を中心に説明する。

１．前払い方法

まず、仮想口座に入金する前払い方法について説明する。図６５は、この発明の第４の実施の形態に従う前払い方法を示す概略図である。ここでは、携帯電話機１３のＲＡＭ１３２内に、後述するワンタイムＩＤ、小口口座残高および小口決済履歴を記憶するための領域が確保されている。また、決済機関９０の利用者情報９１０には、利用者１２を認証するためのキーコードおよびパスワードが含まれている。利用者情報９１０にはまた、携帯電話機１３のメールアドレス、利用状況および会員区分が含まれている。会員区分には個人利用者の「一般」と「加盟店」とがある。仮想口座１１０には、小口口座残高およびワンタイムＩＤが含まれている。図６６および図６７は、図６５に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

まず、利用者１２は携帯電話機１３を用い、メニュー画面で「前払い」を選択する（Ｓ９８）。具体的には、図４７、図４９、図５３、図５７および図６２に示した携帯電話機１３において、利用者１２の操作に応じて入力装置１３６が「前払い」の選択信号をデータ処理部１３１に与える。以降、ステップＳ９９～Ｓ１０３は図５０に示したものと同じであるから、その説明は繰返さない。

パスワードの検証（Ｓ１０２）後、利用者１２は携帯電話機１３を用い、予め付与されている顧客番号を入力する（Ｓ１７５）。具体的には、利用者１２の操作に応じて入力装置１３６が入力された顧客番号をデータ処理部１３１に与える。ここでは利用者１２が顧客番号を入力しているが、最初に入力された顧客番号を

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 439 of 1360

ＲＡＭ１３２に記憶しておき、２回目以降はこの記憶された顧客番号を送信するようにしてもよい。また、上記実施の形態のように携帯電話機１３の電話番号を顧客番号として用いてもよい。

続いて、携帯電話機１３の送受信部１３５がステップＳ１７５で入力された顧客番号、ＲＯＭ１３３に予め登録されているキーコード、およびステップＳ１０１で入力されたパスワードを携帯電話会社１０に送信する（Ｓ１７６）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された顧客番号、キーコードおよびパスワードを受信し、これらをそのままインターネット６０を介して決済機関９０に送信する。すなわち、携帯電話会社１０は携帯電話機１３から送信された顧客番号、キーコードおよびパスワードを決済機関９０に転送する（Ｓ２６５）。

決済機関９０のサーバ９２においては、携帯電話機１３から携帯電話会社１０を介して送信された顧客番号、キーコードおよびパスワードをデータ処理部９２１が受信する（Ｓ２００）。以降、決済機関９０のサーバ９２は、図５０および図５１に示したステップＳ２０３～Ｓ２０５，Ｓ２５０，Ｓ２５１と同じ処理を携帯電話会社１０のサーバ３０に代わって実行する。但しここでは、決済機関９０のサーバ９２は認証異常通知を携帯電話会社１０に送信し、携帯電話会社１０のサーバ３０はこれを携帯電話機１３に転送する（Ｓ２６６）。また、決済機関９０のサーバ９２は利用不可通知を携帯電話会社１０に送信し、携帯電話会社１０のサーバ３０はこれを携帯電話機１３に転送する（Ｓ２６７）。携帯電話機１３のステップＳ１５０～Ｓ１５２，Ｓ１１０，Ｓ１１１は図５１に示したものと同じであるから、その説明は繰返さない。

利用状況の確認（Ｓ２０４）の結果、利用状況が「利用可」の場合、決済機関９０は利用者１２に対して前払金額の入力を要求する。具体的には、決済機関９０のサーバ９２において、データ処理部９２１が前払金額の要求を携帯電話機１３に送信する（Ｓ１３４０）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された前払金額の要求を利用者１２の携帯電話機１３に転送する（Ｓ２６８）。

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 440 of 1360

携帯電話会社１０を介して送信された前払金額の要求を受信する（Ｓ１７７）。

利用者１２はこの要求に応じて携帯電話機１３の入力装置１３６を操作し、所望の前払金額を入力するとともに前払金額の支払方法を選択する（Ｓ１７８）。この支払方法としては、上記と同様に銀行口座からの引落し、デビット決済、クレジット決済の他、振込み、電子マネーによる決済などがある。携帯電話機１３の送受信部１３５は、この入力された前払金額および選択された支払方法を決済機関９０に送信する。携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された前払金額および支払方法を決済機関９０に転送する（Ｓ２６９）。

決済機関９０のサーバ９２においては、携帯電話機１３から携帯電話会社１０を介して送信された前払金額および支払方法をデータ処理部９２１が受信する（Ｓ１３４１）。

続いて、データ処理部９２１は選択された支払方法で所望の前払金額の決済処理を実行する（Ｓ１３４２）。

続いて、データ処理部９２１は決済が可能か否かを判定する（Ｓ１３４３）。決済が不可能な場合、決済機関９０は利用者１２に前払不可を通知する。具体的には、決済機関９０のサーバ９２において、データ処理部９２１が前払不可の通知を携帯電話機１３に送信する（Ｓ１３４４）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された前払不可の通知を携帯電話機１３に転送する（Ｓ２７０）。

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された前払不可の通知を受信し（Ｓ１７９）、前払不可を表示装置１３７に表示する（Ｓ１８０）。

一方、ステップＳ１３４３で決済が可能な場合、決済機関９０は利用者１２に仮想口座の新しい残高とともに前払完了を通知する。具体的には、データ処理部９２１が仮想口座の残高とともに前払完了の通知を携帯電話機１３に送信する（Ｓ１３４５）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された仮想口座の残高および前払完了の通知を利用者１２の携帯電話機１３に転送する（Ｓ２７１）。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 441 of 1360

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された仮想口座の残高および前払完了の通知を受信し（Ｓ１８１）、データ処理部１３１が仮想口座の残高とともに前払完了を表示装置１３７に表示する（Ｓ１８２）。

前払完了の通知（Ｓ１３４５）後、データ処理部９２１は前払金額に基づいて入出金履歴９１２を更新し（Ｓ１３０６）、さらに仮想口座１１０の残高を更新する（Ｓ１３０８）。

上述したステップＳ２６５～Ｓ２７１に係る通信は同一セッション内で行なわれる。したがって、入出金履歴や仮想口座残高を更新する前に通信が遮断された場合は入出金履歴や仮想口座残高は更新されない。

２．仮想店舗での決済

次に、仮想店舗での決済について説明する。以下に仮想口座から仮想店舗に請求金額を送金する２つの方法を挙げる。

２－１．第１の送金方法

図６８は、この発明の第４の実施の形態に従う第１の送金方法を示す概念図である。ここでは、決済機関９０のサーバ９２に設けられたデータベース９２２に、加盟店請求履歴９１８および加盟店入金履歴９２０が記録される。図６９および図７０は、図６８に示した場合における、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

上記第３の実施の形態と同様に、利用者１２のパーソナルコンピュータ４０または携帯電話機１３は注文内容とともに顧客番号を仮想店舗２４に送信する（Ｓ３０１）。仮想店舗２４のサーバ５０はこれらを受信し（Ｓ６０１）、顧客番号とともに請求内容を決済機関９０に送信する（Ｓ６０２）。

決済機関９０のサーバ９２においては、データ処理部９２１が仮想店舗２４から送信された請求内容を受信する（Ｓ１３１０）。

続いて、決済機関９０のサーバ９２は、図５４に示したステップＳ５０２，Ｓ５０３，Ｓ５０５と同じ処理を携帯電話会社１０のサーバ３０に代わって実行する。但しここでは、携帯電話番号の代わりに顧客番号に基づいて決済機関９０の

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 442 of 1360

サーバ９２がデータベース９２２中の利用者情報９１０を検索する（Ｓ５０２）。

利用状況の確認（Ｓ５０３）の結果、利用状況が「利用可」の場合、決済機関９０のサーバ９２においては、データ処理部９２１が顧客番号に基づいてデータベース９２２を検索し、利用者情報９１０の中から携帯電話機１３の電子メールアドレスを読出し、その電子メールアドレスに従って電子請求書を電子メールで携帯電話機１３に送信する（Ｓ５０５）。この電子請求書には、請求番号、請求金額、送金先（加盟店番号）などが記録されている。

続いて、データ処理部９２１は加盟店請求履歴９１８を更新し、仮想店舗２４から送信された電子請求書に基づいて、請求番号、請求日、請求金額などを記録する（Ｓ１３４０）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された電子メールを利用者１２の携帯電話機１３に転送する（Ｓ２７２）。

携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された電子メールを受信し（Ｓ４０１）、データ処理部１３１が利用者１２の操作に応じて電子メールを開封し、電子請求書を表示装置１３７に表示する（Ｓ４１８）。

続いて、利用者１２が電子請求書を確認し、そこに記録されている請求金額を仮想店舗２４に送金する場合は「送金」を選択する。このとき、利用者１２は入力装置１３６を操作して顧客番号およびパスワードも入力する。これにより携帯電話機１３は電子メールに埋込まれている送金ＵＲＬ(Uniform Resource Locator)に従って決済機関９０のサーバ９２に接続され、送受信部１３５がキーコード、顧客番号およびパスワードとともに送金選択信号を決済機関９０に送信する（Ｓ４３０）。携帯電話会社１０のサーバ３０は、携帯電話機１３から送信された送金選択信号をインターネット６０を介して決済機関９０に転送する（Ｓ２７３）。

決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話機１３から携帯電話会社１０を介して送信されたキーコード、顧客番号、パスワードおよび送金選択信号を受信し（Ｓ１３４１）、その受信した顧客番号に基づいてデ

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 443 of 1360

ータベース９２２中の利用者情報９１０を検索する（Ｓ１３４２）。以降、決済機関９０のサーバ９２は図５５に示したステップＳ５１１，Ｓ５１２，Ｓ５２２～Ｓ５２４と同じ処理を携帯電話会社１０のサーバ３０に代わって実行する。

データ処理部９２１がキーコードおよびパスワードを検証し（Ｓ５１１，Ｓ５１２）、両方共一致した場合は仮想口座１１０の新しい残高とともに送金完了の通知を携帯電話会社１０を介して利用者１２の携帯電話機１３に送信する（Ｓ１３４３）。携帯電話会社１０のサーバ３０は、決済機関９０からインターネット６０を介して送信された送金完了の通知を利用者１２の携帯電話機１３に転送する（Ｓ２７５）。携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された送金完了通知を受信し（Ｓ４３１）、さらにデータ処理部１３１が送金後の仮想口座残高とともに送金完了を表示装置１３７に表示する（Ｓ４３２）。

送金完了の通知（Ｓ１３４３）後、決済機関９０のサーバ９２は図５６に示したステップＳ１３２０～Ｓ１３２２と同じ処理を実行する。

仮想口座残高の更新（Ｓ１３２２）後、データ処理部９２１はデータベース９２２中の加盟店請求履歴９１８を更新し、入金日を記録する（Ｓ１３４４）。

続いて、データ処理部９２１はデータベース９２２中の加盟店入金履歴９２０を更新し、請求番号、入金日、入金額、送金顧客番号などを記録する（Ｓ１３４５）。

続いて、データ処理部９２１は入金通知をインターネット６０を介して仮想店舗２４に送信する（Ｓ１３４６）。仮想店舗２４のサーバ５０においては、モデム５０４が決済機関９０から送信された入金通知を受信する（Ｓ６１９）。

ここでは、ステップＳ２７２～Ｓ２７５に係る通信は同一セッション内で行なわれる。

２－２．第２の送金方法

図７１は、この発明の第４の実施の形態に従う第２の送金方法を示す概念図である。図７２および図７３は、図７１に示した場合における、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 444 of 1360

注文を受けた仮想店舗２４は、上記第１の送金方法のように支払内容を決済機関９０を介して利用者１２に通知するのではなく、ここでは支払内容を利用者１２に直接通知する。具体的には、仮想店舗２４のサーバ５０においては、注文の受信（Ｓ６０１）後、データ処理部５０１は仮想店舗２４の加盟店番号と請求金額などの請求内容をインターネット６０を介して利用者１２の携帯電話機１３またはパーソナルコンピュータ４０に送信する（Ｓ６２０）。利用者１２の携帯電話機１３またはパーソナルコンピュータ４０においては、送受信部１３５またはモデム４０４がこれらを受信する（Ｓ３１２）。

利用者１２は通知された請求内容を見て携帯電話機１３を操作し、メニュー画面から「送金」を選択する（Ｓ９７）。図６６に示したステップＳ９９～１０３，Ｓ１７５，Ｓ１７６，Ｓ２６５，Ｓ２００と同様に、利用者１２はパスワードおよび顧客番号を入力し、携帯電話機１３はこれらをキーコードとともに決済機関９０に送信し、決済機関１２はこれらを受信する。

続いて、図６９に示したステップＳ５０２，Ｓ５０３，Ｓ１３１４，Ｓ６０３，Ｓ６０４，Ｓ３０２，Ｓ３０３，Ｓ５１１，Ｓ５１２，Ｓ５２２～Ｓ５２４，Ｓ２７４，Ｓ１５９，Ｓ６１３と同様に、決済機関９０は認証を行ない、ステップＳ５１１，Ｓ５１２でキーコードおよびパスワードの両方が一致した場合、具体的な送金内容を入力するよう利用者１２に要求する。利用者１２はこの要求に応じて具体的な送金内容を入力して決済機関９０に送信する。

具体的には、決済機関９０のサーバ９２においては、データ処理部９２１が送金内容の要求を利用者１２の携帯電話機１３に送信する（Ｓ１３４７）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された送金内容の要求を携帯電話機１３に転送する（Ｓ２７６）。

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された送金内容の要求を受信する（Ｓ４３３）。

続いて、入力装置１３６は利用者１２の操作に応じて入力された送金内容をデータ処理部１３１に与え、送受信部１３５はその入力された送金内容を決済機関９０に送信する（Ｓ４３４）。送金内容としては、送金先の加盟店番号、送金金

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 445 of 1360

額などがある。携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された送金内容を決済機関９０に転送する（Ｓ２７７）。決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話機１３から携帯電話会社１０を介して送信された送金内容を受信する（Ｓ１３４８）。以降は、図７０に示したステップＳ１３４３，Ｓ２７５，Ｓ４３１，Ｓ４３２，Ｓ１３２０～Ｓ１３２２；Ｓ１３４５，Ｓ１３４６，Ｓ６１９と同じであるから、その説明は繰返さない。ただしここでは、図６８に示した請求履歴９１８はないので請求履歴の更新（Ｓ１３４４）は行なわれない。

３．実在店舗での決済

次に、実在店舗での決済について説明する。ここでは、仮想口座からの振替えが可能な小口口座をさらに設け、その小口口座の使用を可能にするワンタイムＩＤ（識別子）を発行する。

３－１．ワンタイムＩＤの発行（小口口座への振替え）

図７４および図７５は、この発明の第４の実施の形態に従ってワンタイムＩＤの発行方法を示す概念図である。図７４は小口決済履歴がない場合を示し、図７５は小口決済履歴がある場合を示す。ここでは、決済機関９０のサーバ９２に設けられたデータベース９２２に、小口口座の入出金履歴９１５が記録される。図７６および図７７は、図７４および図７５に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

実在店舗で決済をするために仮想口座から小口口座に所望の金額を振替えようとする場合、利用者１２は携帯電話機１３を操作し、メニュー画面で「ワンタイムＩＤ」を選択する（Ｓ９６）。具体的には、携帯電話機１３において、入力装置１３６が利用者１２の操作に応じて「ワンタイムＩＤ」の選択信号をデータ処理部１３１に与える。以降、ステップＳ９９～Ｓ１０３，Ｓ１７５は図６６に示したものと同じであるから、その説明は繰返さない。

顧客番号の入力（Ｓ１７５）後、携帯電話機１３においては、送受信部１３５が顧客番号、キーコード、パスワードおよび小口口座情報を決済機関９０に送信する（Ｓ１８５）。小口口座情報には、ＲＡＭ１３２に記録されている小口口座

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 446 of 1360

残高および小口決済履歴が含まれる。但し、初めてワンタイムＩＤを要求する場合、小口決済履歴はまだ存在していない。以降、ステップＳ２６５～Ｓ２６７，Ｓ２００，Ｓ２０２～Ｓ２０５，Ｓ２５０，Ｓ２５１，Ｓ１５０～Ｓ１５２，Ｓ１１０，Ｓ１１１は図６６に示したものと同じであるから、その説明は繰返さない。

利用者１２の認証（Ｓ２０３）の結果、キーコードおよびパスワードが共に一致し、かつ利用状況の確認（Ｓ２０４）の結果、利用状況が「利用可」の場合、決済機関９０は利用者１２に対して仮想口座から小口口座への振替金額を要求する。具体的には、決済機関９０のサーバ９２において、データ処理部９２１が小口口座への希望振替金額の要求を利用者１２の携帯電話機１３に送信する（Ｓ１３５０）。このとき、振替可能な限度額（通常は仮想口座の残高）も併せて送信する。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された振替金額の要求を携帯電話機１３に転送する（Ｓ２７８）。

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された振替金額の要求を受信する（Ｓ１８６）。

この要求に応じ、利用者１２は携帯電話機１３の入力装置１３６を操作して所望の振替金額を指定する（Ｓ１８７）。入力装置１３６は利用者１２により指定された振替金額をデータ処理部１３１に与える。

データ処理部１３１はステップＳ１８７で指定された決済金額をステップＳ１８６で受信した限度額と比較し、指定された決済金額が限度額以内か否かを判定する（Ｓ１８８）。指定された振替金額が限度額を超えている場合、データ処理部１３１は振替不可を表示装置１３７に表示する（Ｓ１８９）。一方、指定された振替金額が限度額以内の場合、送受信部１３５はその指定された振替金額を決済機関９０に送信する（Ｓ１９０）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が利用者１２の携帯電話機１３から送信された振替金額をインターネット６０を介して決済機関９０に転送する（Ｓ２７９）。

決済機関９０のサーバ９２においては、データ処理部９２１が利用者１２の携帯電話機１３から携帯電話会社１０を介して送信された振替金額を受信し（Ｓ１

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 447 of 1360

３５１）、さらにランダムにワンタイムＩＤを生成する（Ｓ１３５２）。

続いて、データ処理部９２１はステップＳ１３５１で受信した振替金額に基づいて、仮想口座の入出金履歴９１２を更新し（Ｓ１３２０）、仮想口座の決済履歴９１４を更新し（Ｓ１３２１）、仮想口座１１０の残高を更新し（Ｓ１３２２）、さらに小口口座の入出金履歴９１５を更新する（Ｓ１３４５）。

たとえば図７４に示すように利用者１２が振替金額を１０００円に指定した場合、仮想口座の入出金履歴９１２には１０００円が小口口座に出金された旨が記録される。また、仮想口座１１０の残高は１０００円減額され、小口口座の残高は１０００円増額される。さらに、小口口座の入出力履歴９１５には１０００円が入金された旨が記録される。この場合、小口決済履歴は携帯電話機１３から送信されて来ないので、仮想口座の決済履歴９１４は更新されない。

次に、図７５に示すように携帯電話機１３の小口決済履歴に３００円を使用した旨が記録されている（つまり携帯電話機１３の小口口座残高が７００円になっている）場合において利用者１２が振替金額を１５００円に指定したときは、この振替金額（１５００円）と現在の小口口座残高（７００円）との差額（８００円）が計算され、仮想口座の入出力履歴９１２には８００円が出金された旨が記録される。また、携帯電話機１３の小口決済履歴に基づいて仮想口座の決済履歴９１４には３００円が決済に使用された旨が記録される。また、上記差額に基づいて仮想口座１１０の残高は８００円減額され、２００円になる。小口口座から３００円が決済に使用されたが、新たに８００円が小口口座に振替えられるので、小口口座の残高は上記振替金額に等しい１５００円になる。また、小口口座の入出金履歴９１５には携帯電話機１３の小口決済履歴に基づいて３００円が出金された旨が記録され、さらに上記差額に基づいて８００円が入金された旨が記録される。

最後に、データ処理部９２１はステップＳ１３５２で生成したワンタイムＩＤや小口口座残高などの振替内容を利用者１２の携帯電話機１３に送信する（Ｓ１３５３）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された振替内容を携帯電話機１３に転送する（Ｓ２８０）。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 448 of 1360

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された振替内容を受信する（Ｓ１１９）。

続いて、データ処理部１３１はＲＡＭ１３２に記録されている小口決済履歴をクリアする（Ｓ１９２）。続いて、データ処理部１３１は、ＲＡＭ１３２に記録されている小口口座残高を書替え（Ｓ１９３）、さらにＲＡＭ１３２に記録されているワンタイムＩＤを書替える（Ｓ１９４）。

たとえば図７４に示した場合、決済機関９０で生成された「９８７６５」のワンタイムＩＤが携帯電話機１３のＲＡＭ１３２に記録される。また、利用者１２が指定した振替金額に従って小口口座残高が「０円」から「１０００円」に更新される。また、図７５に示した場合、決済機関９０で生成された「３４５６７」の新しいワンタイムＩＤが携帯電話機１３のＲＡＭ１３２に記録される。また、決済機関９０で計算された「１５００円」の新しい小口口座残高が携帯電話機１３のＲＡＭ１３２に記録される。

最後に、データ処理部１３１は小口口座残高とともに小口口座への入金完了を表示装置１３７に表示する（Ｓ１９５）。

３－２．ワンタイムＩＤの使用（小口口座からの支払い）

図７８は、この発明の第４の実施の形態に従い、ワンタイムＩＤを使用して実在店舗で決済する方法を示す概念図である。図７９は、図７８に示した場合における、携帯電話機、実在店舗のＰＯＳ端末、および決済機関のサーバの動作を示すフローチャートである。

小口口座に所望の金額を振替えてワンタイムＩＤを獲得した後、実在店舗２６で決済を行なう場合、利用者１２は携帯電話機１３を操作し、メニュー画面で「支払い」を選択する（Ｓ９５）。具体的には、携帯電話機１３において、入力装置１３６が利用者１２の操作に応じて「支払い」の選択信号をデータ処理部１３１に与える。以降、ステップＳ９９～Ｓ１０３は図６６に示したものと同じであるから、その説明は繰返さない。

パスワードの検証（Ｓ１０２）後、データ処理部１３１はＲＡＭ１３２に記録されているワンタイムＩＤが有効か否かを判定する（Ｓ７３５）。ワンタイムＩＤには有効日が付与されており、小口口座の残高はその有効日までしか実在店舗

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 449 of 1360

での決済に使用することができない。ワンタイムＩＤは実在店舗での決済に１回使用すれば無効になるようにしてもよい。

ワンタイムＩＤが無効な場合、データ処理部１３１はその旨を表示装置１３７に表示する（Ｓ７３６）。一方、ワンタイムＩＤが有効な場合、データ処理部１３１は小口口座からの支払いが可能である旨を表示装置１３７に表示する（Ｓ７３７）。以降、ステップＳ７１６～Ｓ７１９，Ｓ８０１は図５９に示したものと同じであるから、その説明は繰返さない。

残高検証（Ｓ７１８）の結果、ＰＯＳ端末２７から送信された決済金額が小口口座の残高以内の場合、携帯電話機１３のインターフェイス部１３９はＰＯＳ端末２７にＲＡＭ１３２に記録されているワンタイムＩＤを送信する（Ｓ７３８）。

続いて、データ処理部１３１はＲＡＭ１３２に記録されている小口決済履歴を更新する（Ｓ７３９）。具体的には、データ処理部１３１は、ＰＯＳ端末２７から送信された決済金額、決済日、実在店舗２６の加盟店番号などを記憶する。

続いて、データ処理部１３１はＲＡＭ１３２に記録されている小口口座の残高を更新する（Ｓ７４０）。具体的には、データ処理部１３１は、小口口座の残高から決済金額を減算して新しい残高を記録する。この時点で、携帯電話機１３の小口口座の残高は決済機関９０の小口口座の残高とずれる。

最後に、データ処理部１３１は小口口座の新しい残高とともに決済の完了を表示装置１３７に表示する（Ｓ７４１）。

実在店舗２６のＰＯＳ端末２７においては、インターフェイス部２７６が携帯電話機１３から送信されたワンタイムＩＤを受信する（Ｓ８１０）。

続いて、データ処理部２７１はその決済金額に基づいて売上計上処理を実行する（Ｓ８１１）。

続いて、インターフェイス部２７６は、加盟店番号とともにワンタイムＩＤ、決済日、決済金額、顧客番号などの決済内容を決済機関９０に送信する（Ｓ８０５）。

決済機関９０のサーバ９２においては、データ処理部９２１がＰＯＳ端末２７から送信された決済内容を受信し（Ｓ１３３３）、その受信した決済内容に基づいて加盟店の入金履歴９２０を更新する（Ｓ１３５５）。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 450 of 1360

続いて、データ処理部９２１はその支払を承認した旨の通知を実在店舗２６に送信する（Ｓ１３２４）。実在店舗２６のＰＯＳ端末２７は、決済機関９０から送信された支払承認の通知を受信する（Ｓ８０６）。

最後に、データ処理部９２１はたとえば月末に１ヶ月間の総支払金額を計算し、実在店舗２６に対する支払処理を実行する（Ｓ１３２５）。

上述した第４の実施の形態では、携帯電話会社１０のサーバ３０が携帯電話機１３から送信されたキーコードをそのまま決済機関９０のサーバ９２に転送しているが、携帯電話機１３から送信されたキーコードをこれと１対１に対応する別のキーコードに変換して決済機関９０のサーバ９２に送信するようにしてもよい。

また、小口口座への振替えの際にワンタイムＩＤをダウンロードするようにしているが、利用者１２が携帯電話機１３で決済機関９０が提供するサービスサイトにアクセスする度に自動的に新しいワンタイムＩＤをダウンロードするようにしてもよい。この場合、ワンタイムＩＤの更新頻度が増すため、セキュリティがさらに高くなる。

また、ワンタイムＩＤを１次元または２次元バーコードのイメージとし、実在店舗での決済の際には携帯電話機１３に表示されたバーコードをＰＯＳ端末２７のリーダで光学的に読取るようにしてもよい。この場合、携帯電話機１３から情報を読取るための専用機器をＰＯＳ端末２７に取付ける必要はなく、既存のバーコードリーダを用いればよい。また、小口口座の残高をワンタイムＩＤのバーコードに付加してもよい。

この発明の第４の実施の形態によれば、決済機関９０が携帯電話機１３から出力されるキーコードを取得し、利用者１２の認証を行なっているため、認証を携帯電話会社１０に依存することはない。そのため、決済会社９０だけで本サービスを提供することができる。

また、仮想口座とは別に小口口座を設け、実在店舗で決済する際には予め仮想口座から小口口座に振替えを行なっておき、小口口座から代金を支払うようにしているため、上記第１～第２の実施の形態のように仮想口座の残高が真の残高からずれることはない。また、決済機関が小口口座からの出金を可能にするためのワンタイムＩＤを発行し、ワンタイムＩＤが有効でかつ決済金額が小口口座の残

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 451 of 1360

高以内の場合だけ携帯電話機１３からＰＯＳ端末２７にワンタイムＩＤが出力され、ＰＯＳ端末２７はこのワンタイムＩＤに基づいて決済を完了するようにしているため、セキュリティが高くなる。

上記各コンピュータには所定のプログラムがインストールされている。この各プログラムは、フローチャートで示した各列に並ぶ一連のステップを対応のコンピュータに実行させるためのものである。各プログラムはＣＤ－ＲＯＭのようなコンピュータ読取可能な媒体に記録して配布可能である。

今回開示された実施の形態はすべての点で例示であって制限的なものではないと解釈されるものである。本発明の範囲は上述した実施の形態ではなく特許請求の範囲によって定められ、特許請求の範囲と均等の意味およびその範囲内でのすべての変更が含まれることを意図するものである。

産業上の利用可能性

この発明は、携帯電話機を用いた決済サービスに適用可能である。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 452 of 1360

請求の範囲

1．売り主と携帯電話機の利用者たる買い主との間の決済を仲介する方法であって、前記利用者の金銭を蓄積するための第１の口座を有するコンピュータにおいて、

前記携帯電話機から送信された所望の金額を受信するステップと、

前記受信した所望の金額を前記利用者の第１の口座に入金してその口座の残高を更新するステップと、

前記更新した第１の口座の残高を前記携帯電話機に送信するステップと、

決済金額を受信するステップと、

前記受信した決済金額を前記第１の口座の残高から減じるステップと、

前記受信した決済金額を前記売り主に支払うステップとを含む、方法。

2．前記受信した所望の金額を前記利用者に対して課金するステップをさらに含む、請求項１に記載の方法。

3．前記携帯電話機から送信された識別情報を受信するステップと、

前記受信した識別情報に基づいて前記利用者の認証を行なうステップとをさらに含む、請求項１に記載の方法。

4．前記識別情報は前記利用者に固有の利用者固有情報を含む、請求項３に記載の方法。

5．前記利用者固有情報は前記携帯電話機の電話番号を含む、請求項４に記載の方法。

6．前記利用者固有情報はパスワードをさらに含む、請求項５に記載の方法。

7．前記利用者固有情報は前記利用者に予め付与された利用者識別子を含む、請求項４に記載の方法。

8．前記利用者固有情報はパスワードをさらに含む、請求項７に記載の方法。

9．前記識別情報は前記携帯電話機に固有の電話機固有情報をさらに含む、請求項４に記載の方法。

１０．前記電話機固有情報は前記携帯電話機の製造番号を含む、請求項９に記載の方法。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 453 of 1360

１１．前記電話機固有情報は前記携帯電話機のサブスクライバ識別子を含む、請求項９に記載の方法。

１２．前記サブスクライバ識別子は携帯電話局を介して送信される、請求項１１に記載の方法。

１３．前記コンピュータは第２の口座をさらに有し、

前記携帯電話機から送信された振替金額を受信するステップと、

前記受信した振替金額を前記第１の口座から前記第２の口座に振替えるステップと、

前記第２の口座の残高を使用可能にするためのワンタイム識別子を生成して前記携帯電話機に送信するステップとをさらに含む、請求項１に記載の方法。

１４．前記コンピュータは携帯電話会社に設けられる、請求項１に記載の方法。

１５．前記コンピュータは決済機関に設けられる、請求項１に記載の方法。

１６．前記コンピュータは金融機関に設けられる、請求項１に記載の方法。

１７．売り主と携帯電話機の利用者たる買い主との間の決済を仲介する方法であって、前記利用者の金銭を蓄積するための口座を有する金融機関のコンピュータにおいて、

携帯電話局のコンピュータから決済金額を受信するステップと、

前記受信した決済金額を前記口座の残高から減じるステップと、

前記受信した決済金額を前記売り主に支払うステップとを含む、方法。

１８．前記携帯電話機から送信された金額を前記携帯電話局のコンピュータを介して受信するステップと、

前記受信した金額を前記利用者の口座に振替えてその口座の残高を更新するステップと、

前記更新した口座の残高を前記携帯電話局のコンピュータを介して前記携帯電話機に送信するステップとをさらに含む、請求項１７に記載の方法。

１９．売り主と携帯電話機の利用者たる買い主との間の決済に用いられ、前記利用者の金銭を蓄積するための第１の口座を有するコンピュータにアクセス可能な携帯電話機であって、

前記利用者の操作に応じて前記第１の口座に入金されるべき所望の金額を入力

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 454 of 1360

する入力手段と、

前記入力された金額を前記コンピュータに送信し、前記コンピュータから送信された前記第１の口座の残高を受信する送受信手段と、

前記受信した第１の口座の残高を記憶する手段とを備える、携帯電話機。

２０．前記送受信手段はさらに前記利用者の認証に必要な識別情報を前記コンピュータに送信する、請求項１９に記載の携帯電話機。

２１．前記識別情報は前記利用者に固有の利用者固有情報を含む、請求項２０に記載の携帯電話機。

２２．前記利用者固有情報を記憶する手段をさらに備える、請求項２１に記載の携帯電話機。

２３．前記利用者固有情報は前記携帯電話機の電話番号を含む、請求項２１に記載の携帯電話機。

２４．前記利用者固有情報はパスワードをさらに含む、請求項２３に記載の携帯電話機。

２５．前記利用者固有情報は前記利用者に予め付与された利用者識別子を含む、請求項２１に記載の携帯電話機。

２６．前記利用者固有情報はパスワードをさらに含む、請求項２５に記載の携帯電話機。

２７．前記識別情報は前記携帯電話機に固有の電話機固有情報をさらに含む、請求項２１に記載の携帯電話機。

２８．前記電話機固有情報を記憶する手段をさらに備える、請求項２７に記載の携帯電話機。

２９．前記電話機固有情報は携帯電話機の製造番号を含む、請求項２８に記載の携帯電話機。

３０．前記電話機固有情報は前記携帯電話機のサブスクライバ識別子を含む、請求項２８に記載の携帯電話機。

３１．前記送受信手段はさらに決済金額を受信し、

前記送受信手段により受信された決済金額を記憶する手段をさらに備え、

前記送受信手段はさらに前記記憶された決済金額を読出して前記コンピュータ

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 455 of 1360

に送信する、請求項１９に記載の携帯電話機。

３２．前記記憶された第１の口座の残高から前記記憶された決済金額を減算する手段をさらに備える、請求項３１に記載の携帯電話機。

３３．前記コンピュータは第２の口座をさらに有し、

前記入力手段は前記利用者の操作に応じて前記第１の口座から前記第２の口座に振替えられるべき振替金額を入力し、

前記送受信手段はさらに前記入力された振替金額を前記コンピュータに送信し、

前記送受信手段はさらに前記第２の口座の残高を使用可能にするためのワンタイム識別子を受信し、

前記ワンタイム識別子が有効か否かを判定する手段と、

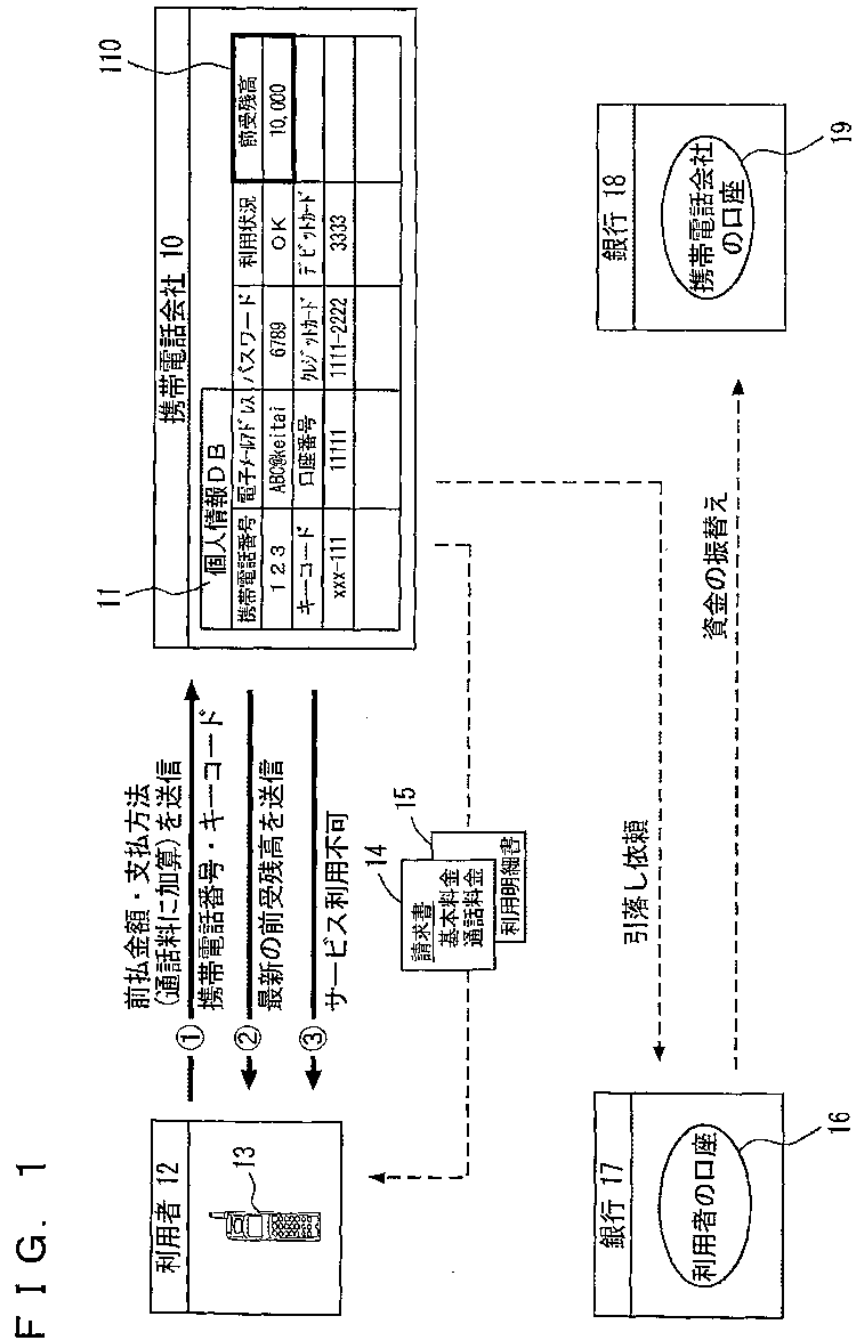
前記ワンタイム識別子の判定の結果、前記ワンタイム識別子が有効な場合、前記送受信手段により受信された決済金額が前記第２の口座の残高以内か否かを判定する手段と、

前記決済金額の判定の結果、前記決済金額が前記第２の口座の残高以内の場合、前記受信したワンタイム識別子を出力する手段と、

前記決済金額を前記第２の口座から減じる手段とをさらに備える、請求項３１記載の携帯電話機。

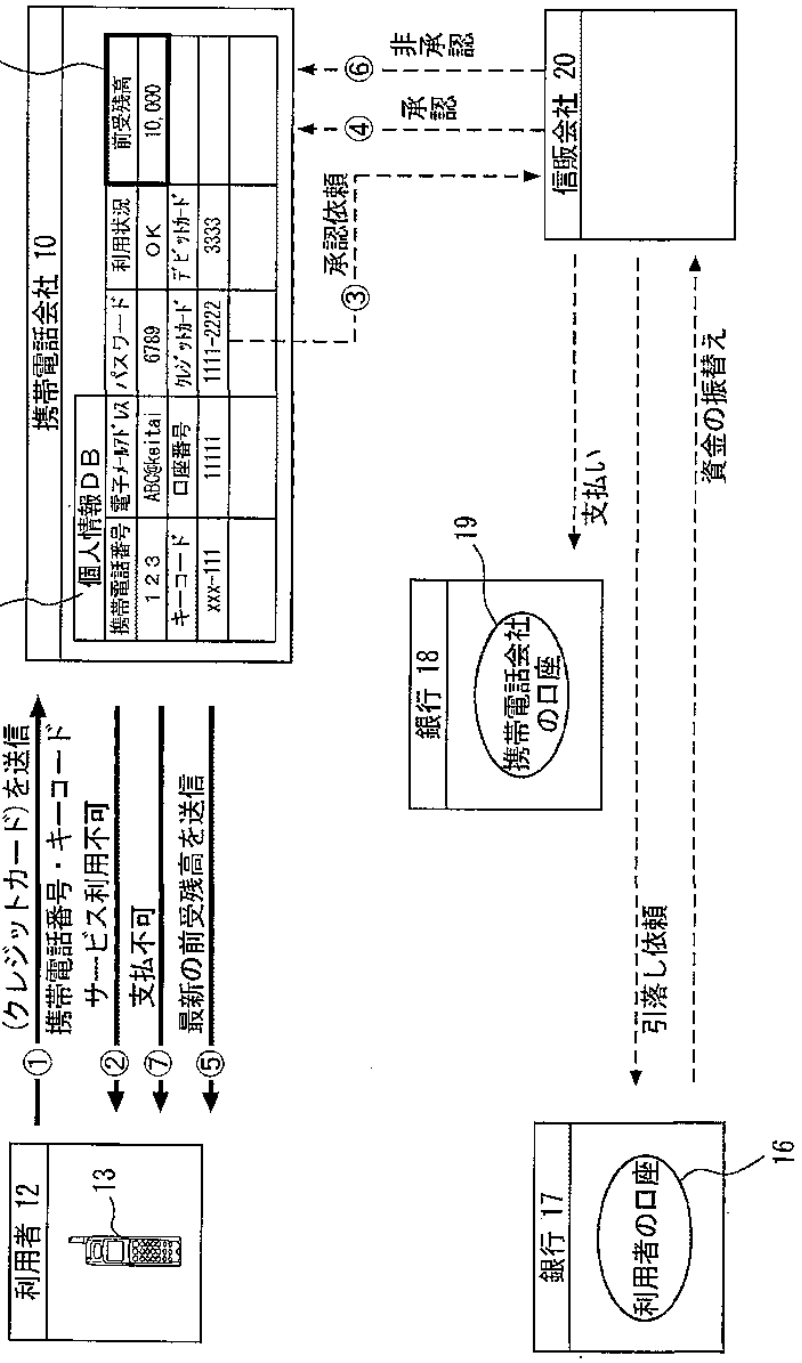
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 456 of 1360

FIG. 1



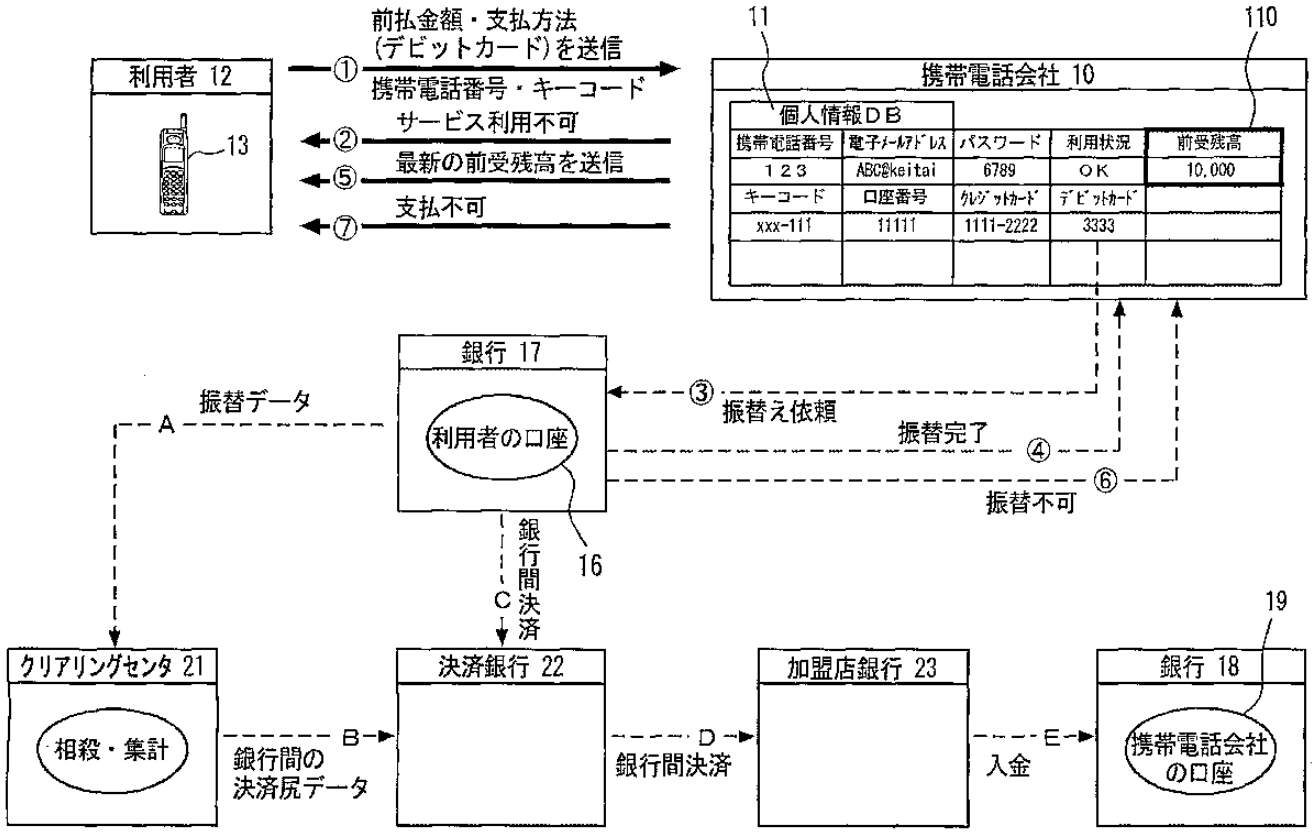
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 457 of 1360

FIG. 2



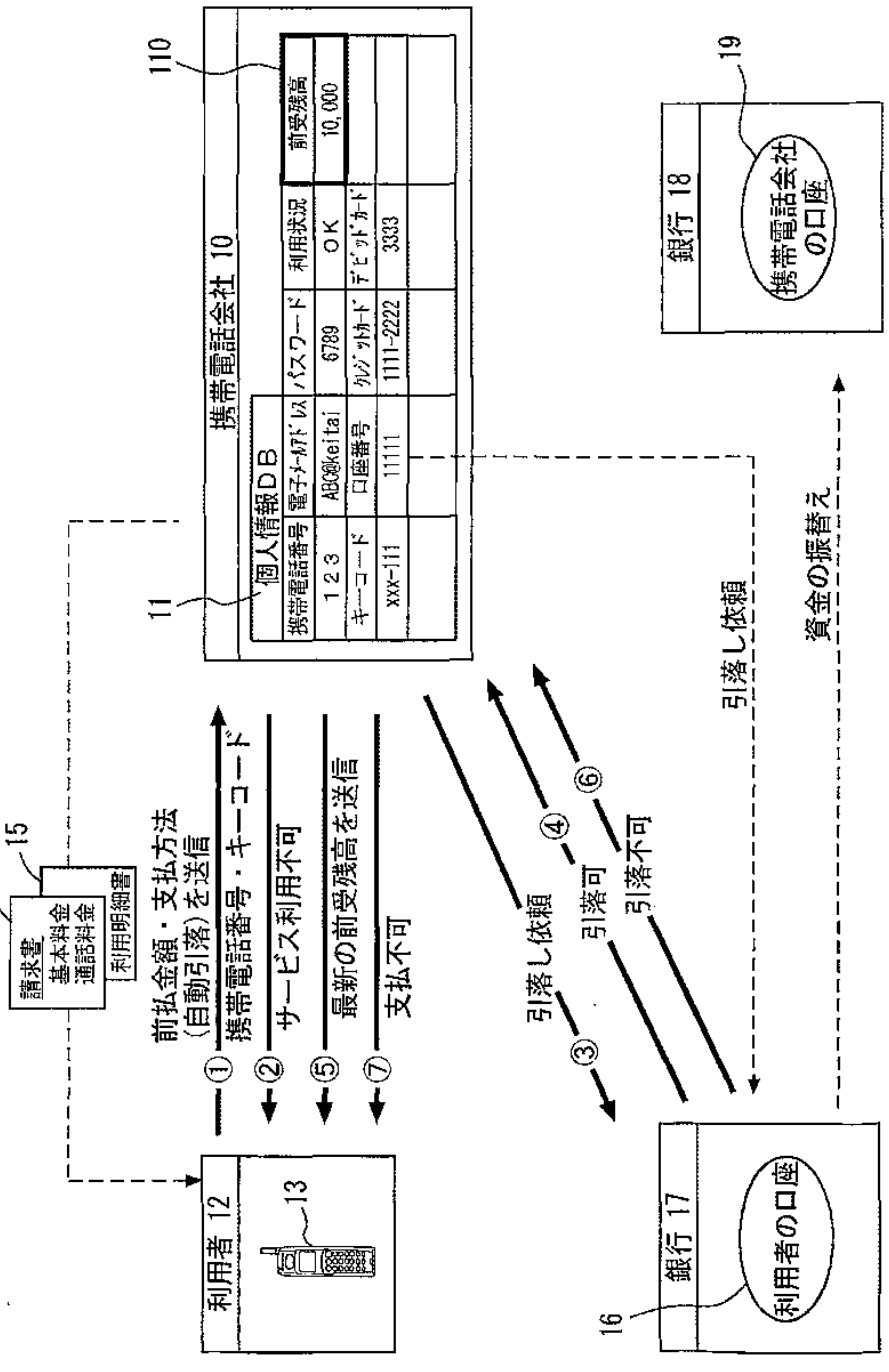
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 458 of 1360

FIG. 3



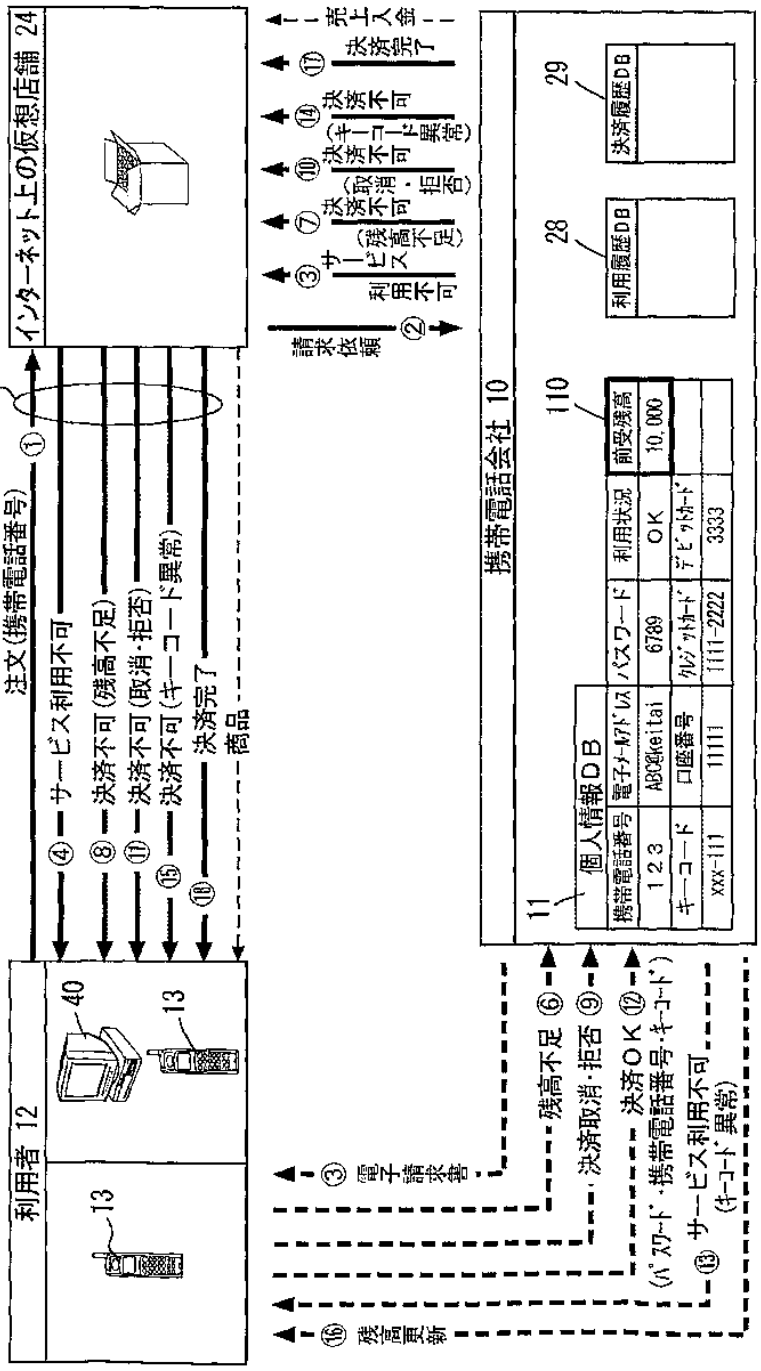
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 459 of 1360

FIG. 4



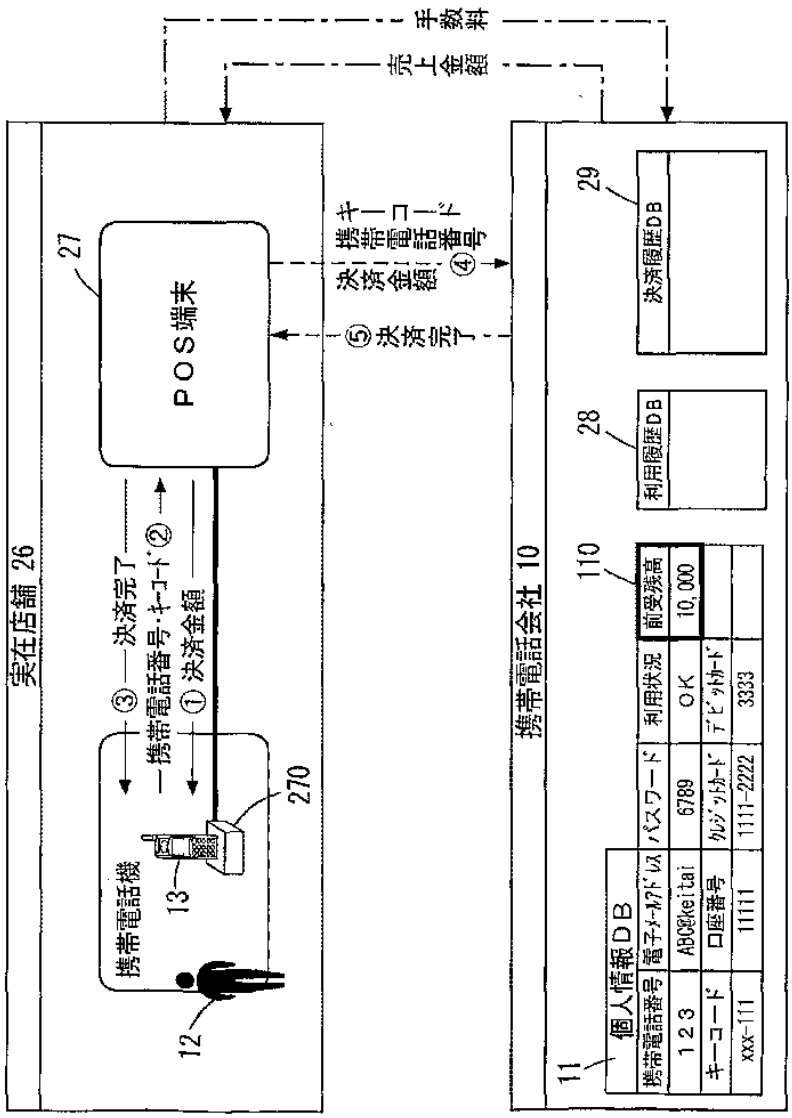
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 460 of 1360

FIG. 5



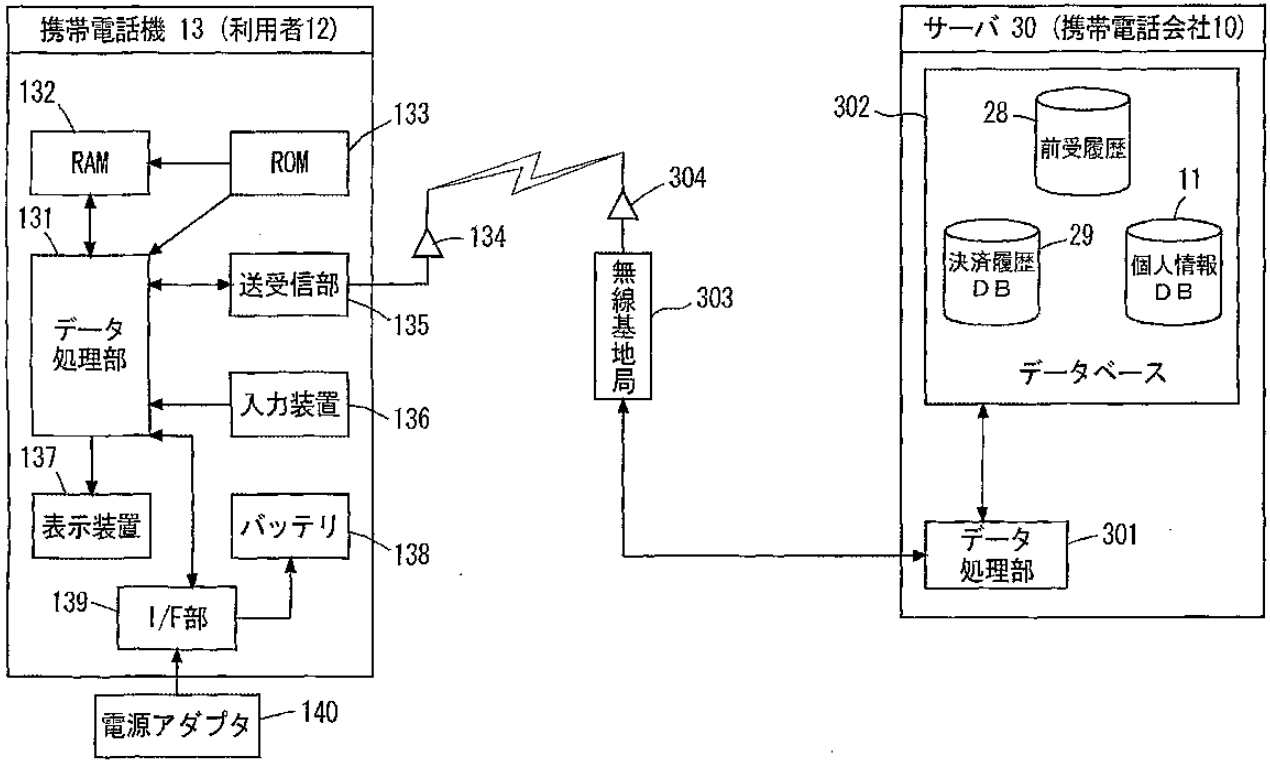
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 461 of 1360

FIG. 6



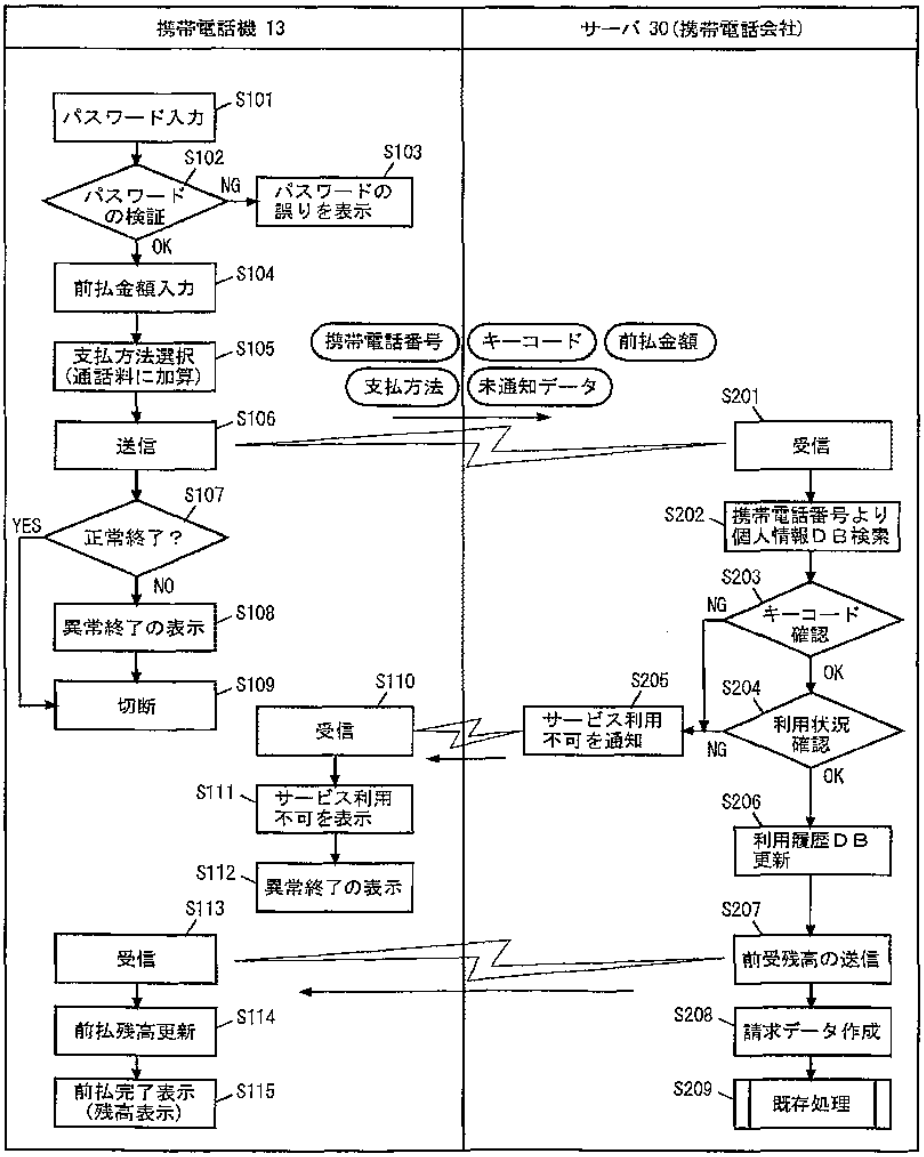
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 462 of 1360

FIG. 7



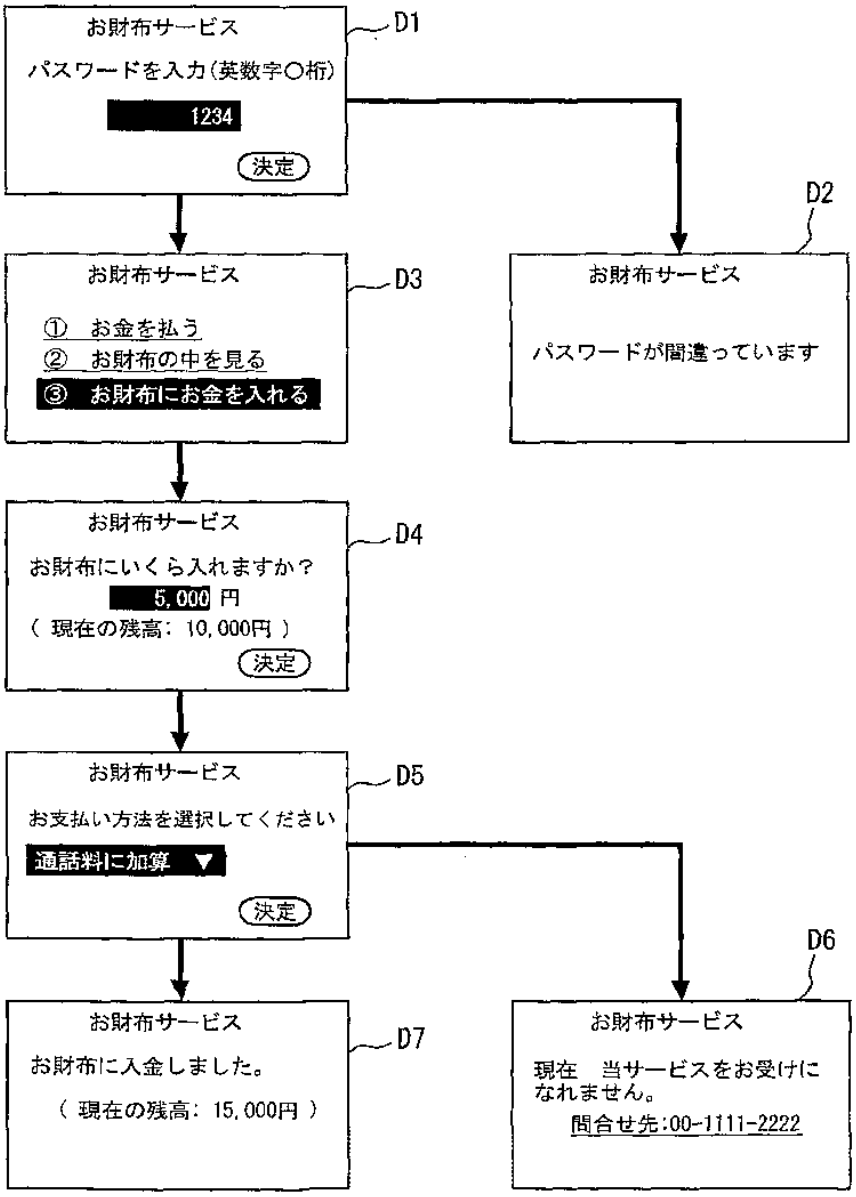
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 463 of 1360

FIG. 8



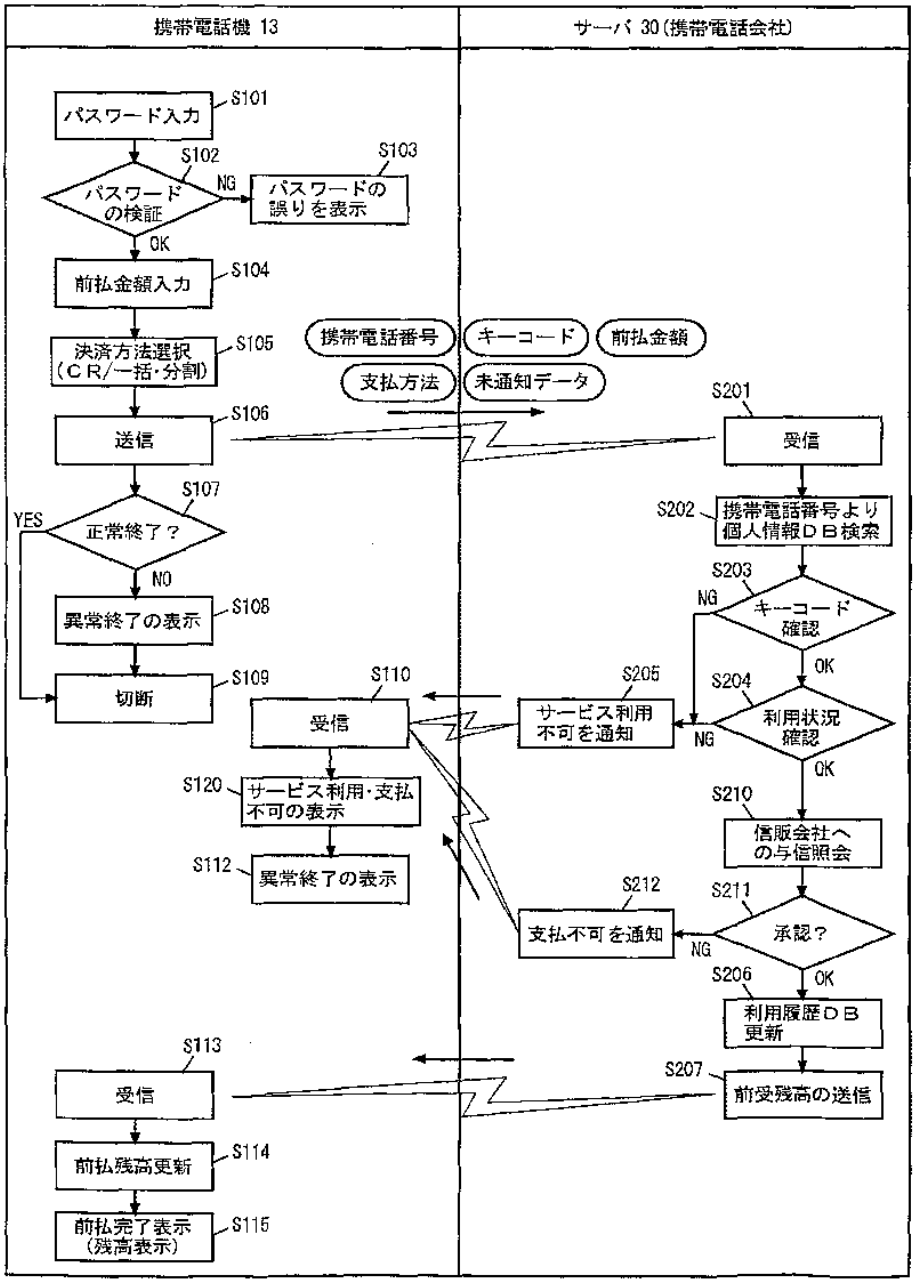
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 464 of 1360

FIG. 9



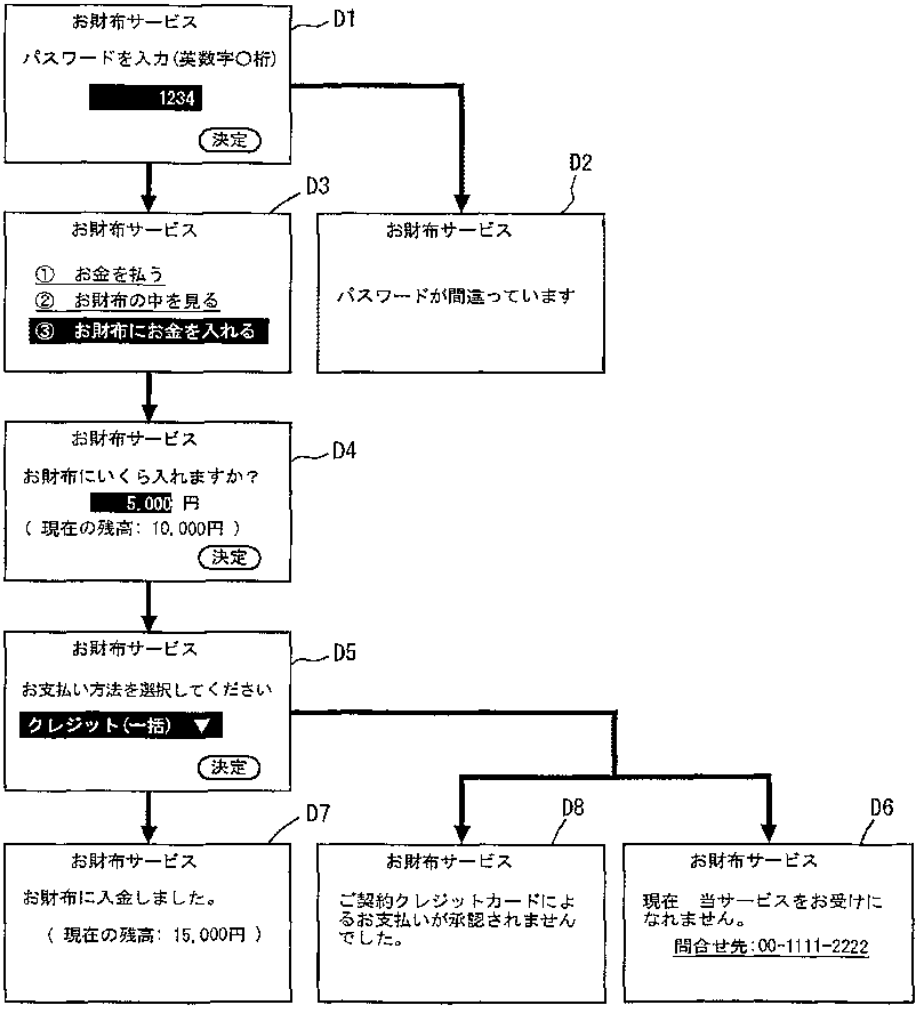
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 465 of 1360

FIG. 10



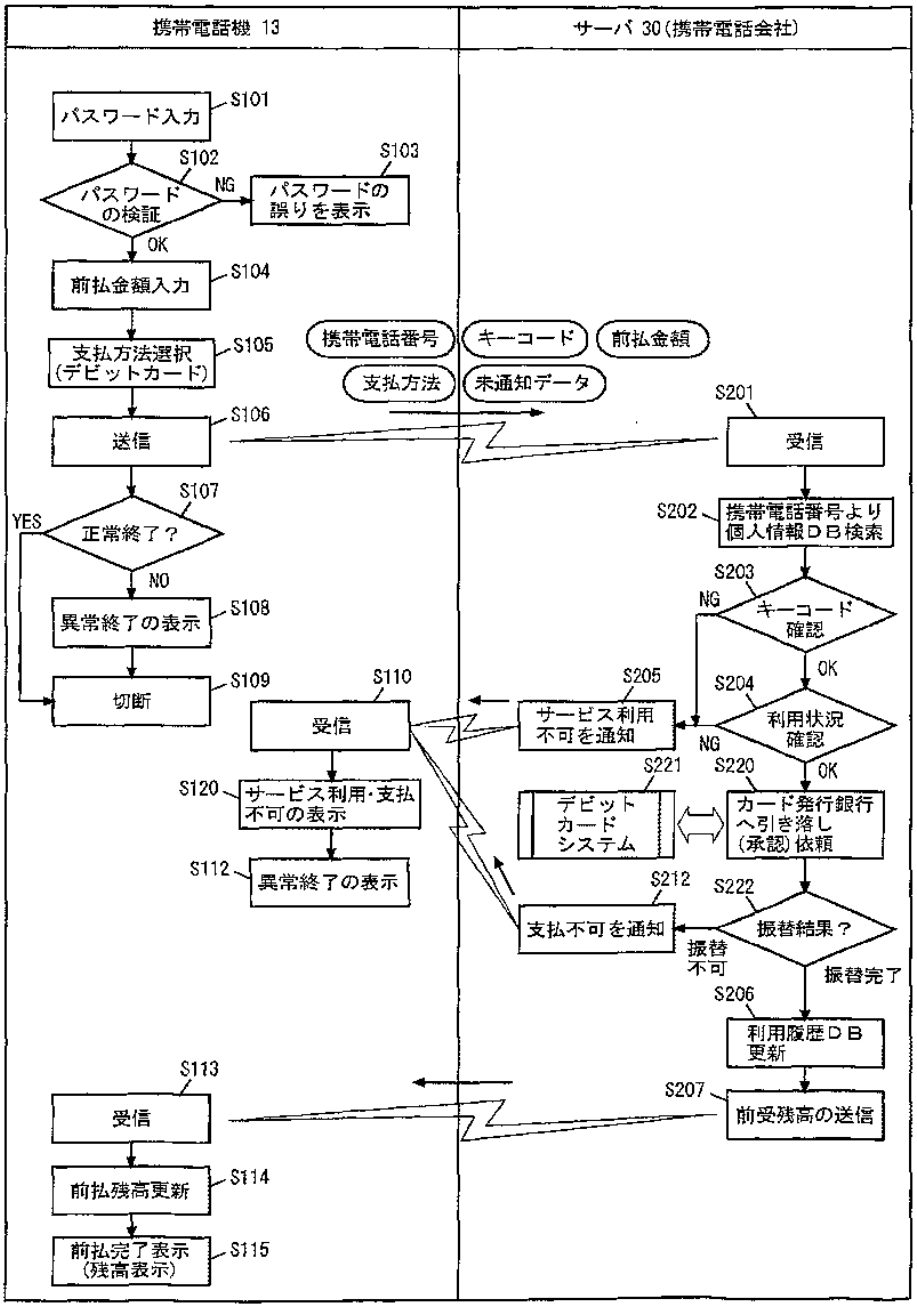
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 466 of 1360

FIG. 11



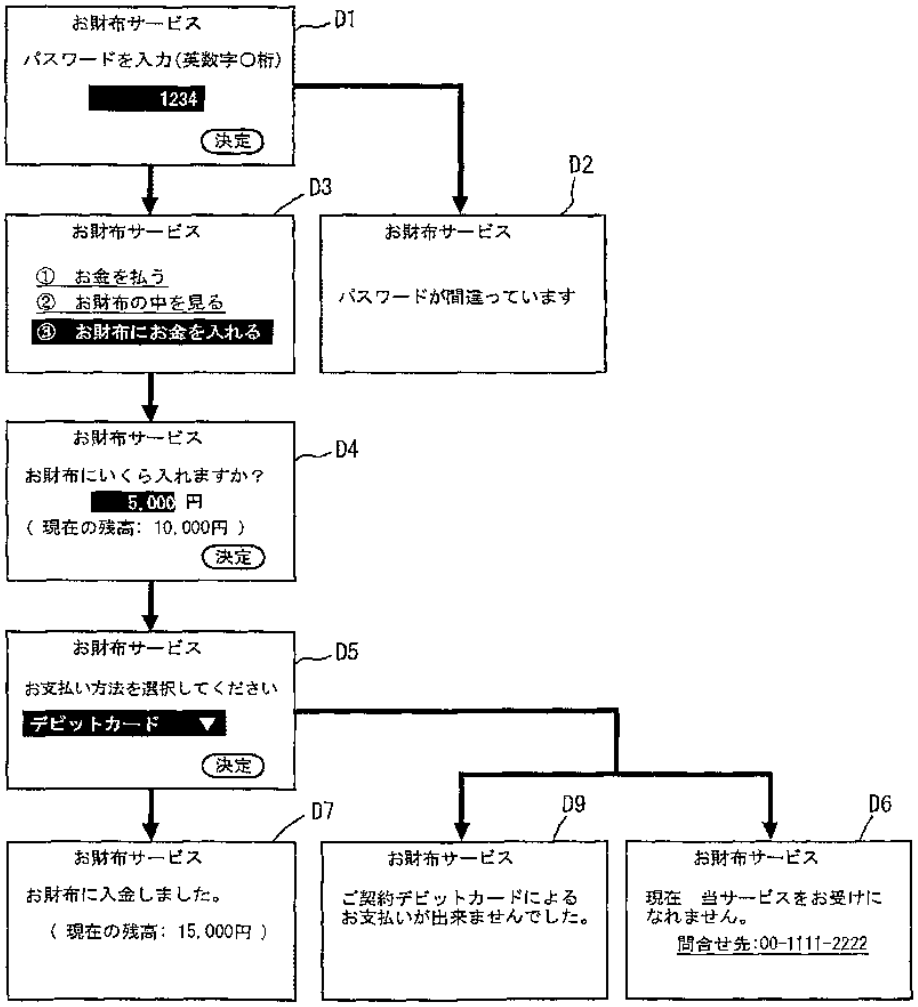
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 467 of 1360

FIG. 12



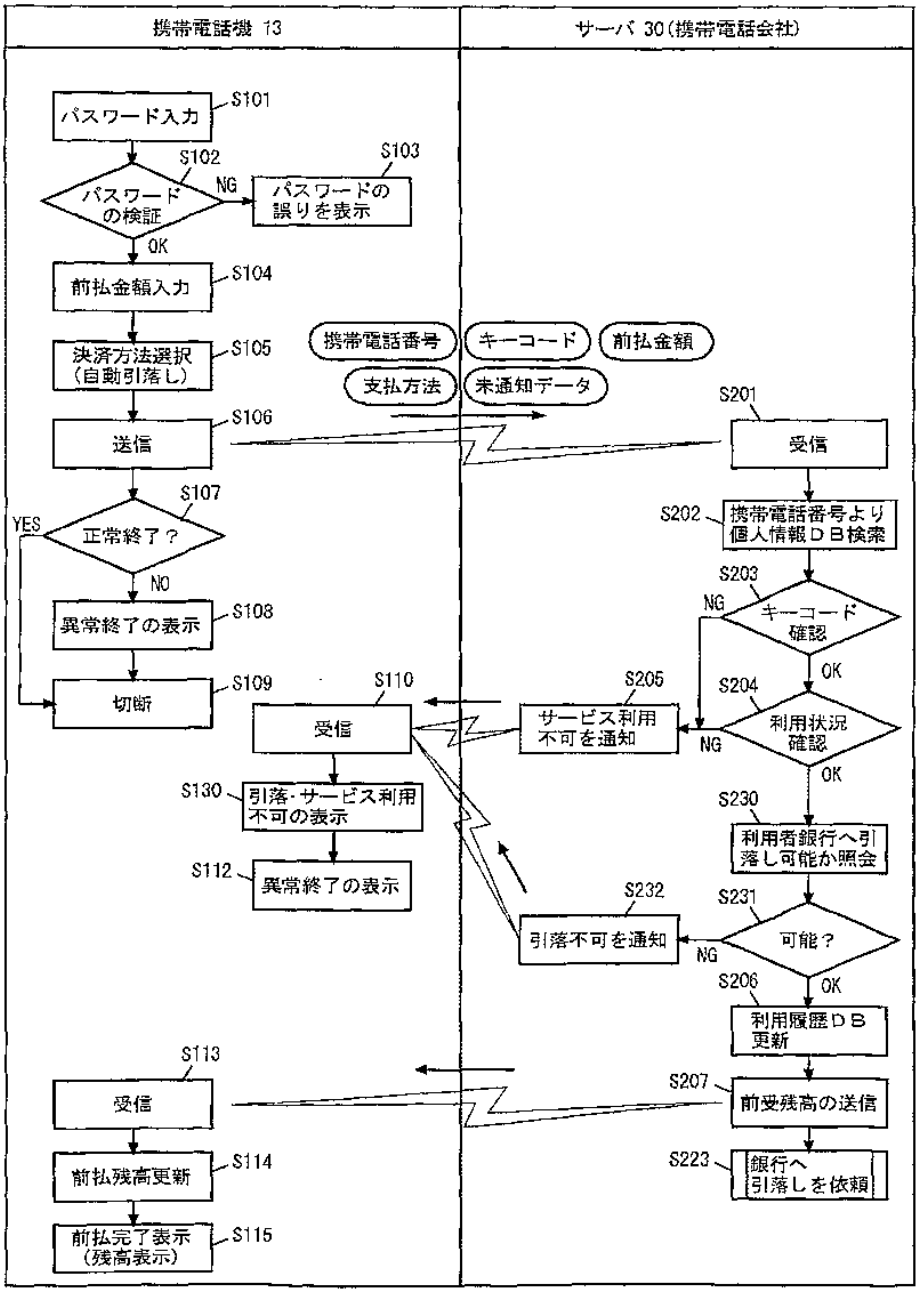
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 468 of 1360

FIG. 13



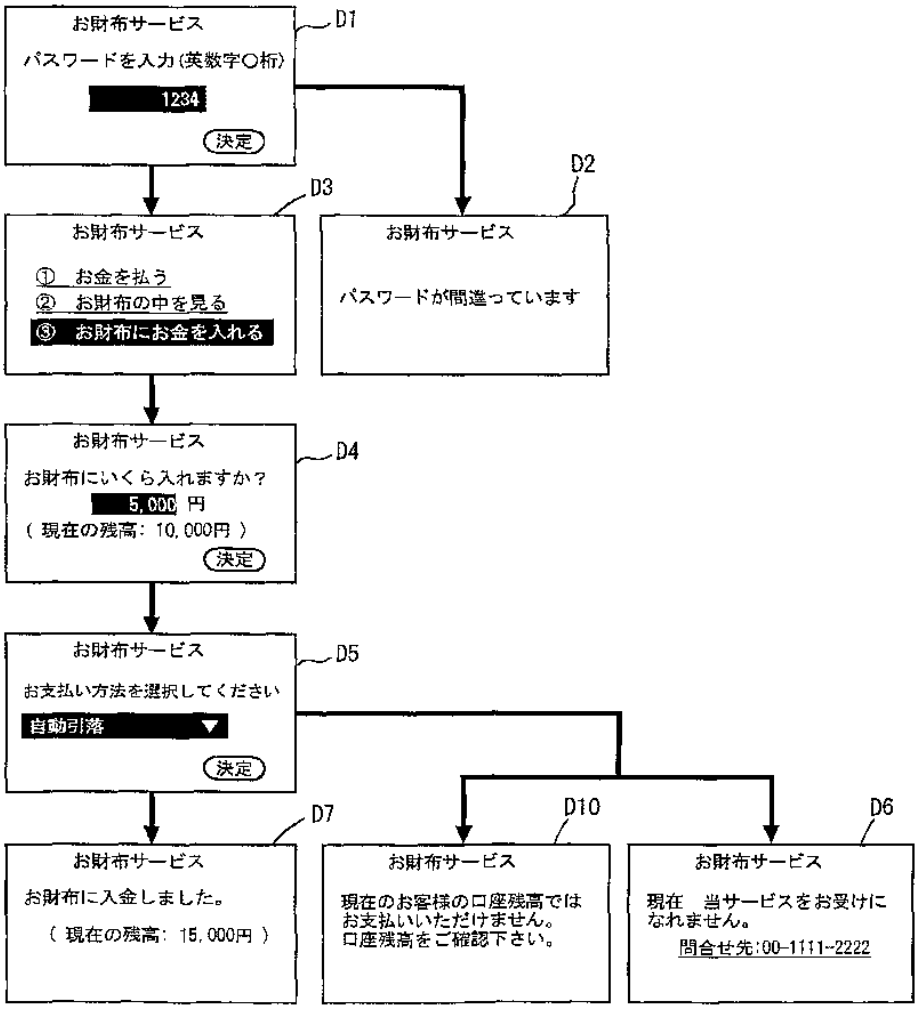
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 469 of 1360

FIG. 14



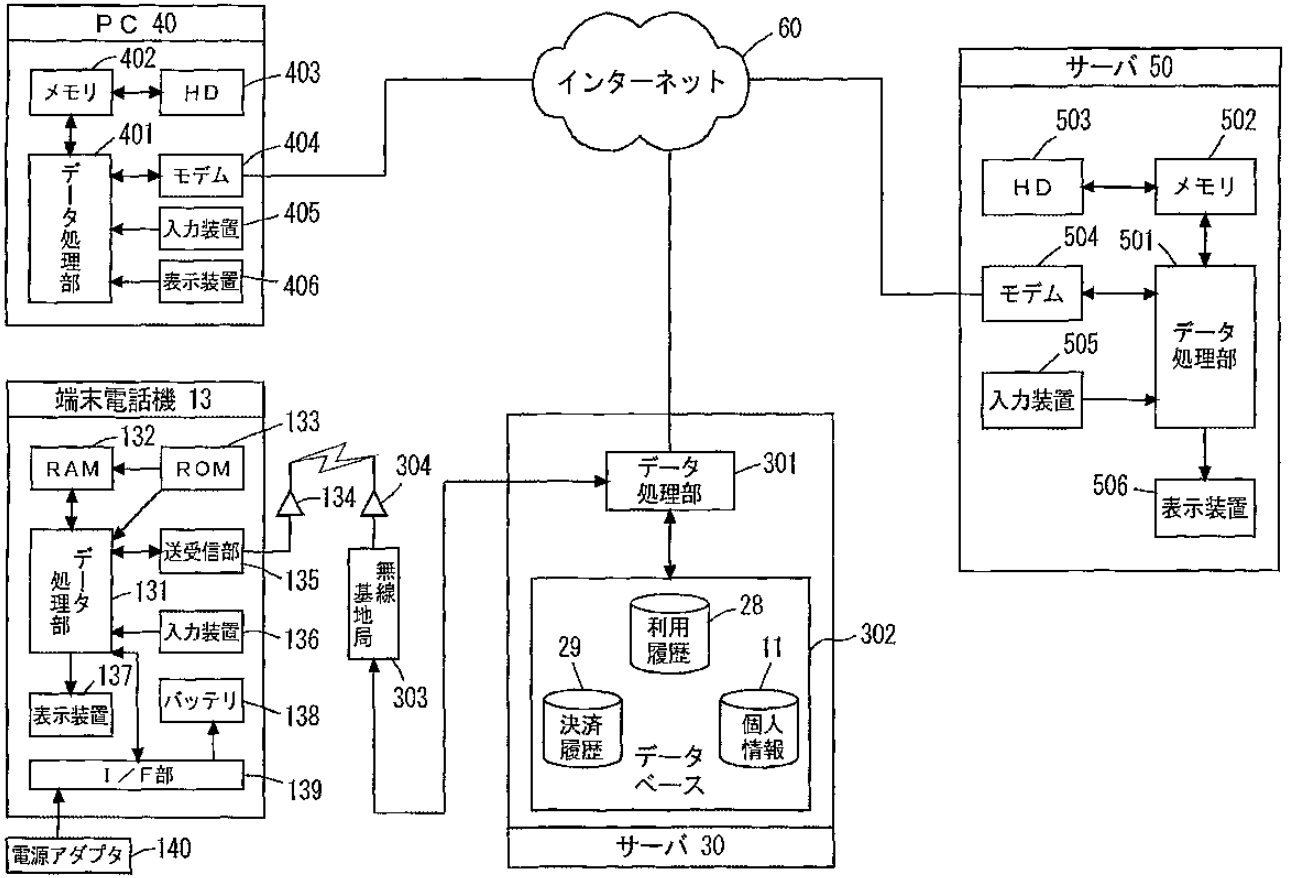
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 470 of 1360

FIG. 15



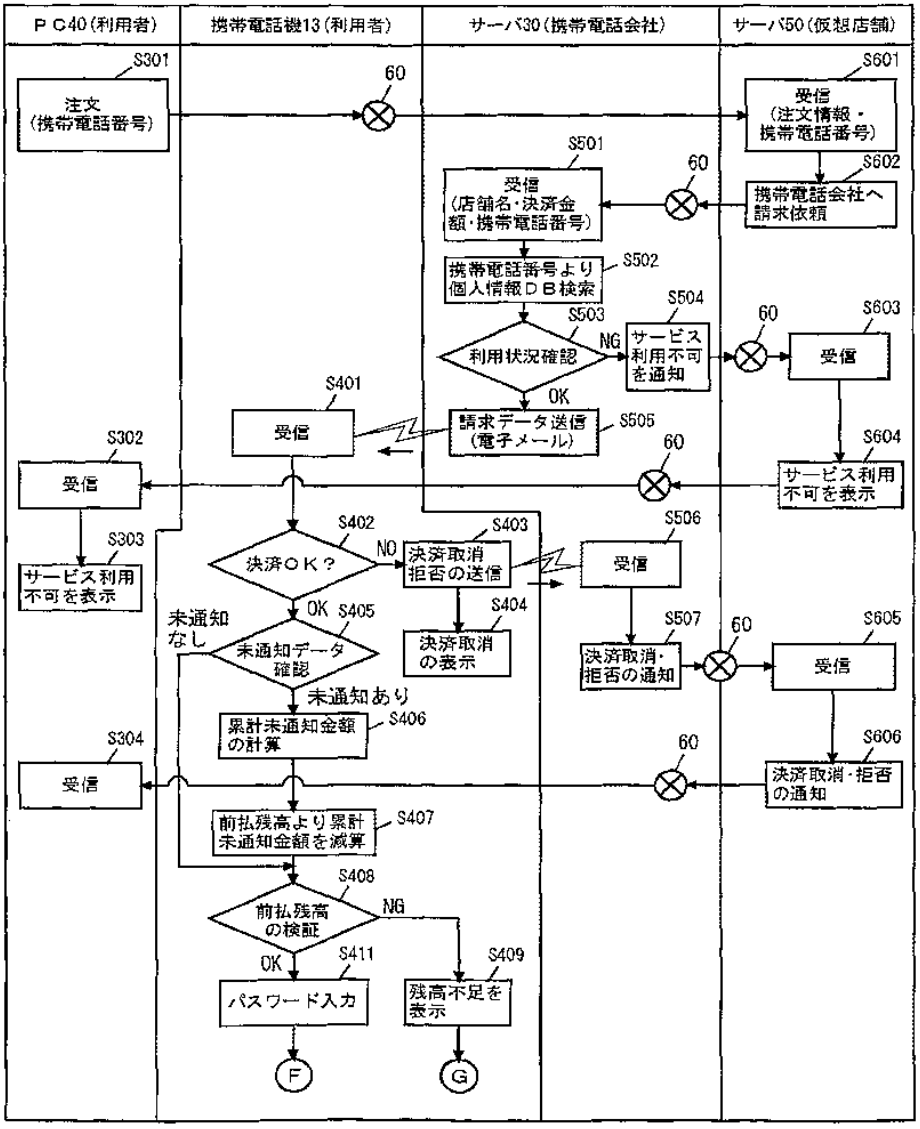
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 471 of 1360

FIG. 16



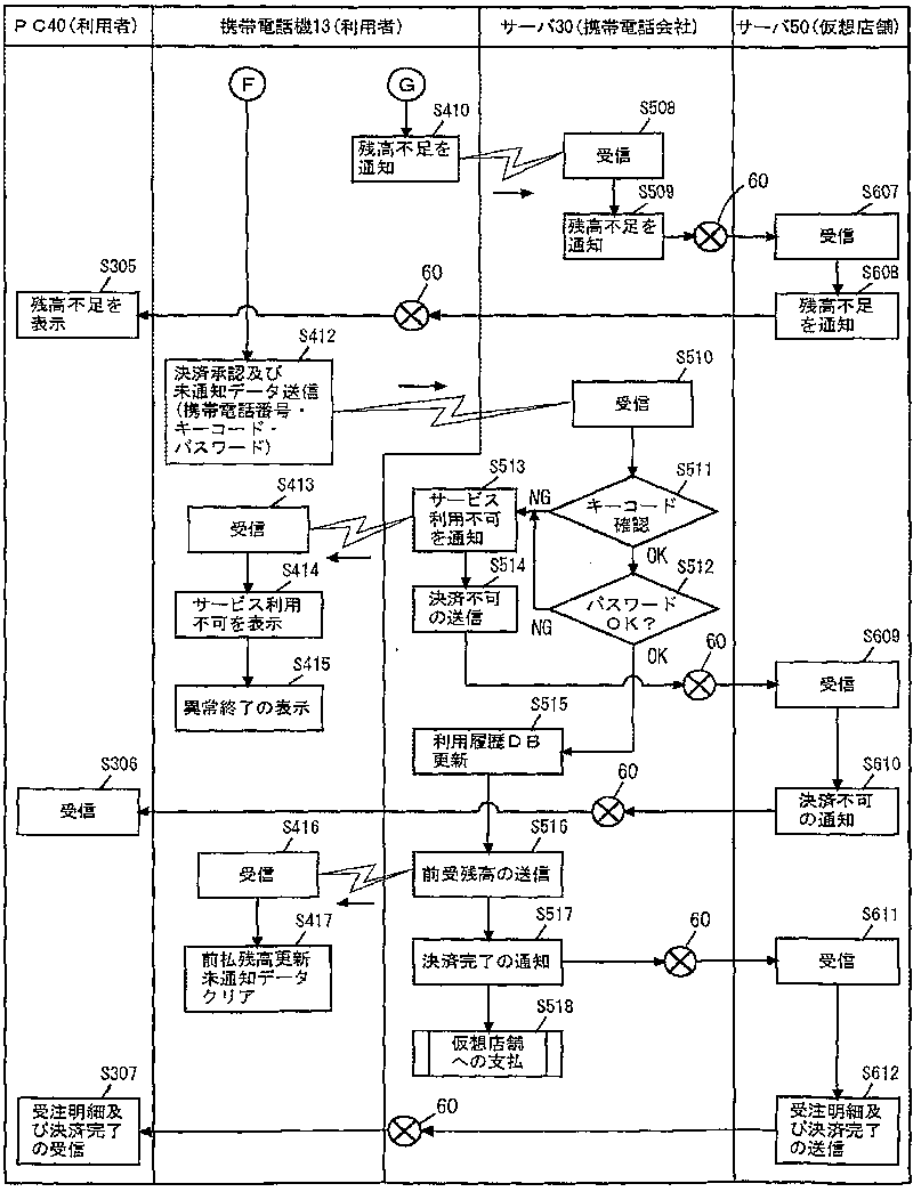
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 472 of 1360

FIG. 17



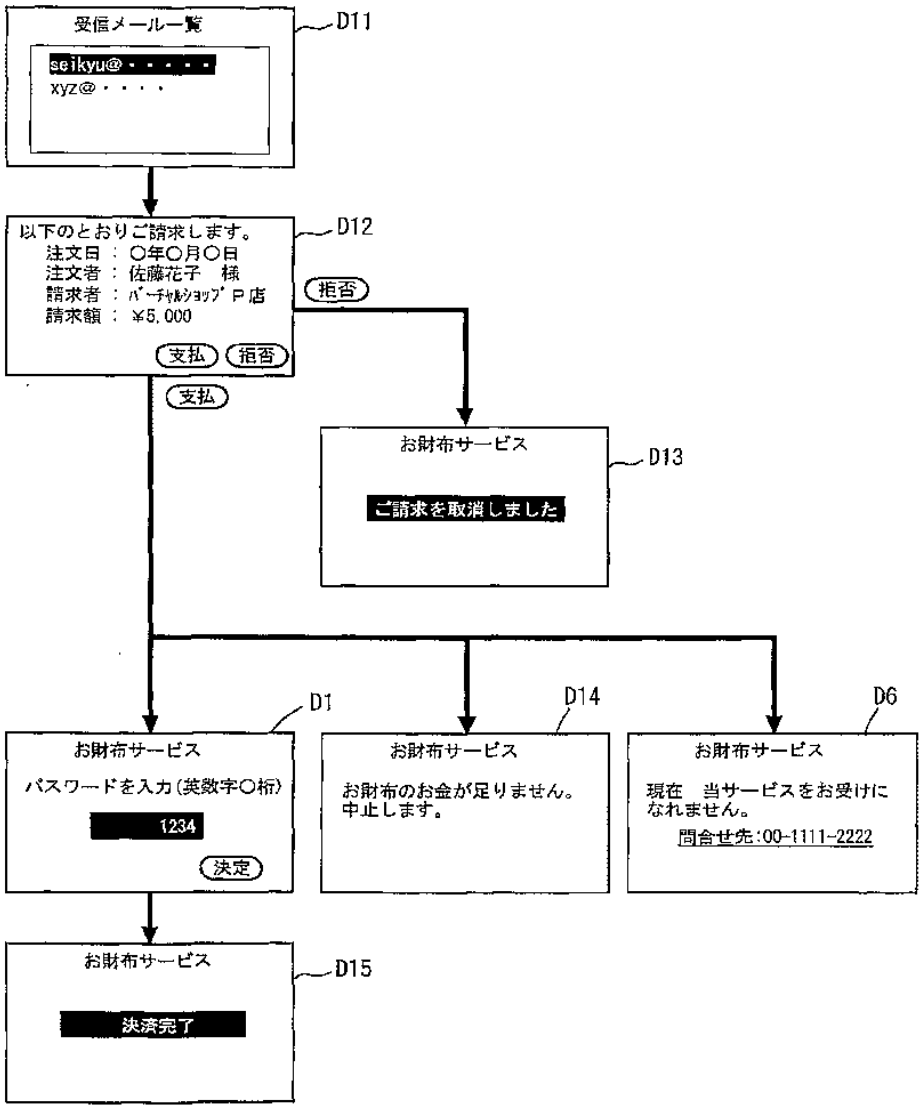
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 473 of 1360

FIG. 18



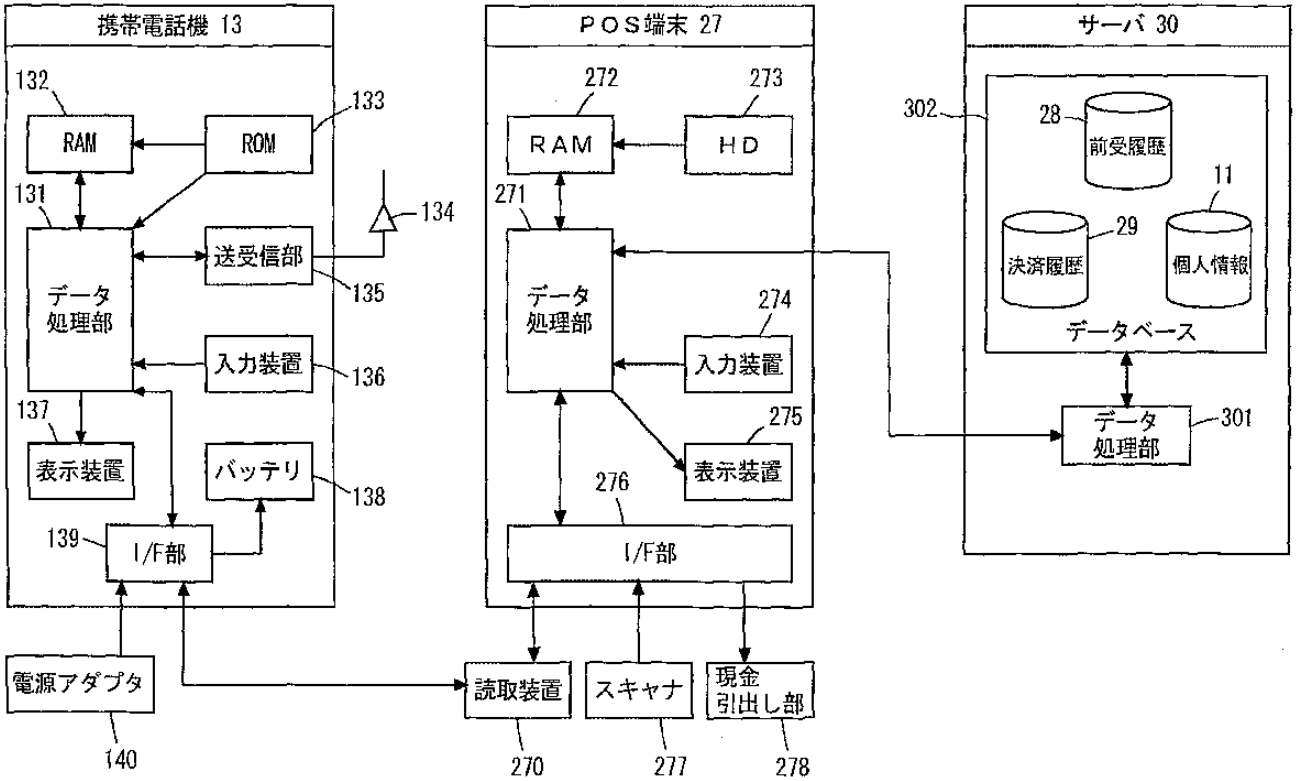
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 474 of 1360

FIG. 19



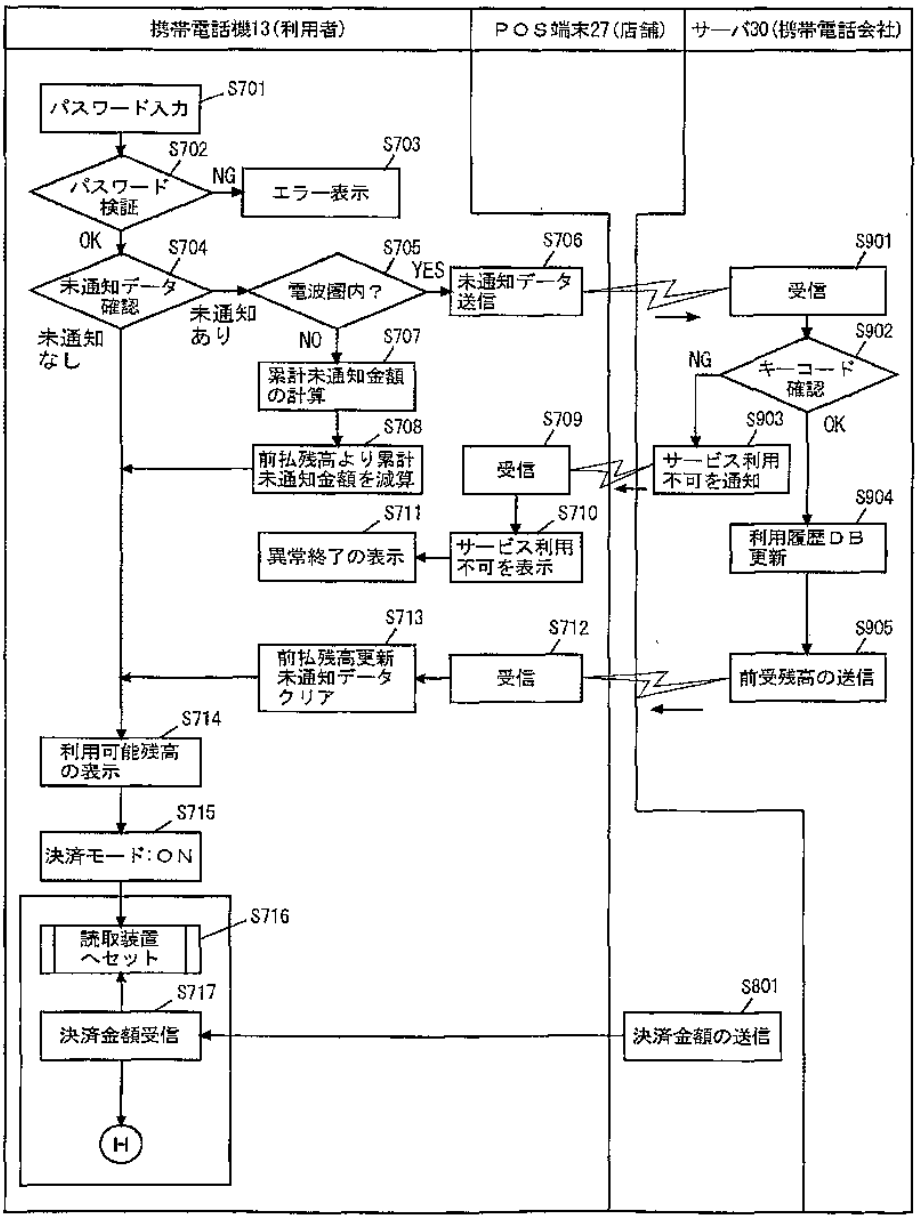
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 475 of 1360

FIG. 20



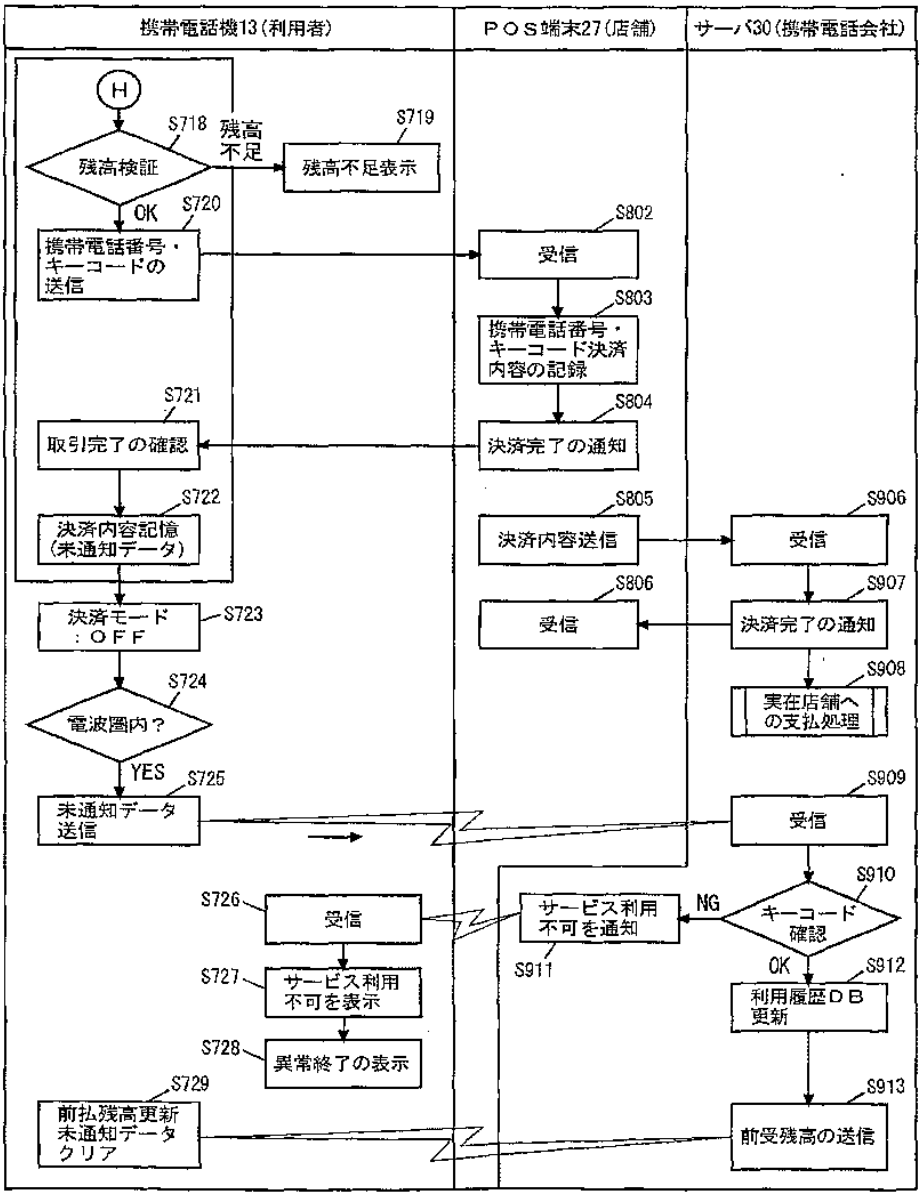
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 476 of 1360

FIG. 21



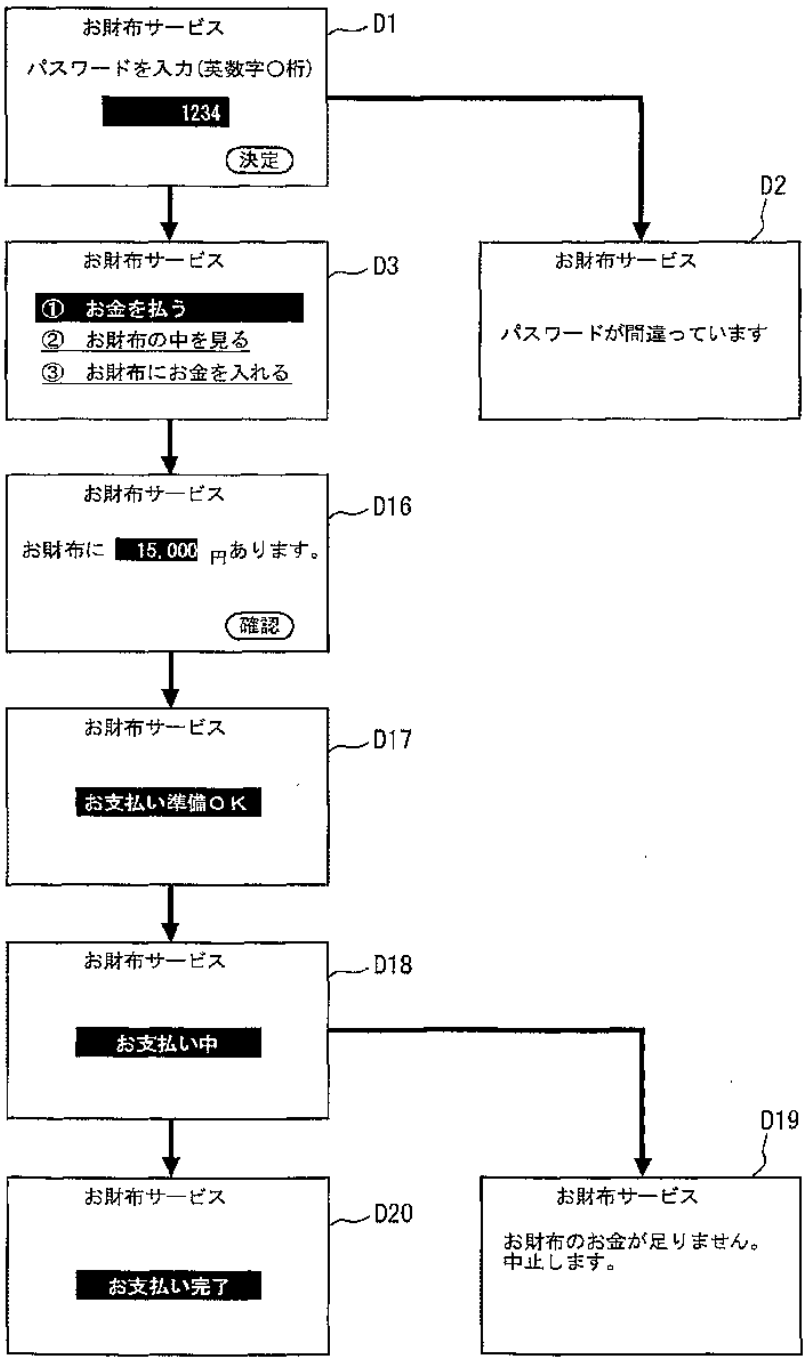
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 477 of 1360

FIG. 22



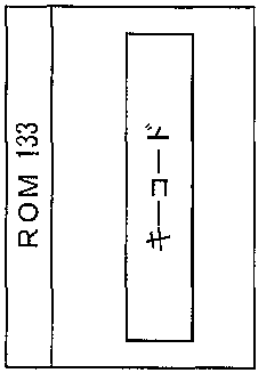
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 478 of 1360

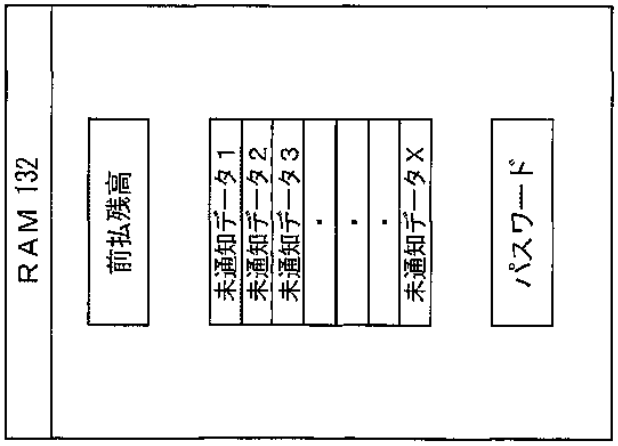
FIG. 23



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 479 of 1360

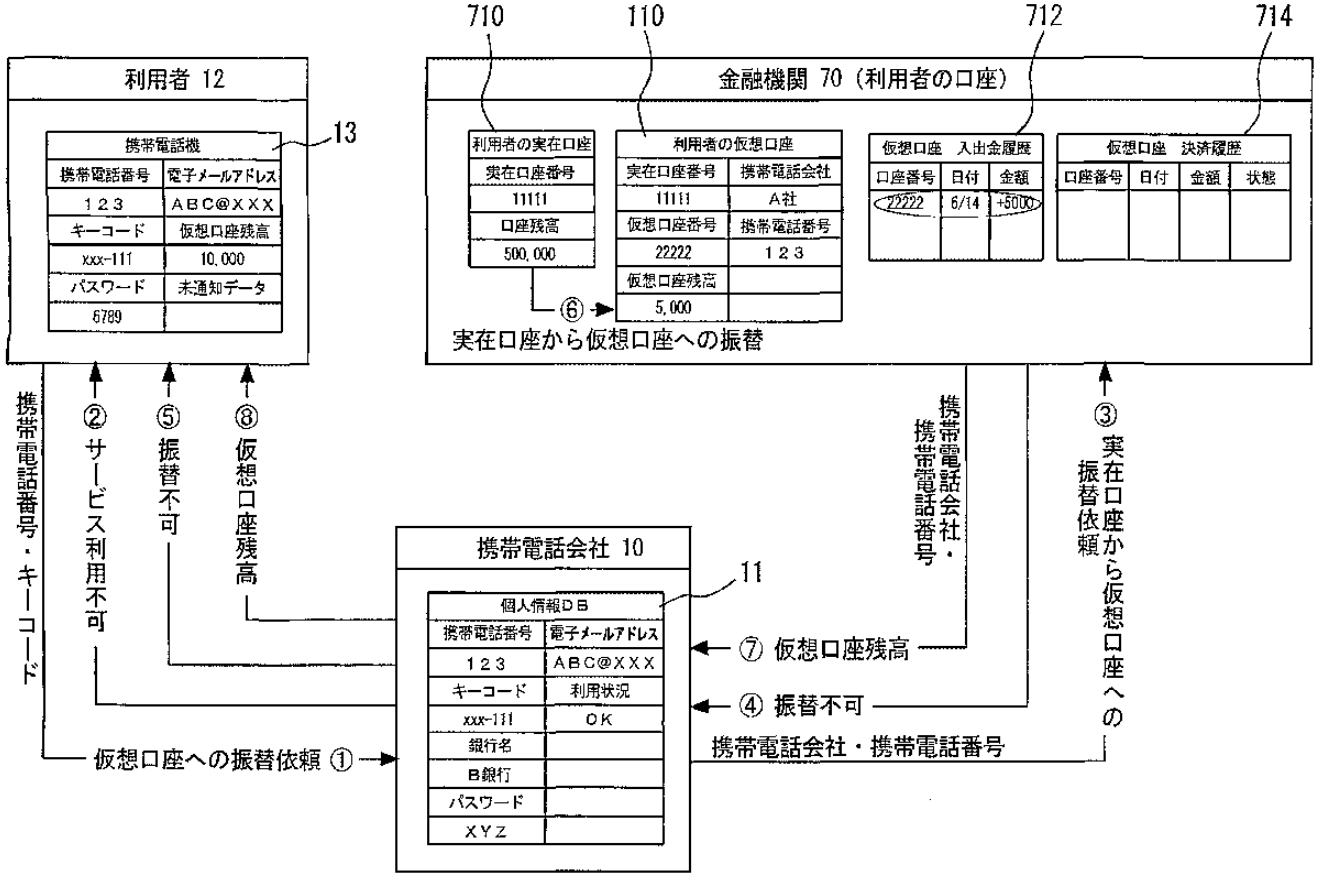
FIG. 24





PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 480 of 1360

FIG. 25



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 481 of 1360

FIG. 26

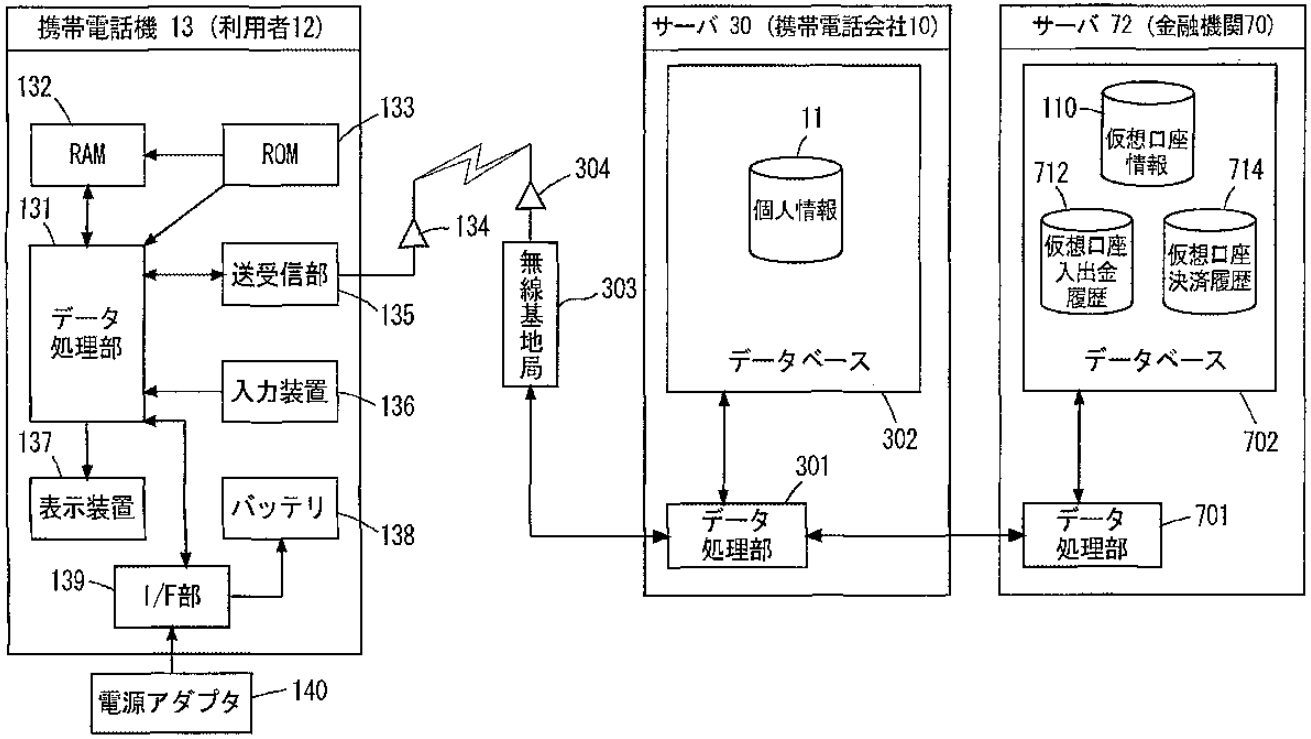
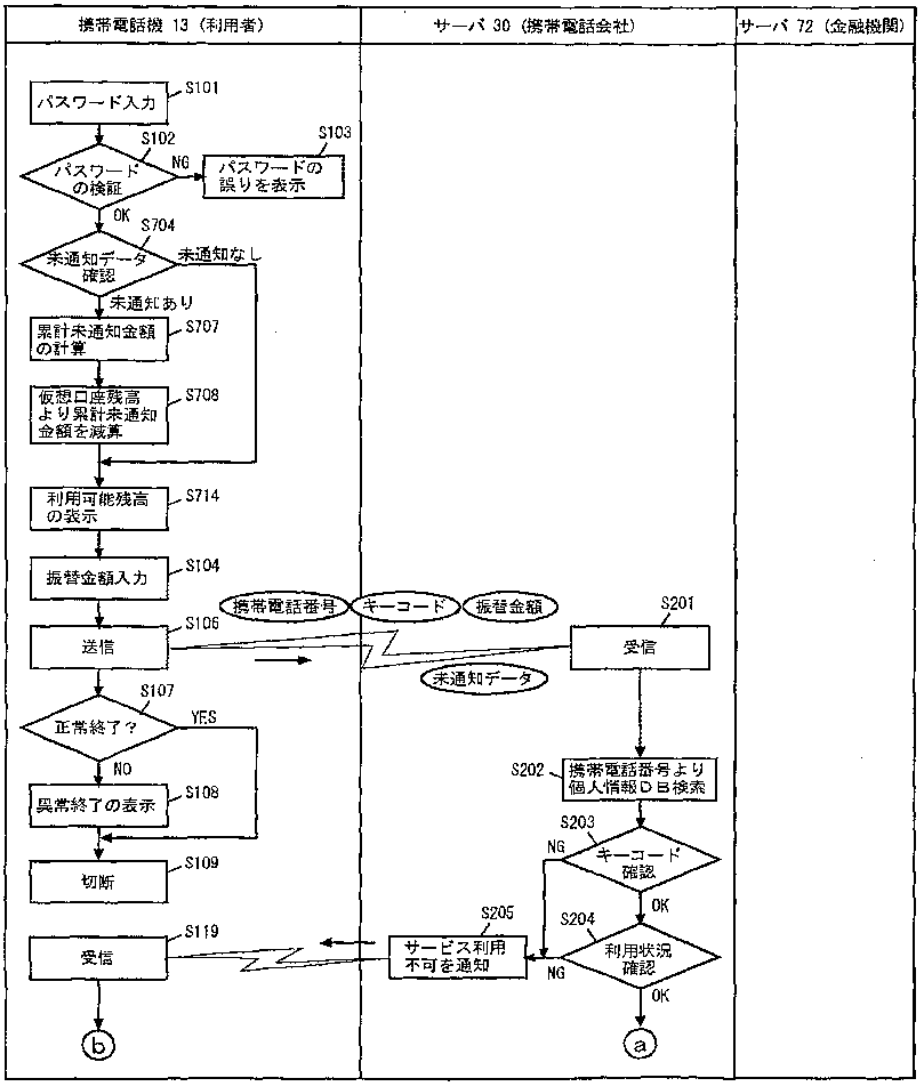
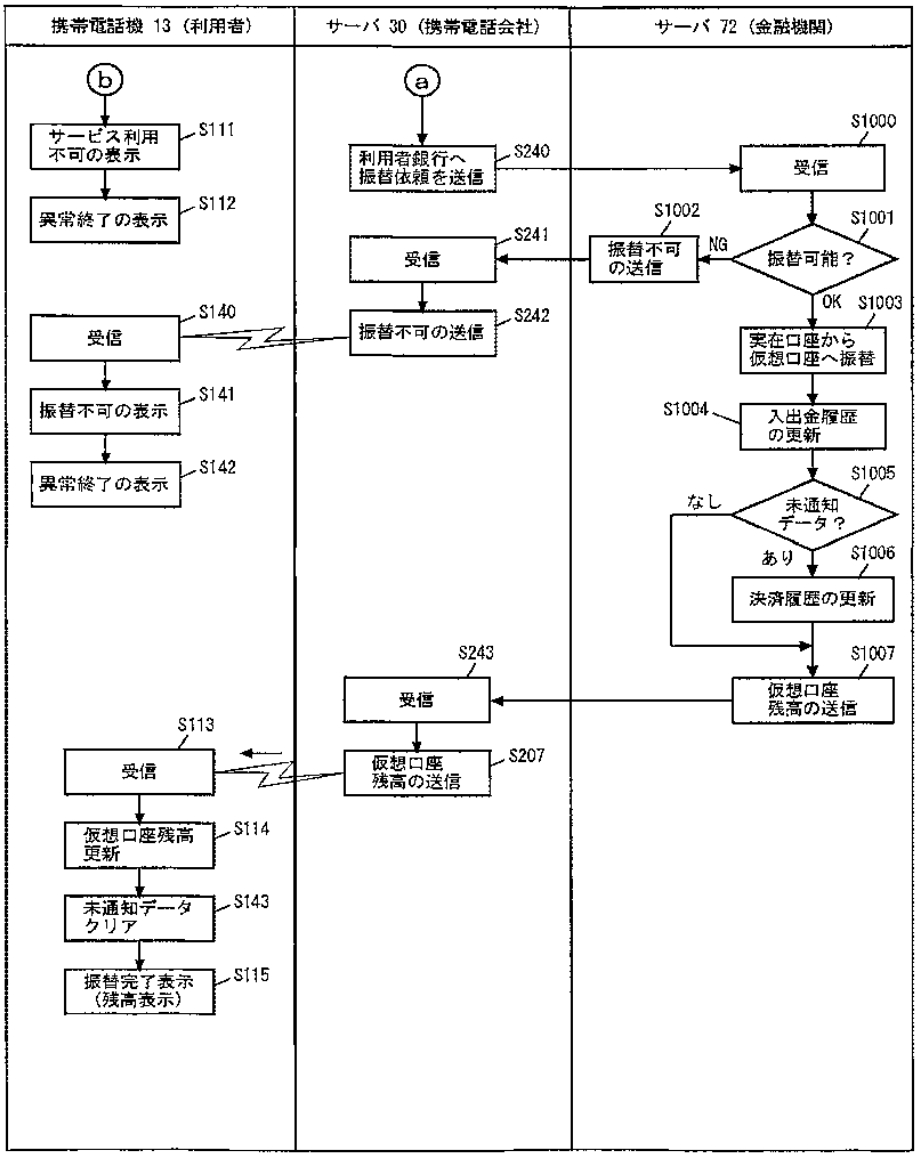

携帯電話機 13（利用者12）
132
RAM
ROM
133
131
データ処理部
送受信部
134
135
入力装置
136
137
表示装置
バッテリ
138
139
I/F部
電源アダプタ
140
304
無線基地局
303
サーバ 30（携帯電話会社10）
11
個人情報
データベース
302
301
データ処理部
サーバ 72（金融機関70）
110
仮想口座情報
712
714
仮想口座入出金履歴
仮想口座決済履歴
データベース
702
データ処理部
701

FIG. 27



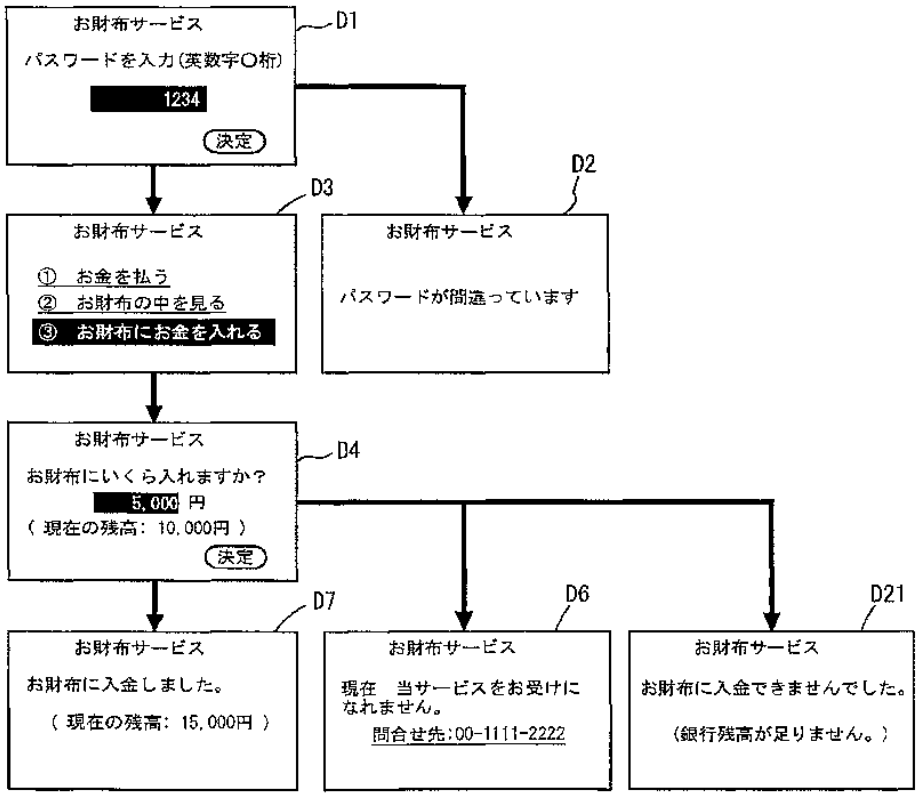
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 483 of 1360

FIG. 28



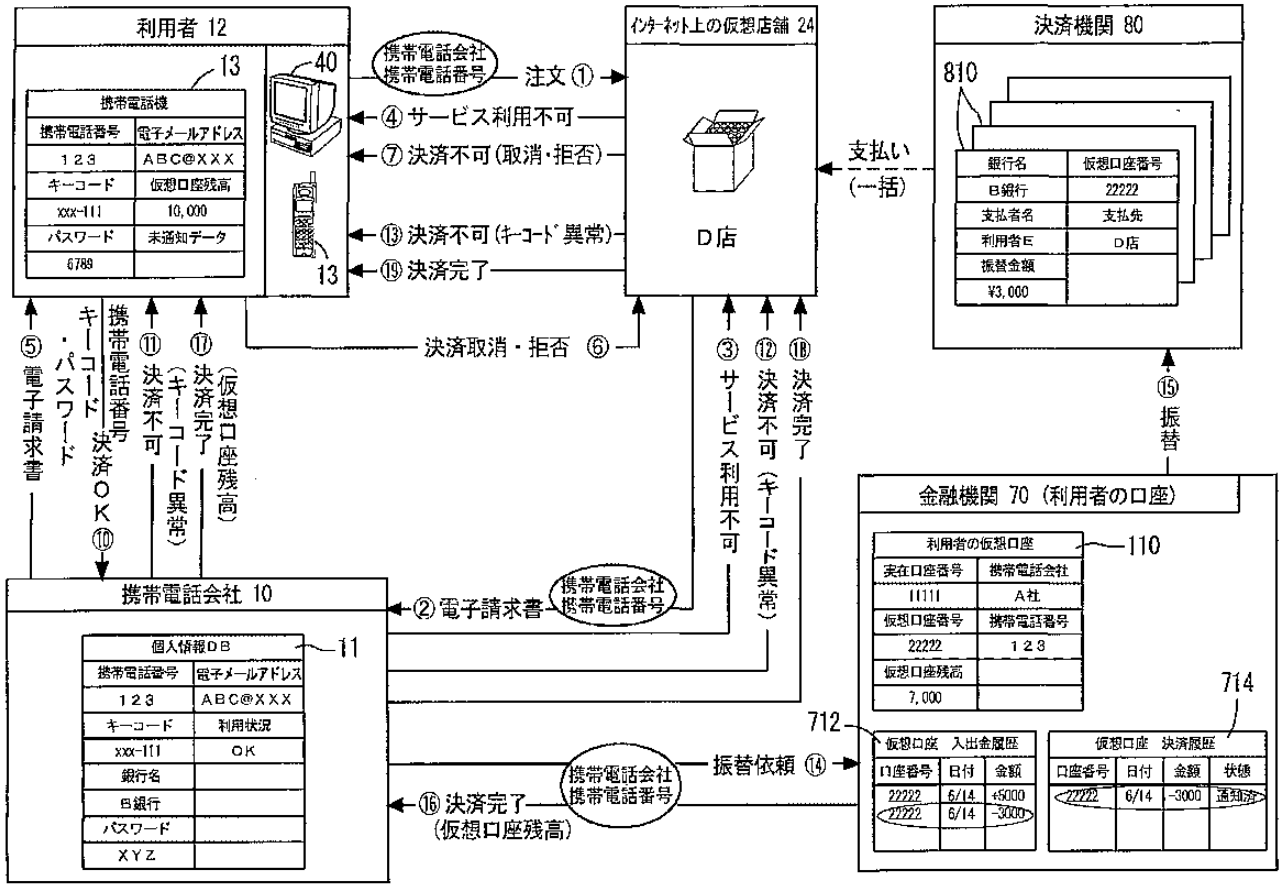
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 484 of 1360

FIG. 29



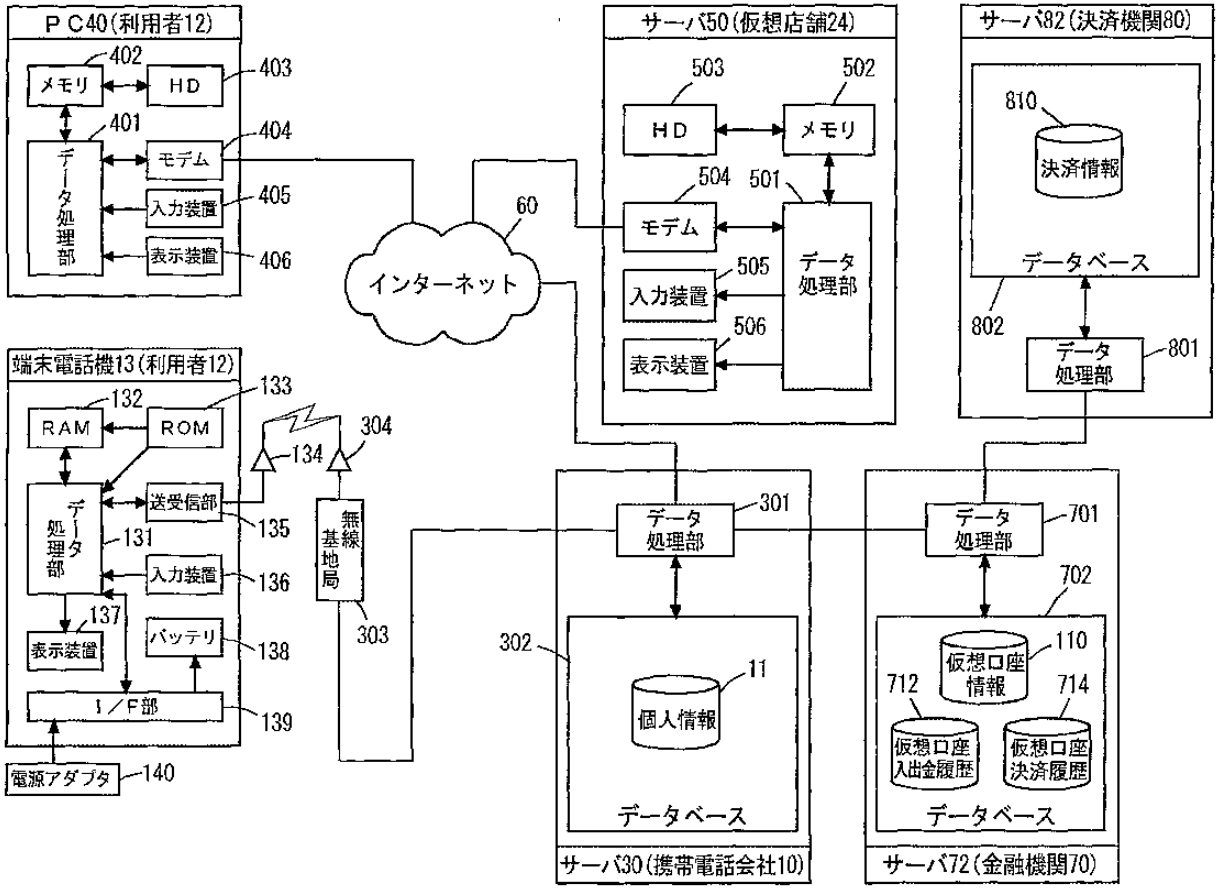
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 485 of 1360

FIG. 30



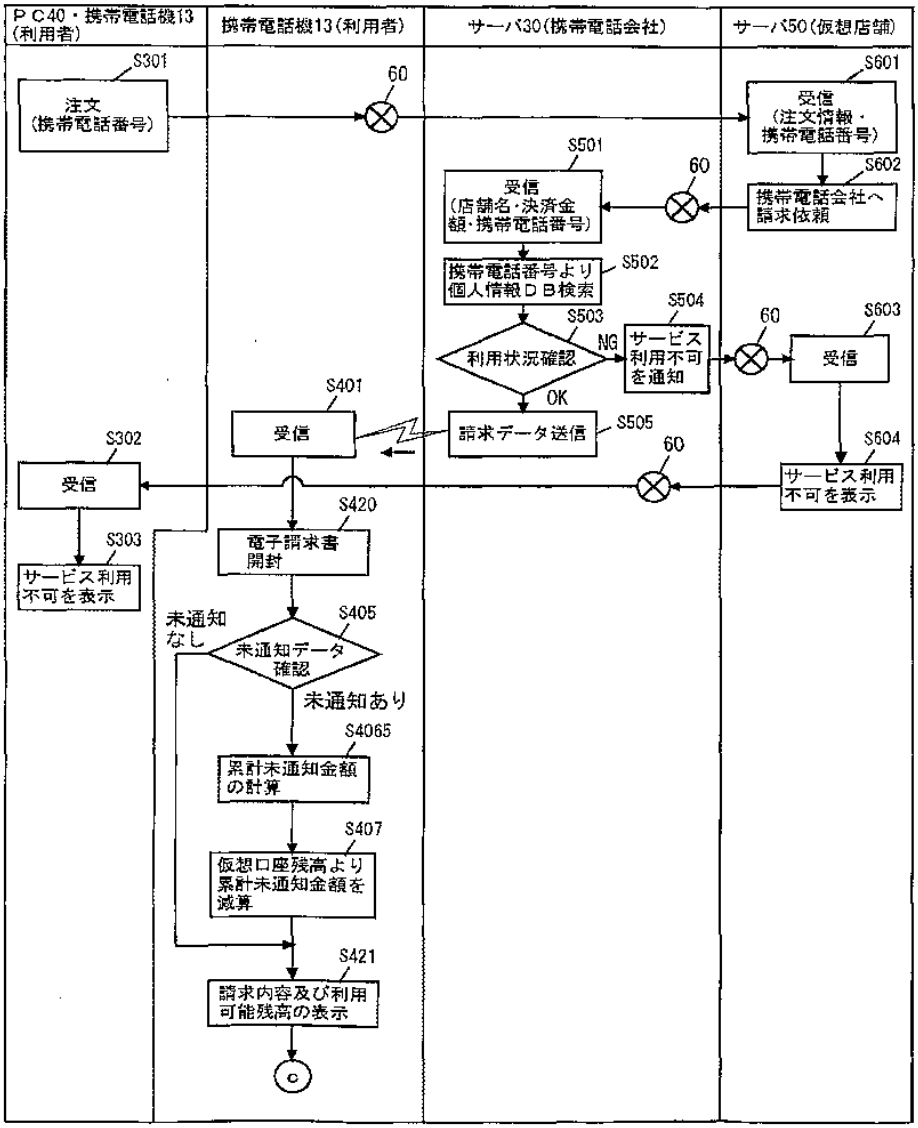
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 486 of 1360

FIG. 31



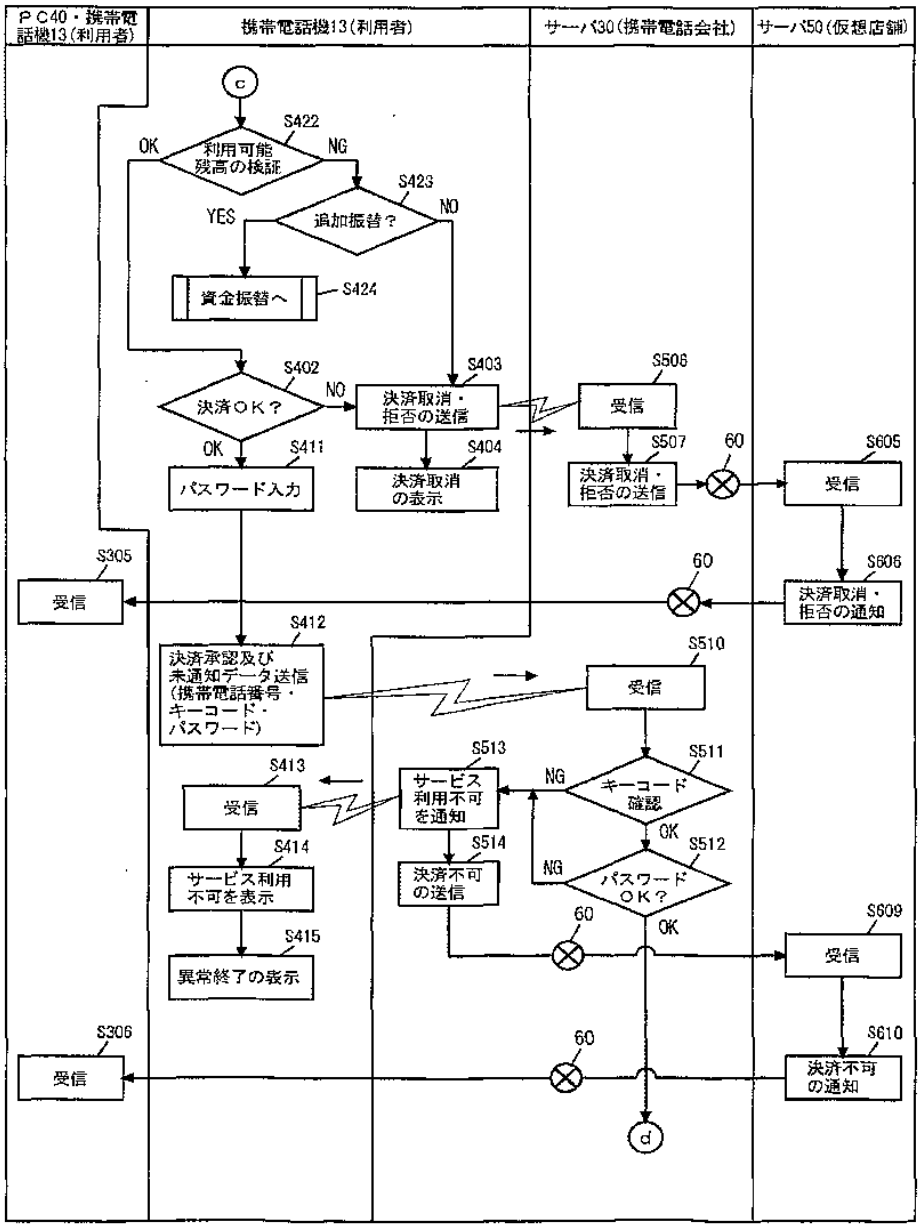
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 487 of 1360

FIG. 32



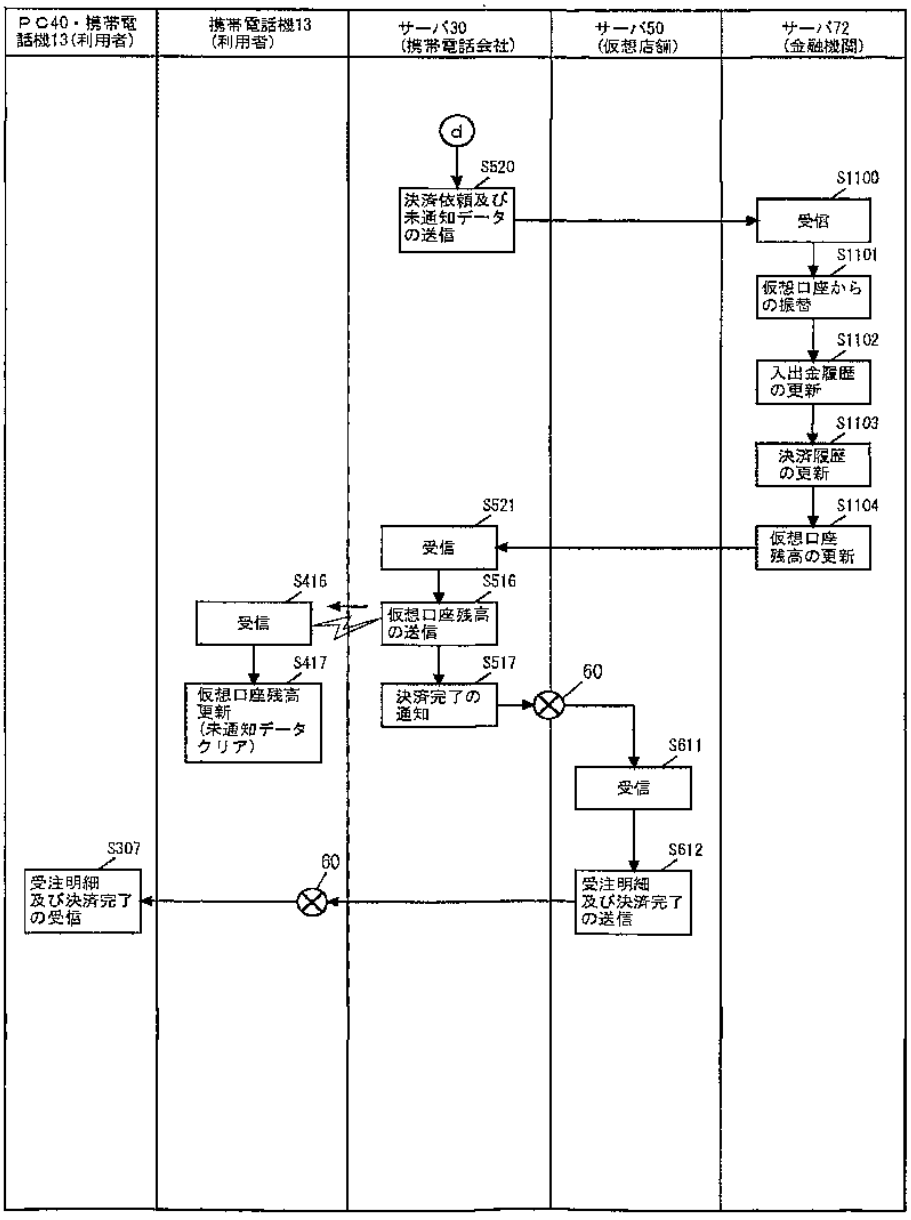
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 488 of 1360

FIG. 33



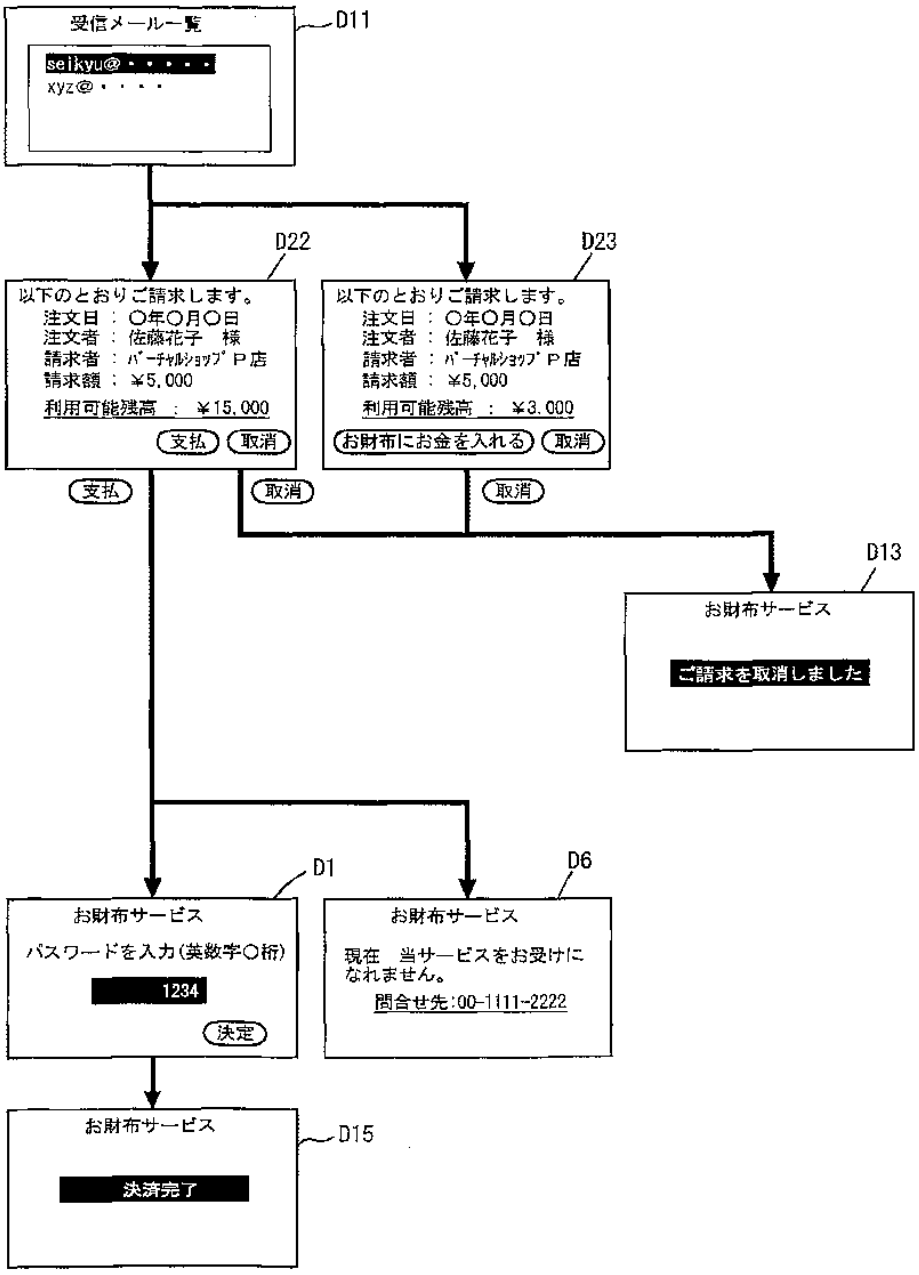
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 489 of 1360

FIG. 34



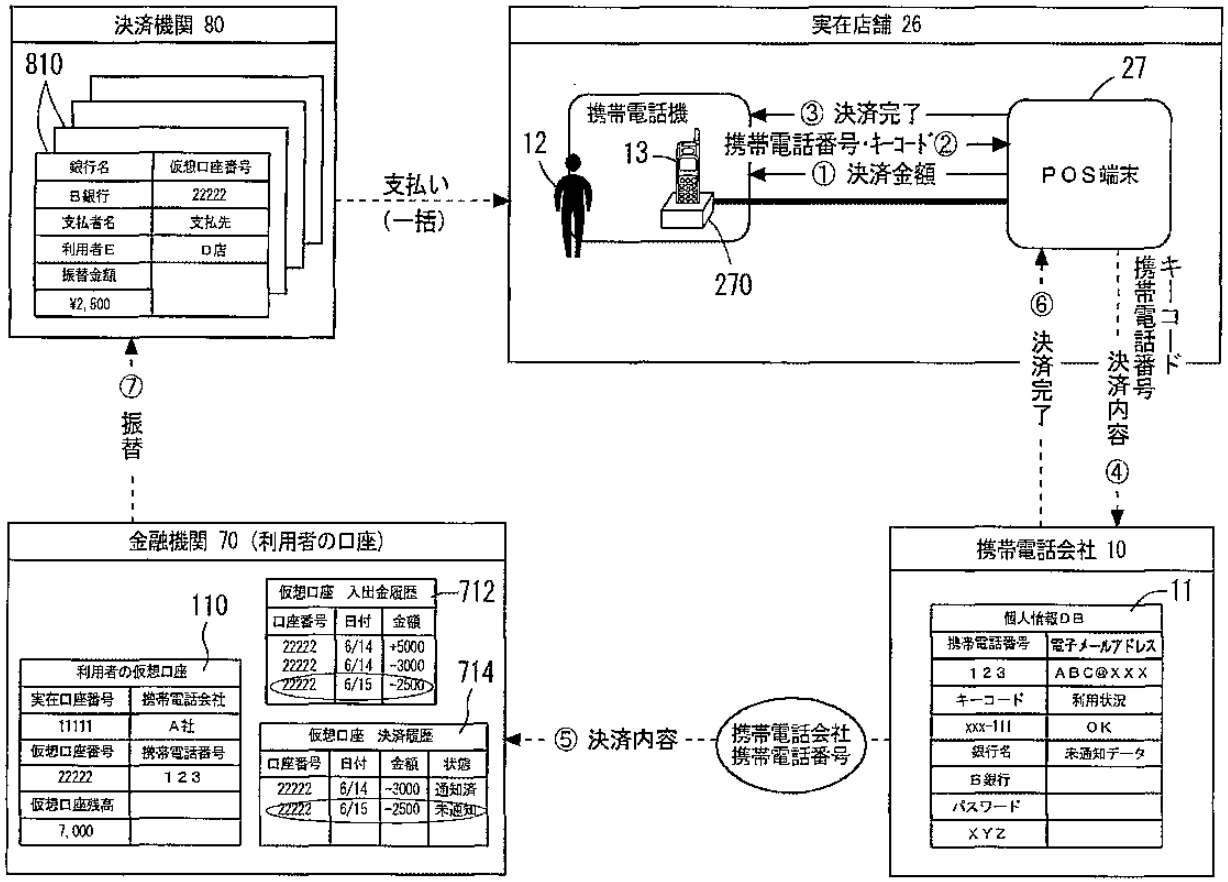
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 490 of 1360

FIG. 35



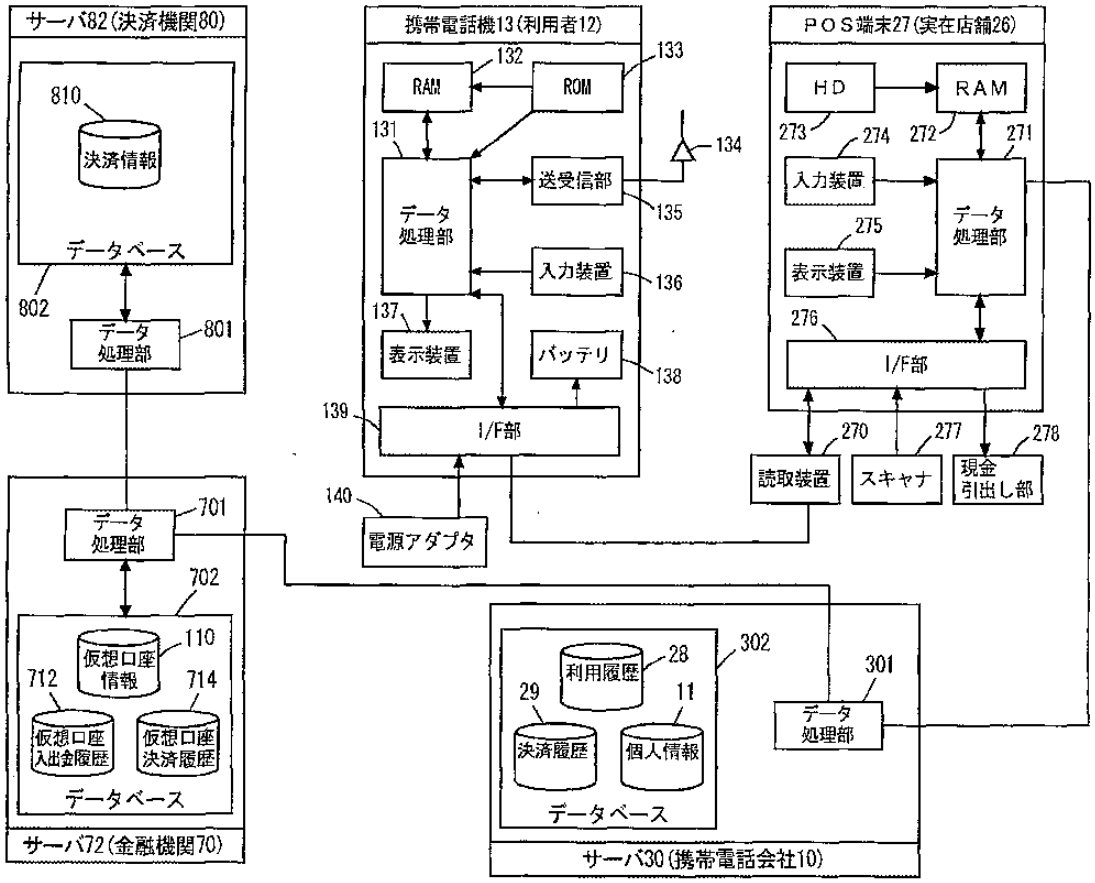
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 491 of 1360

FIG. 36



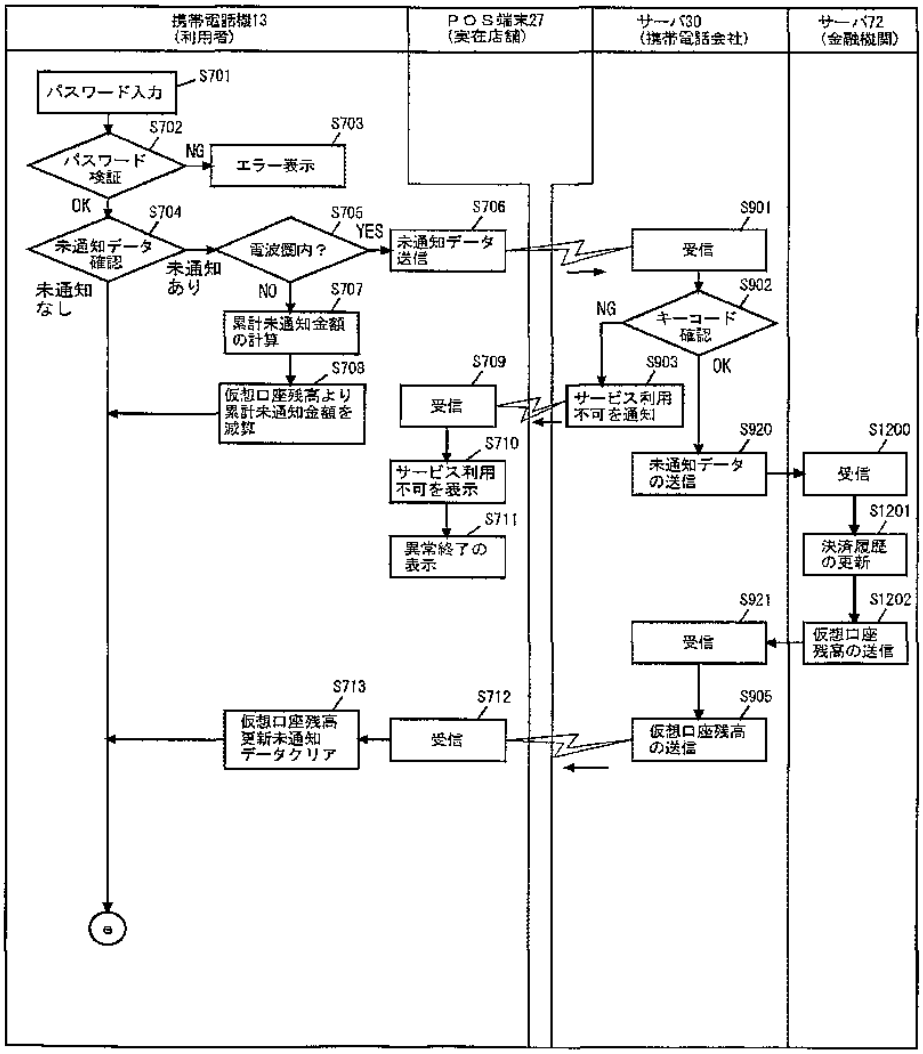
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 492 of 1360

FIG. 37



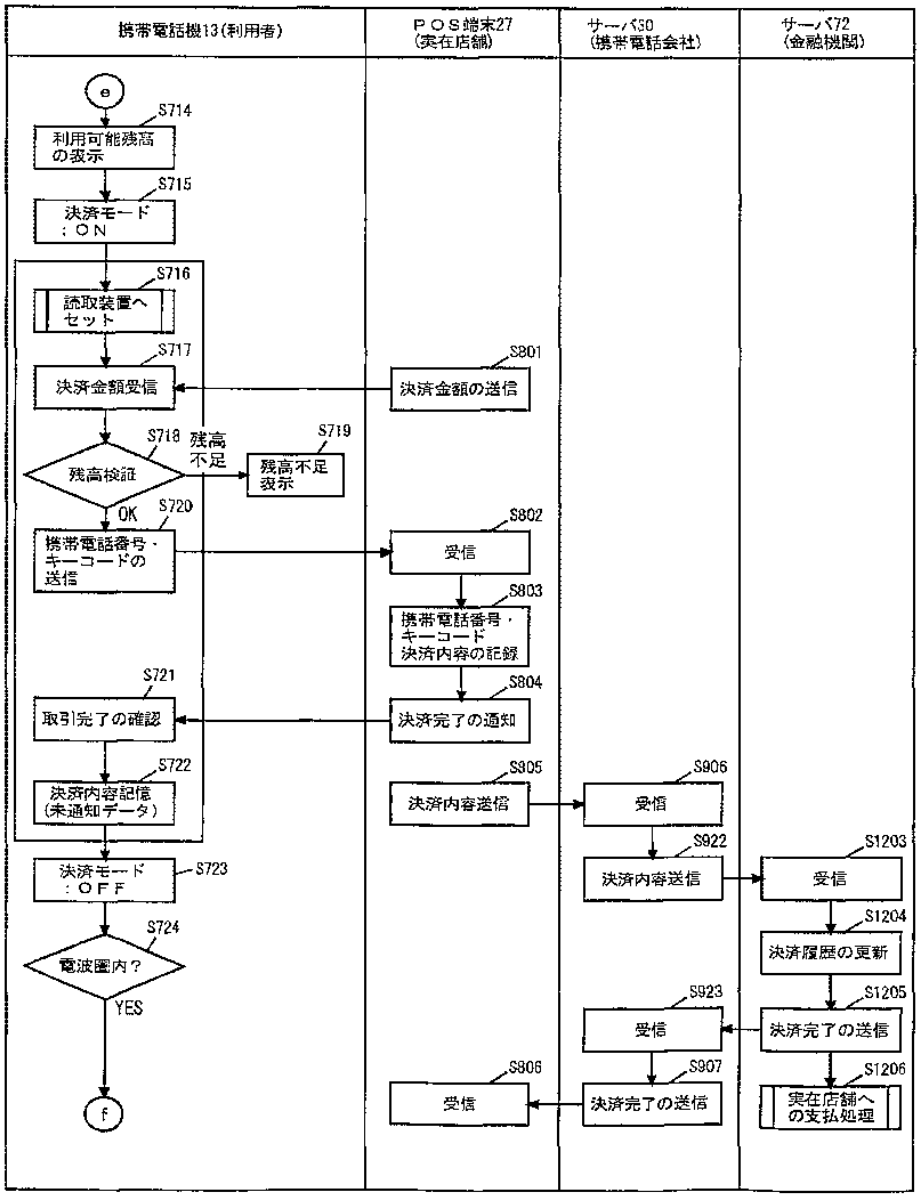
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 493 of 1360

FIG. 38



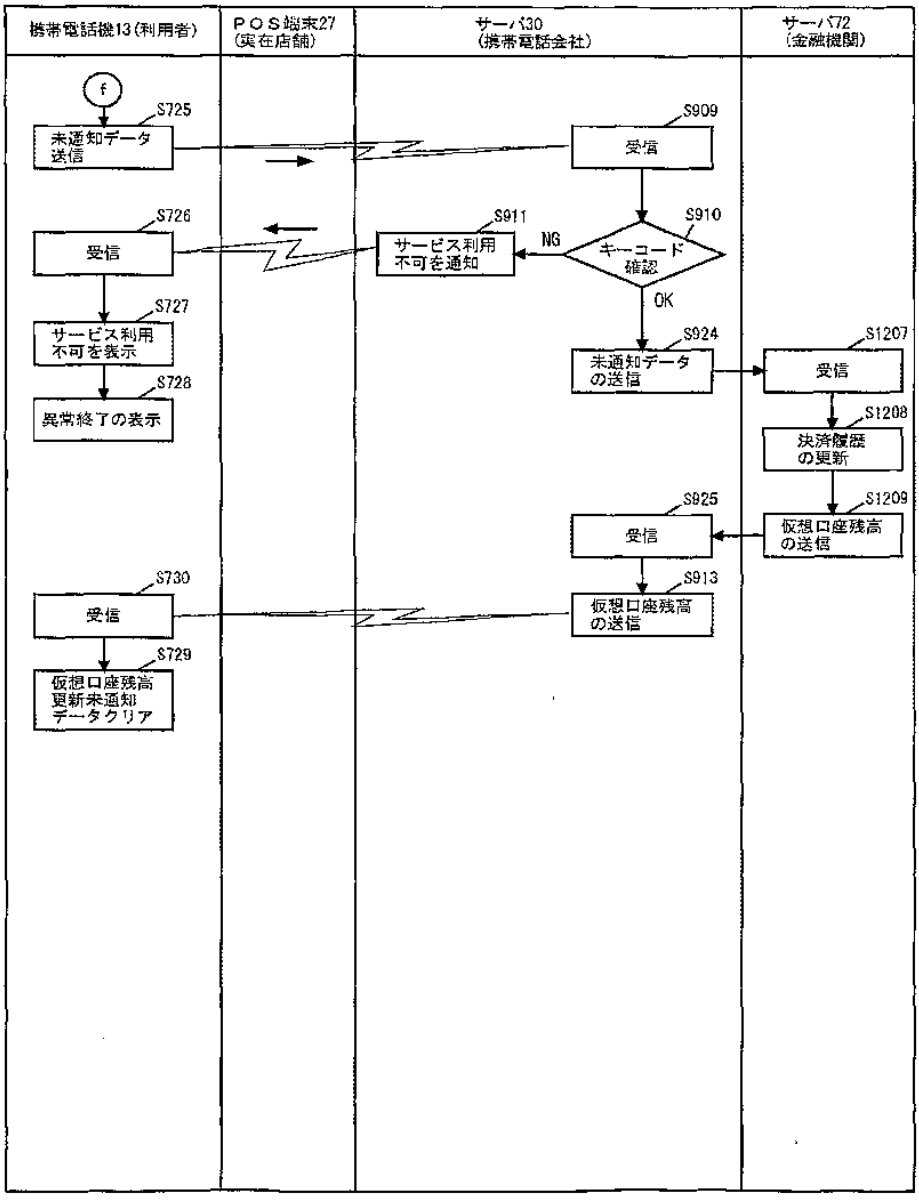
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 494 of 1360

FIG. 39



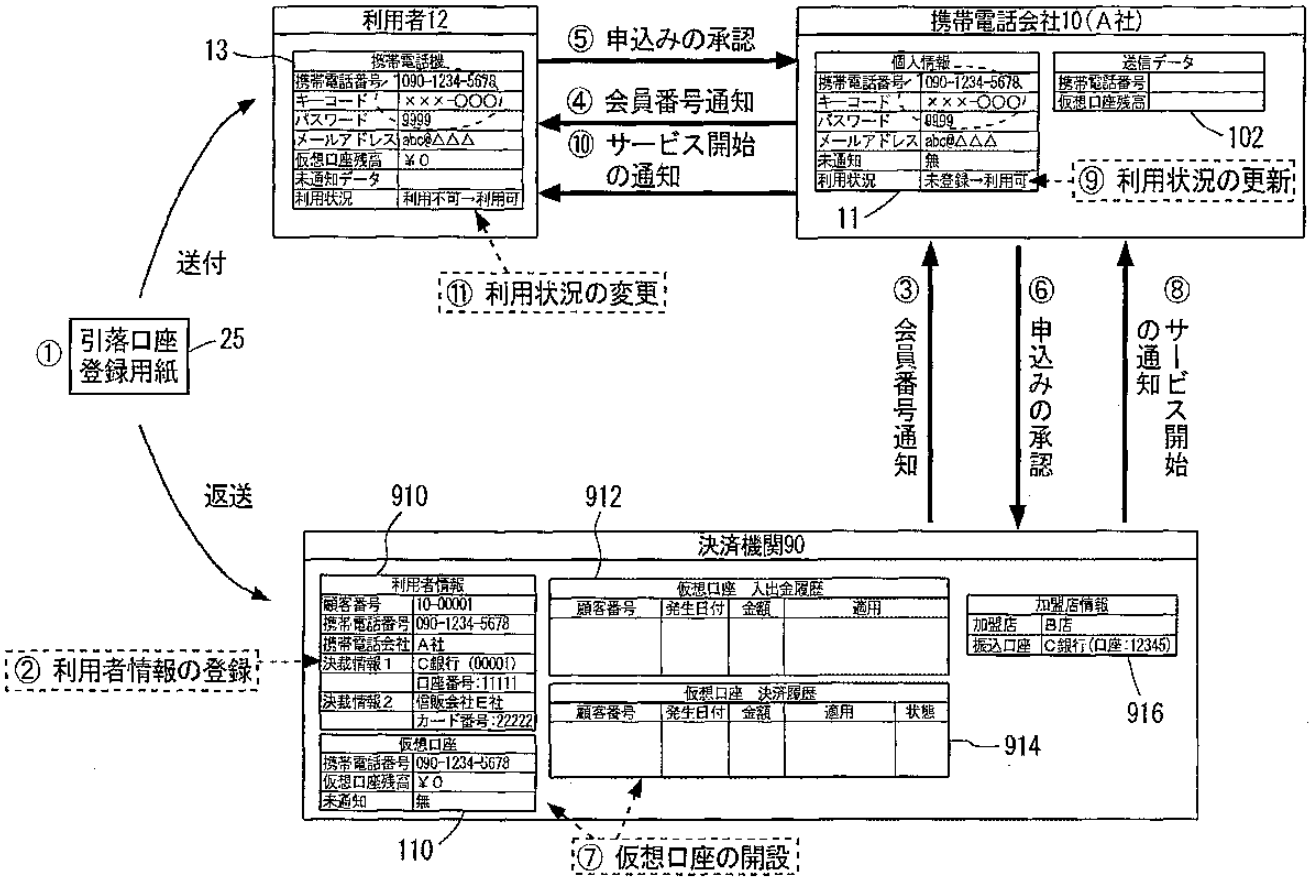
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 495 of 1360

FIG. 40



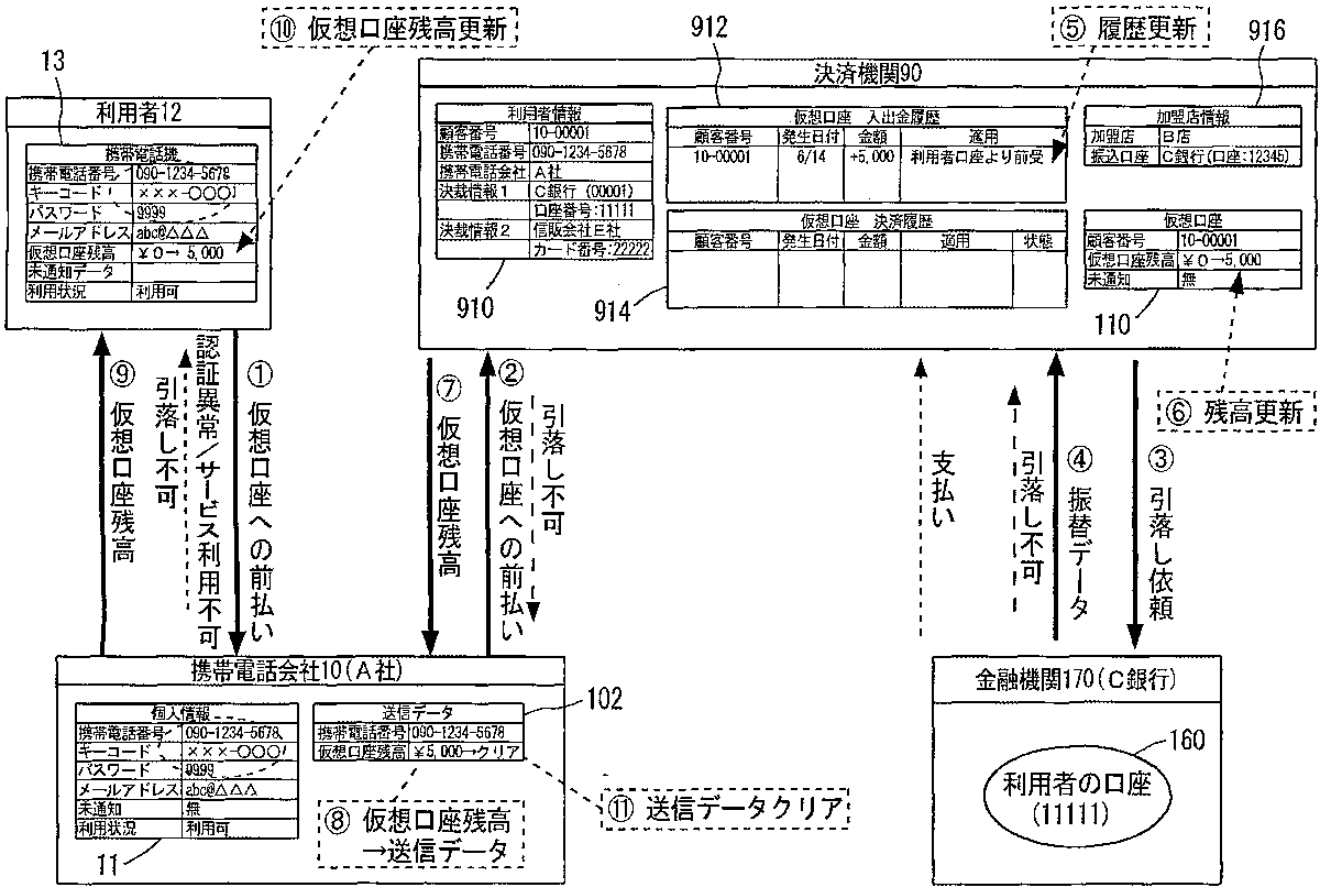
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 496 of 1360

FIG. 41



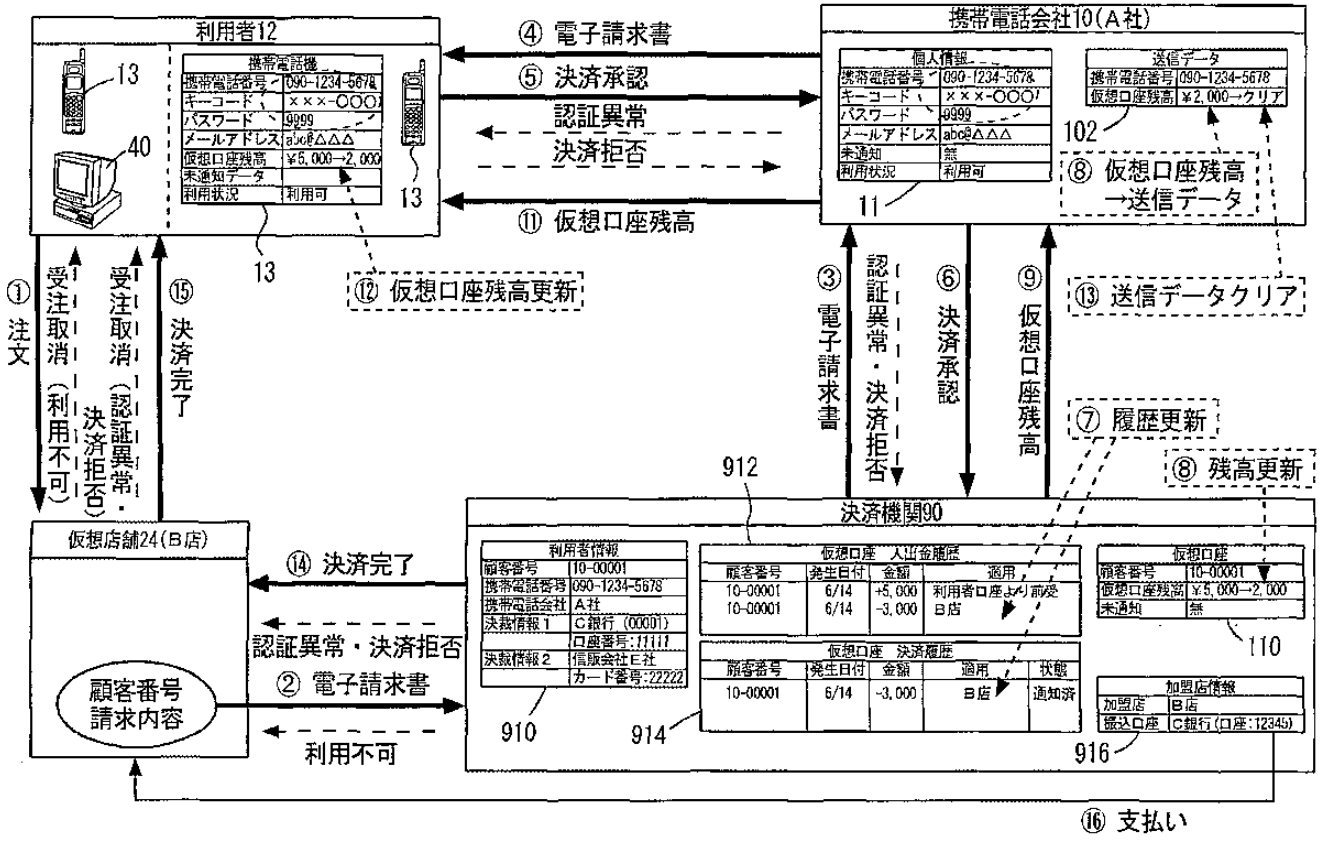
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 497 of 1360

FIG. 42



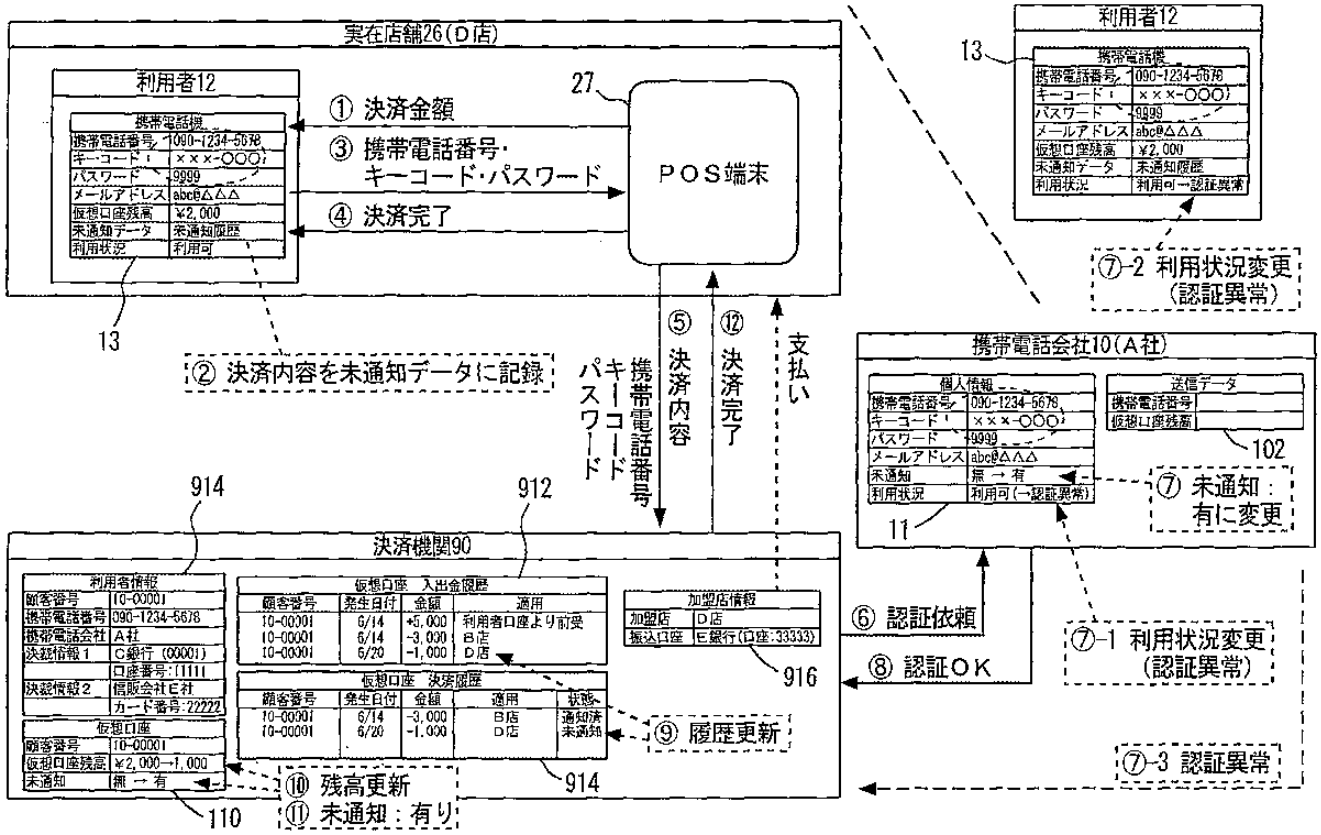
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 498 of 1360

FIG. 43



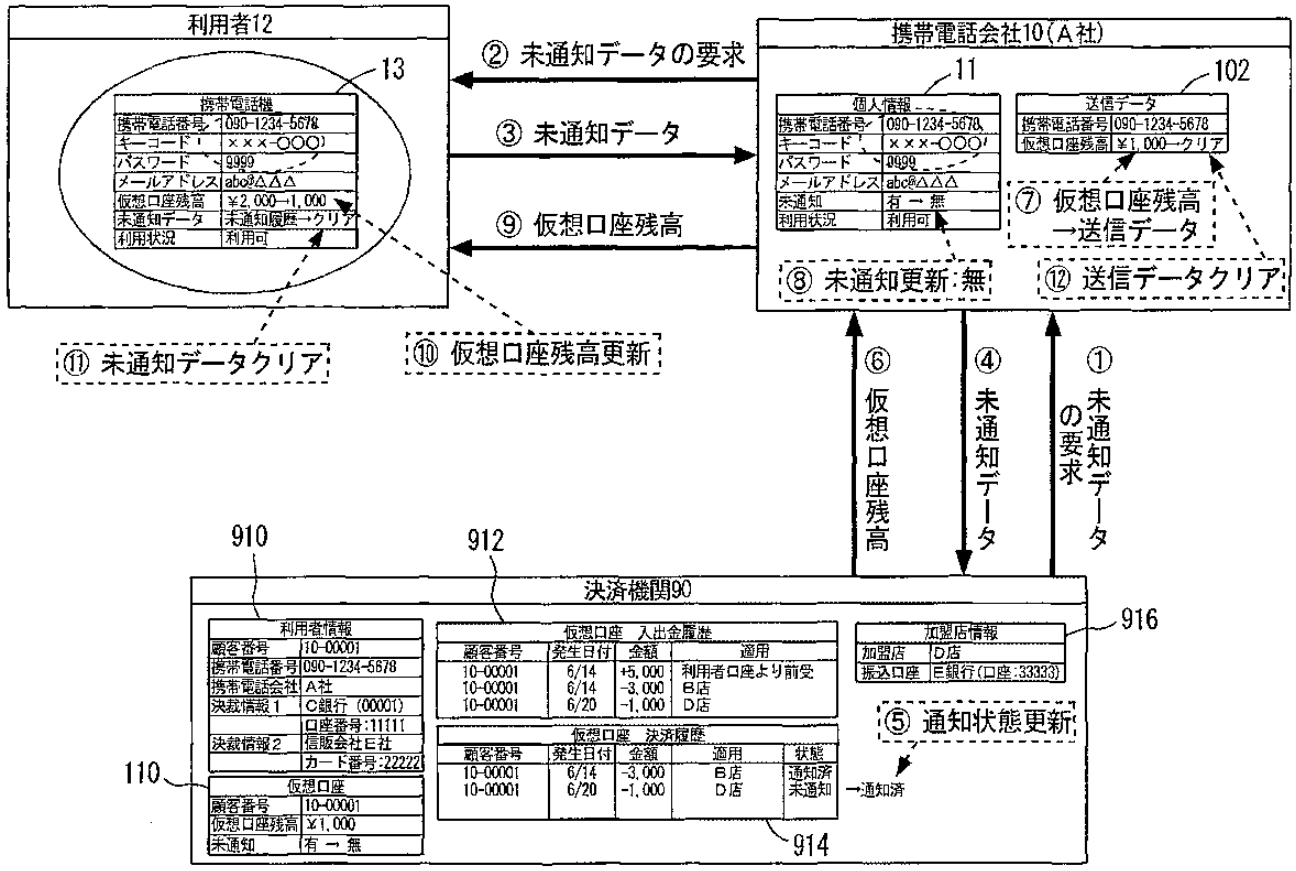
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 499 of 1360

FIG. 44



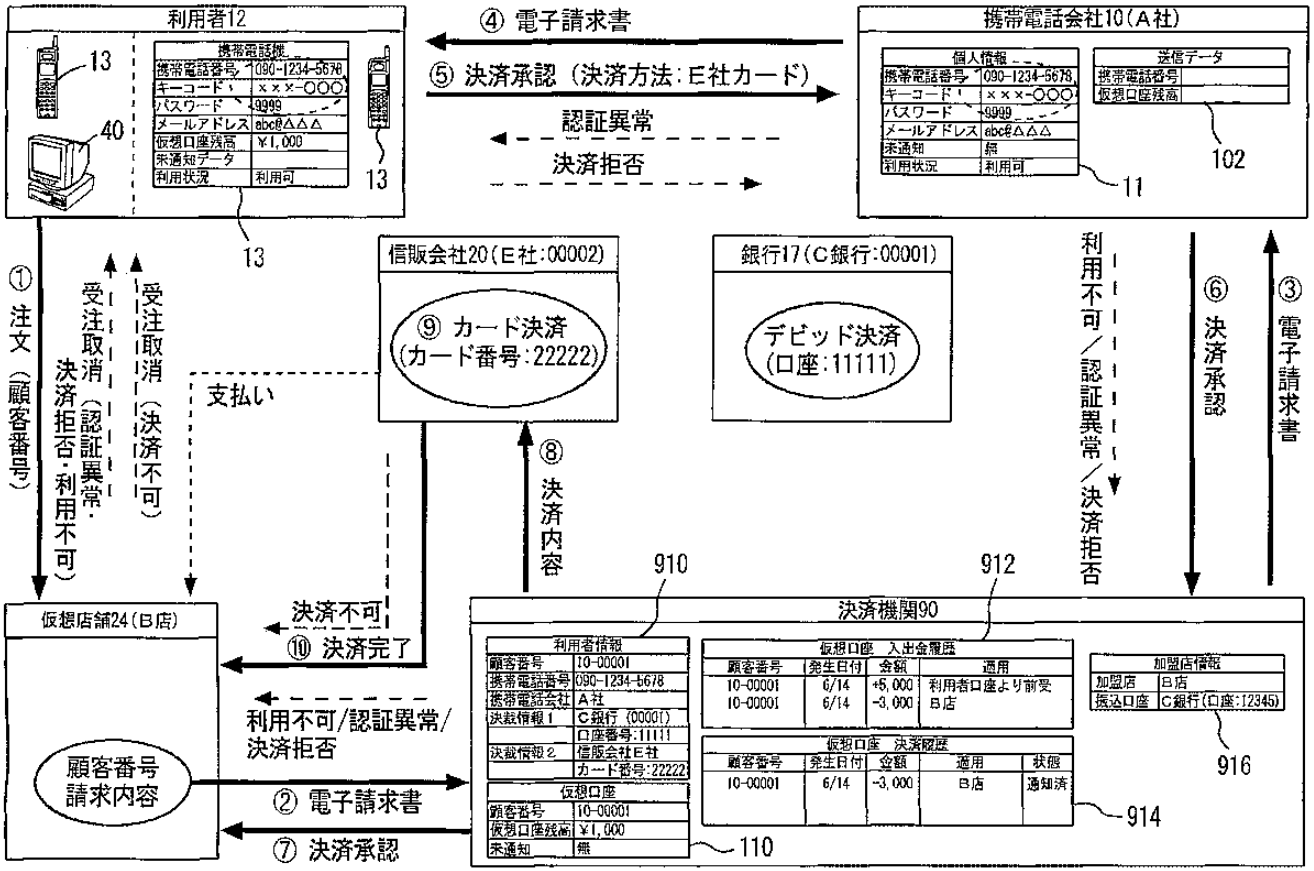
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 500 of 1360

FIG. 45



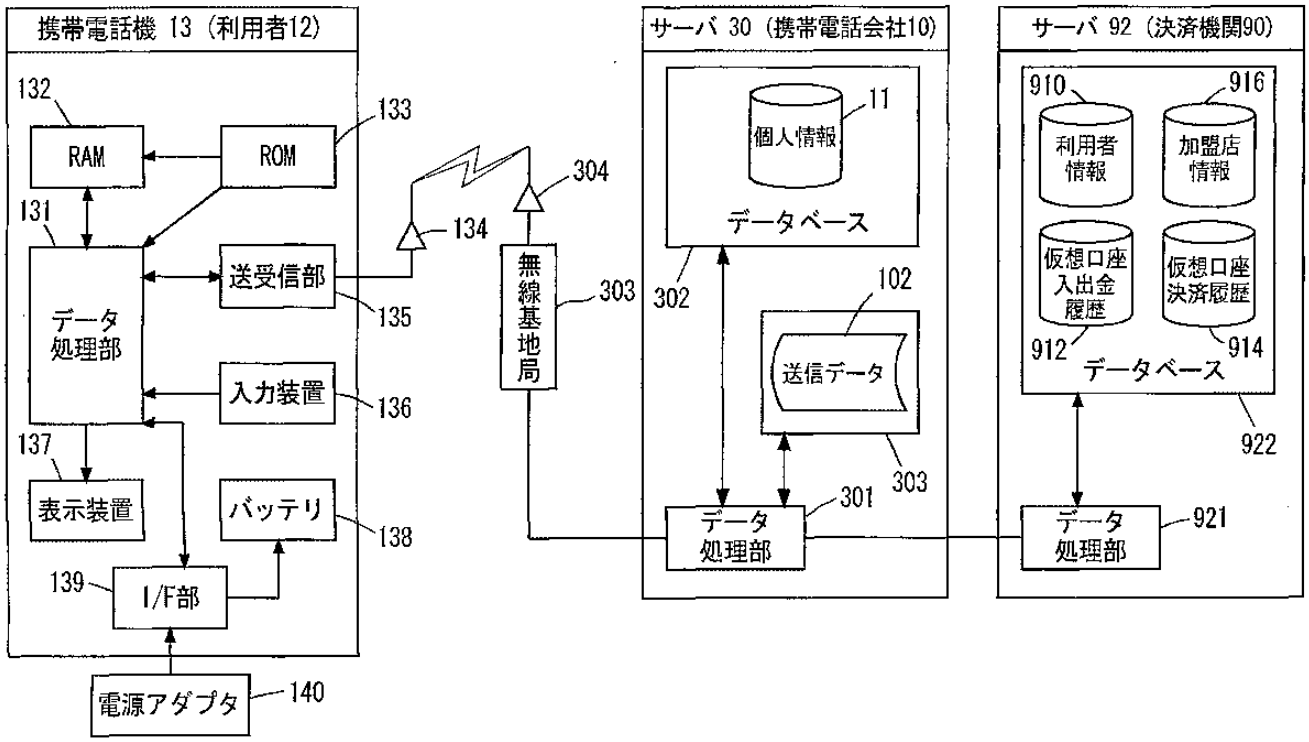
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 501 of 1360

FIG. 46



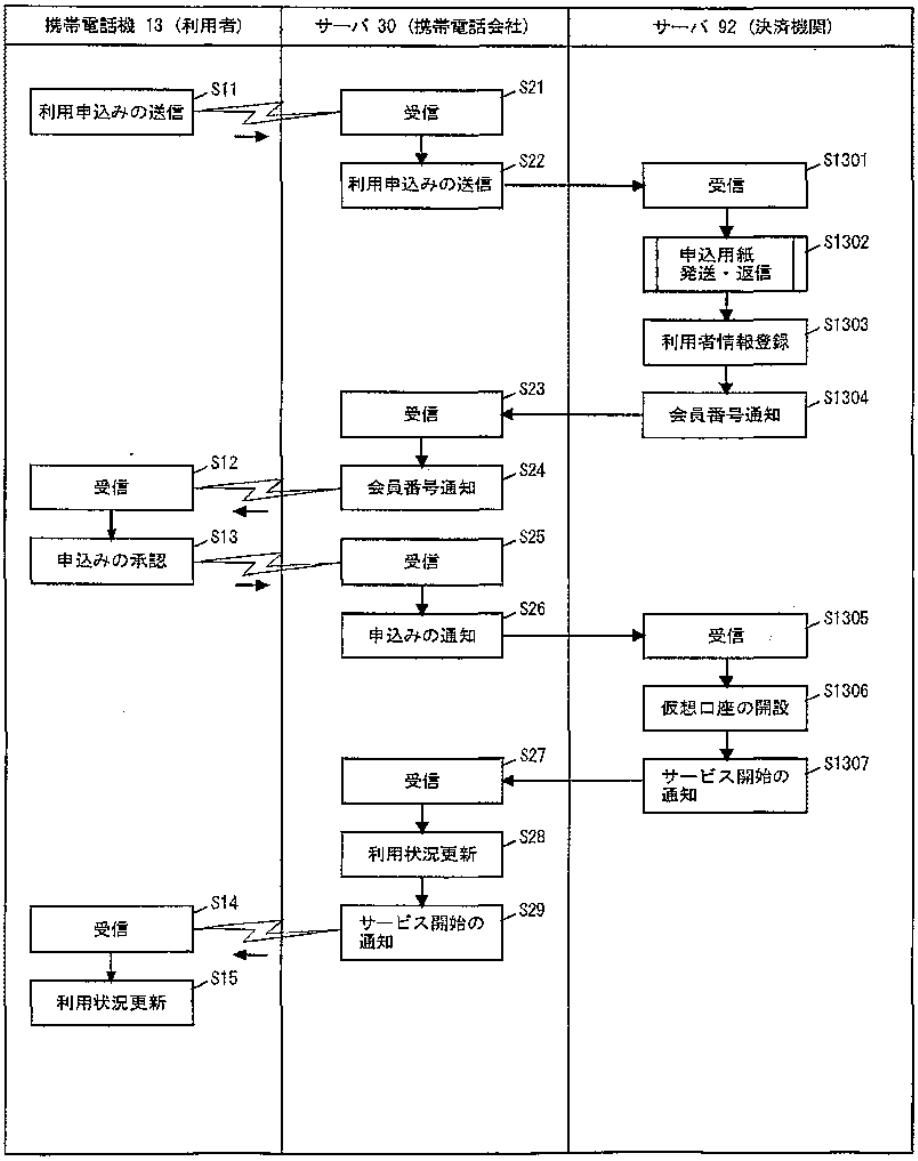
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 502 of 1360

FIG. 47



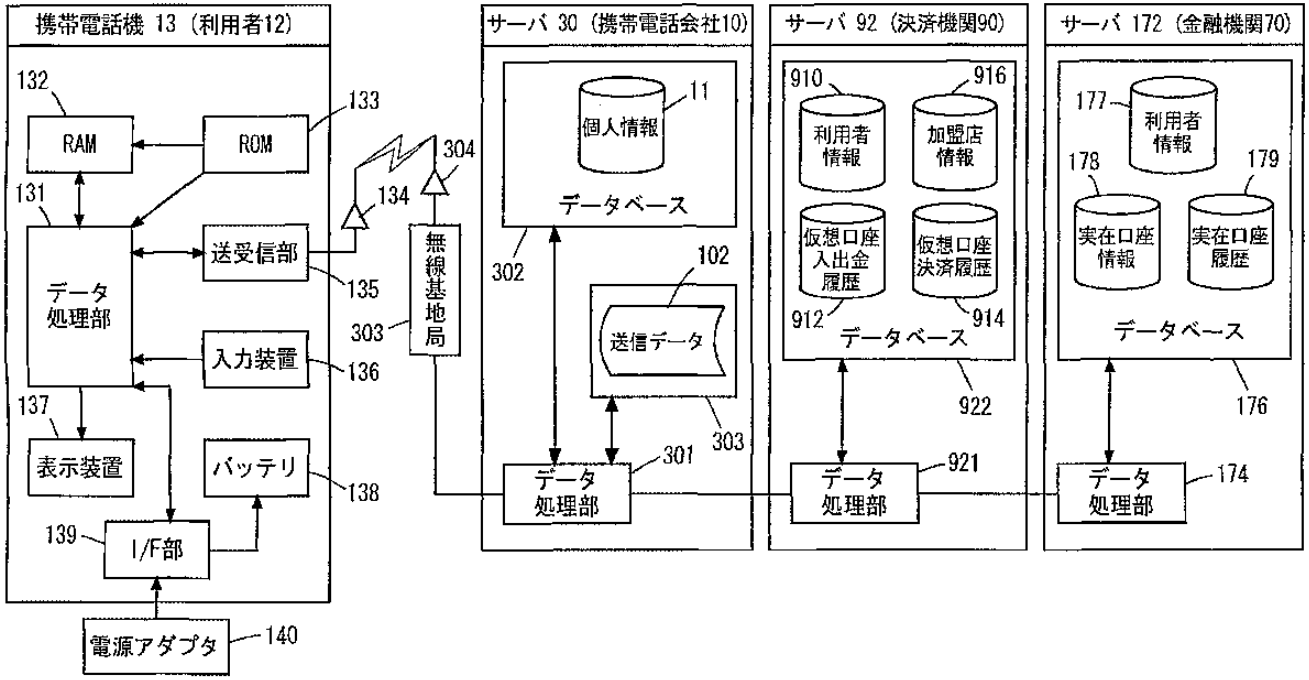
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 503 of 1360

FIG. 48



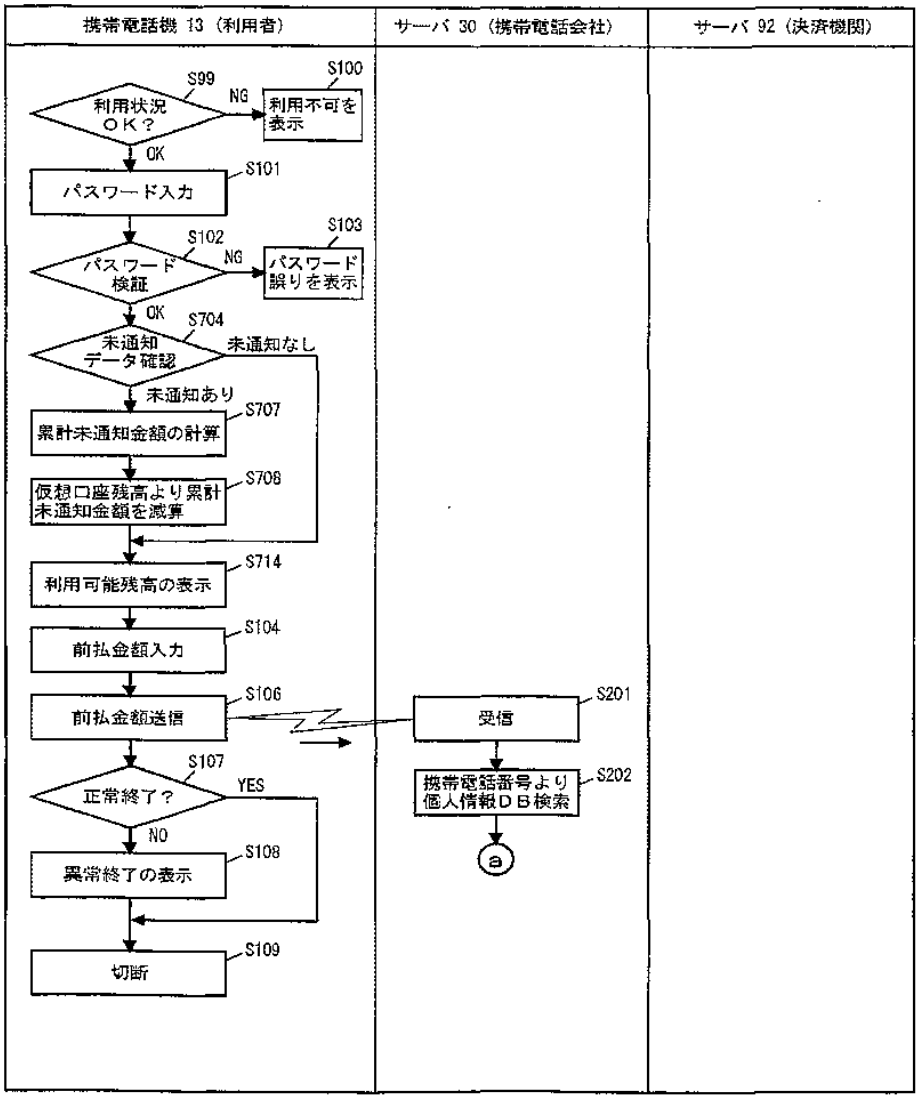
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 504 of 1360

FIG. 49



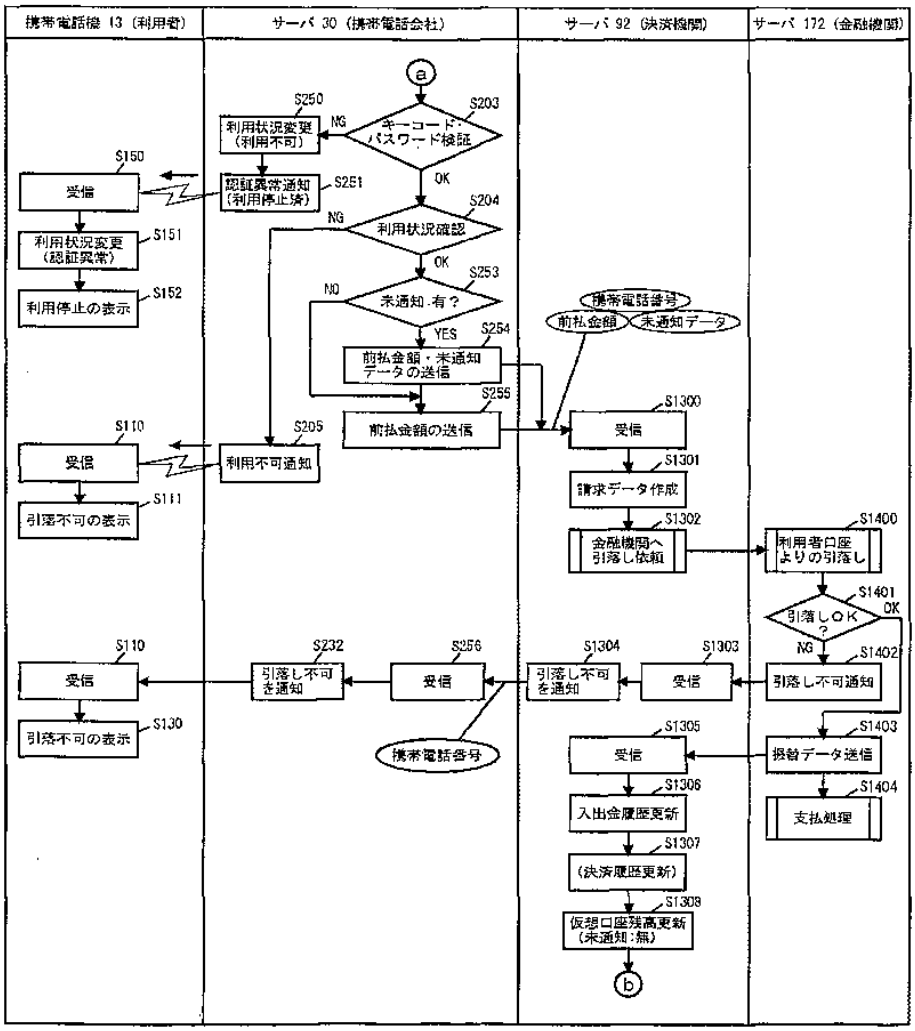
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 505 of 1360

FIG. 50



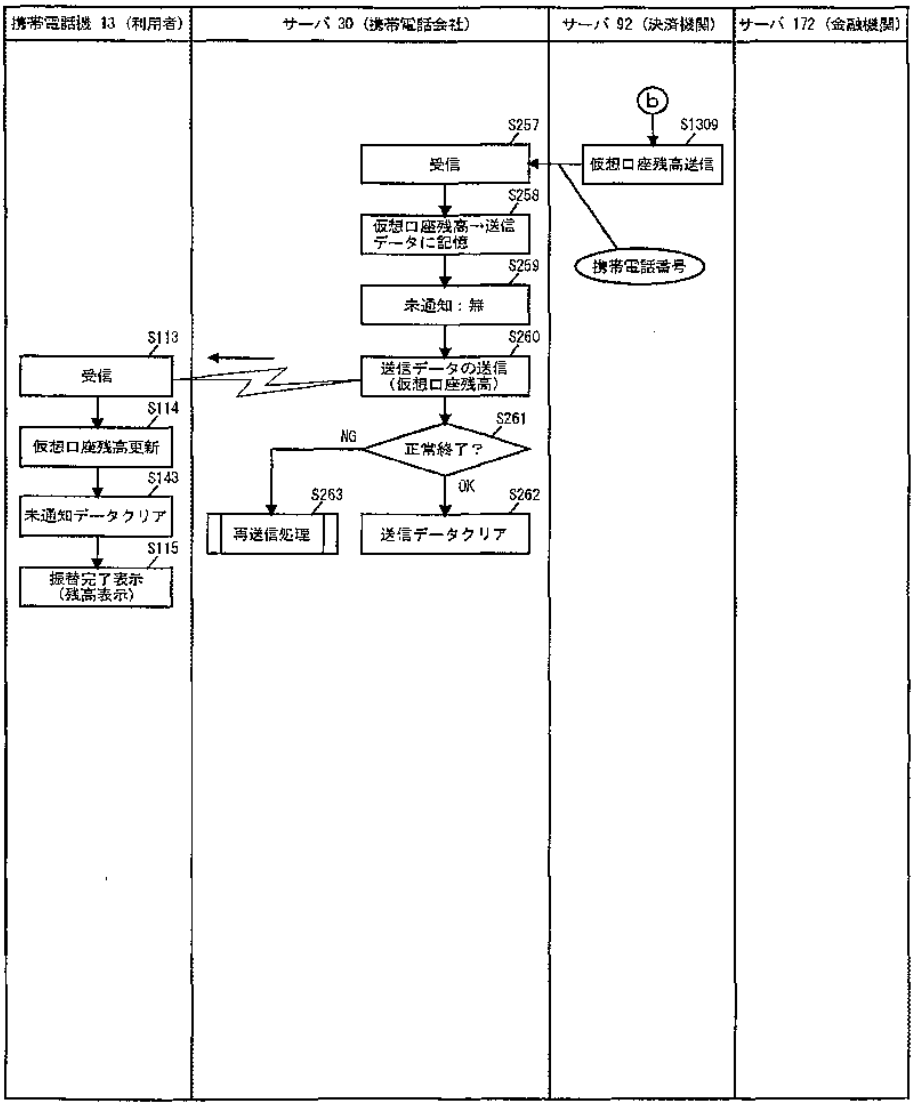
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 506 of 1360

FIG. 51



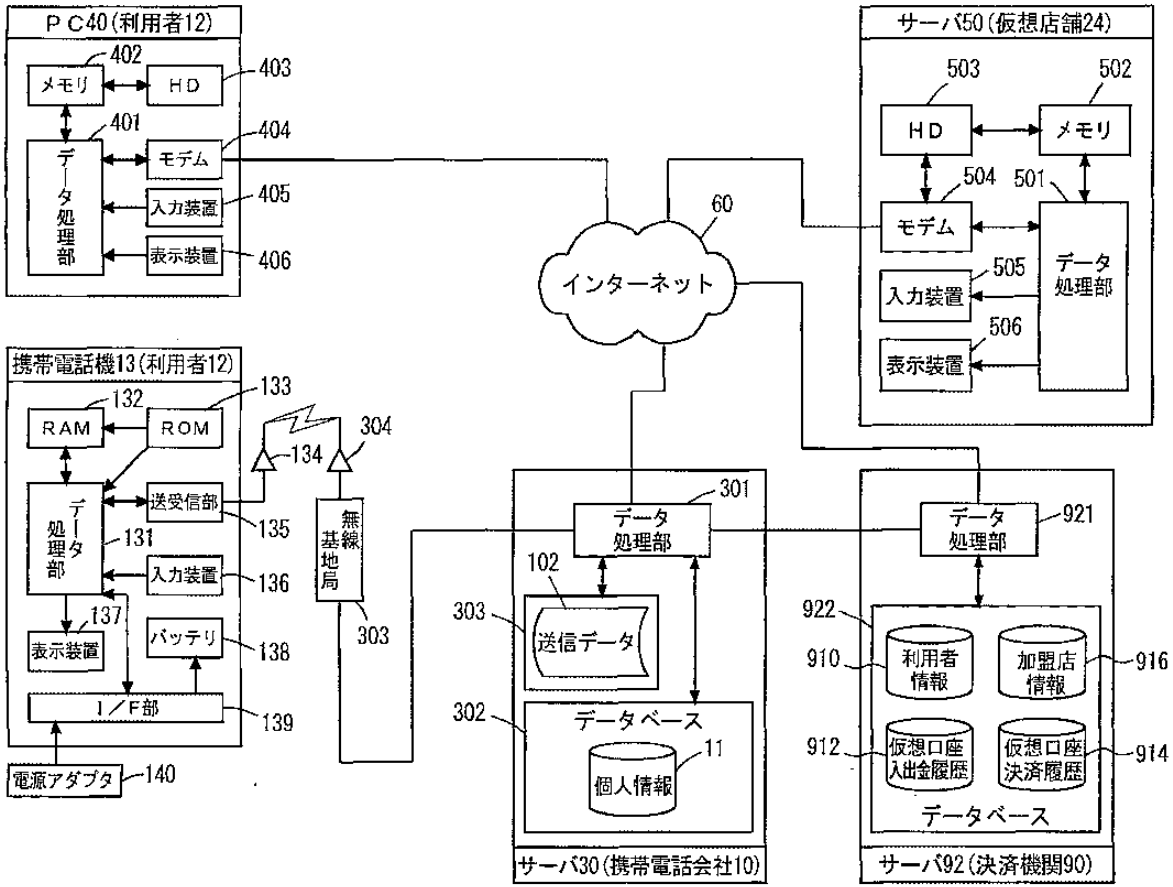
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 507 of 1360

FIG. 52



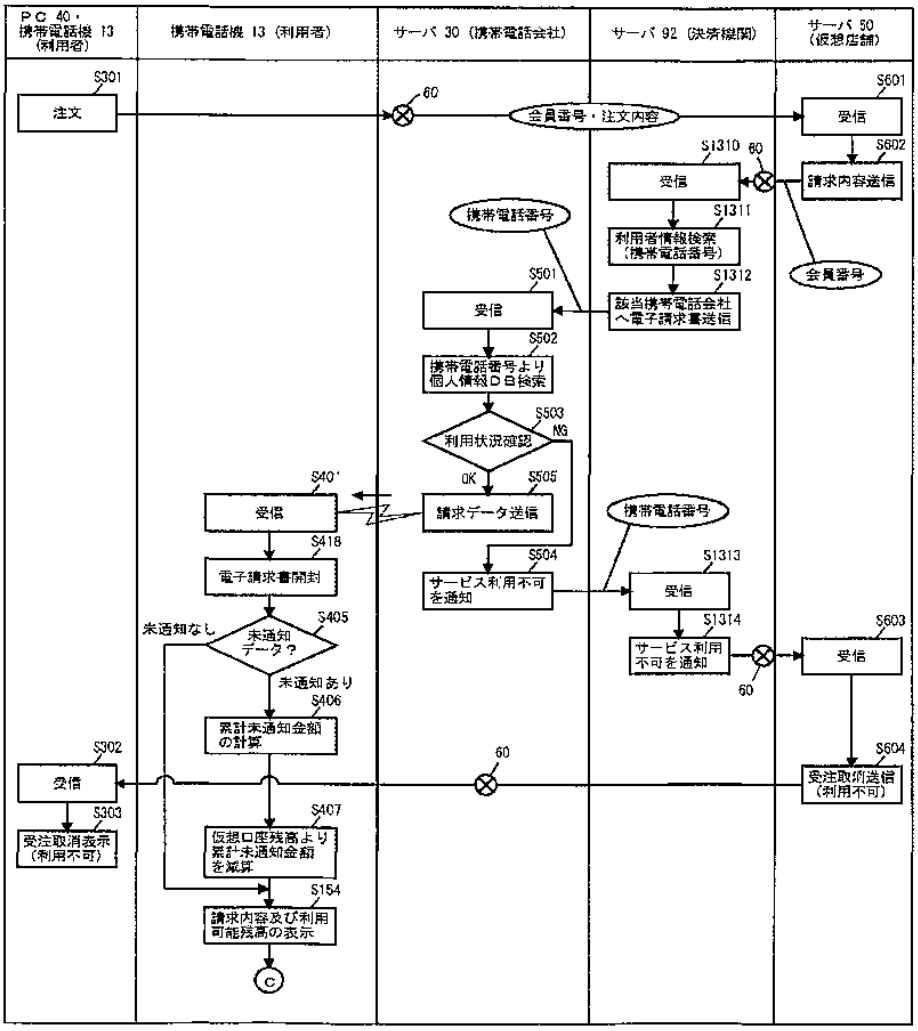
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 508 of 1360

FIG. 53



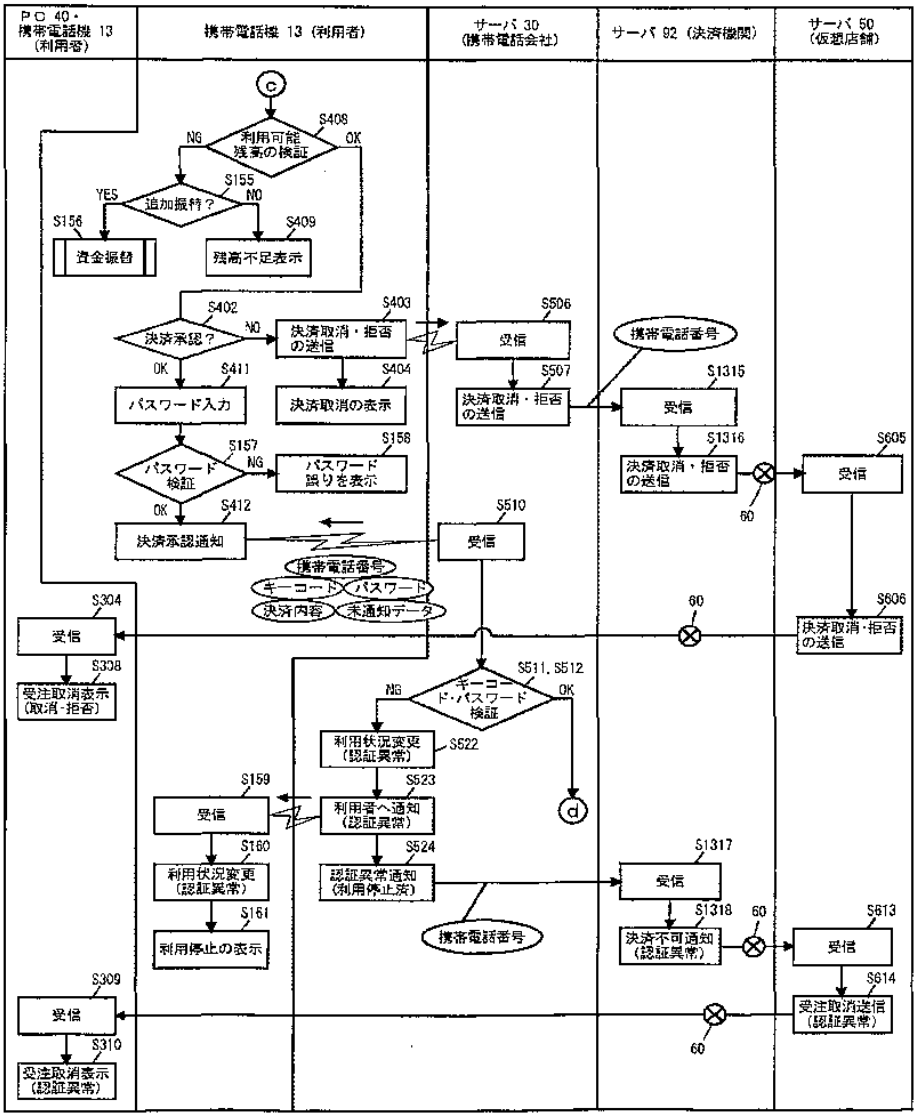
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 509 of 1360

FIG. 54



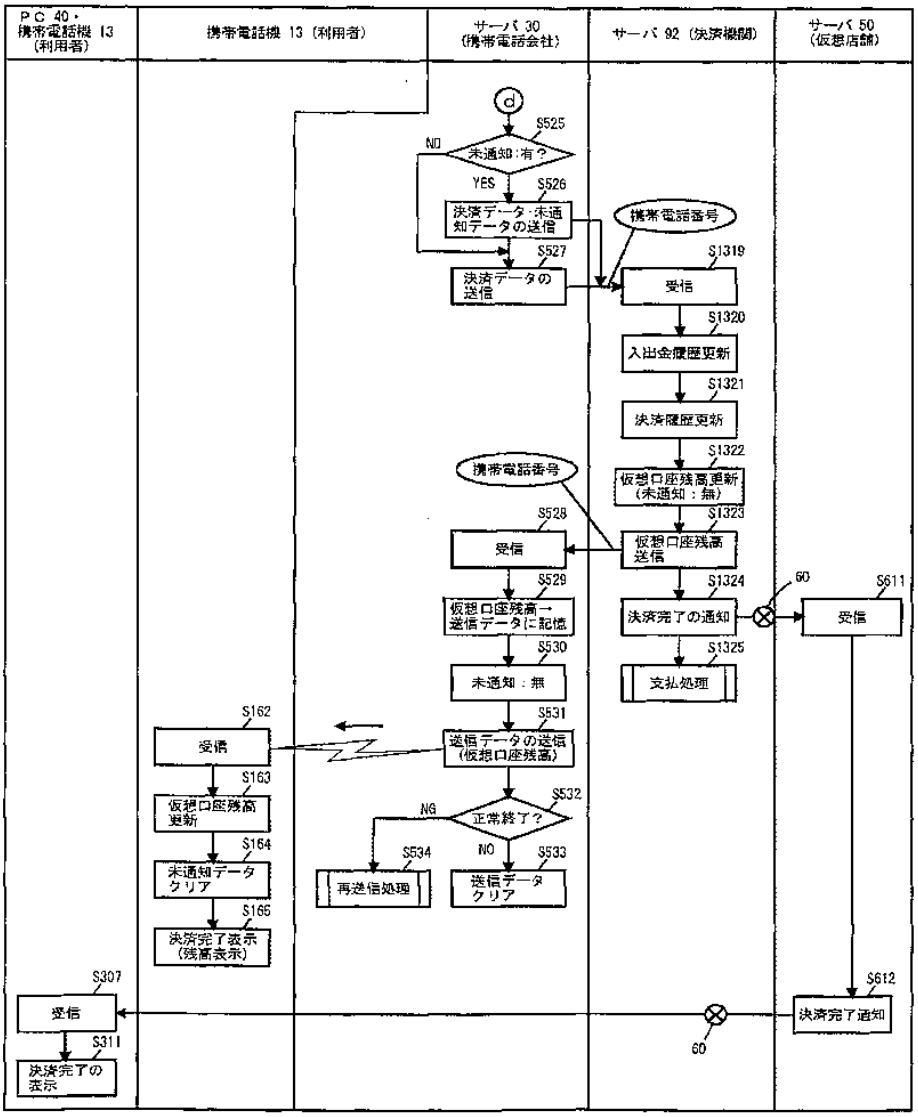
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 510 of 1360

FIG. 55



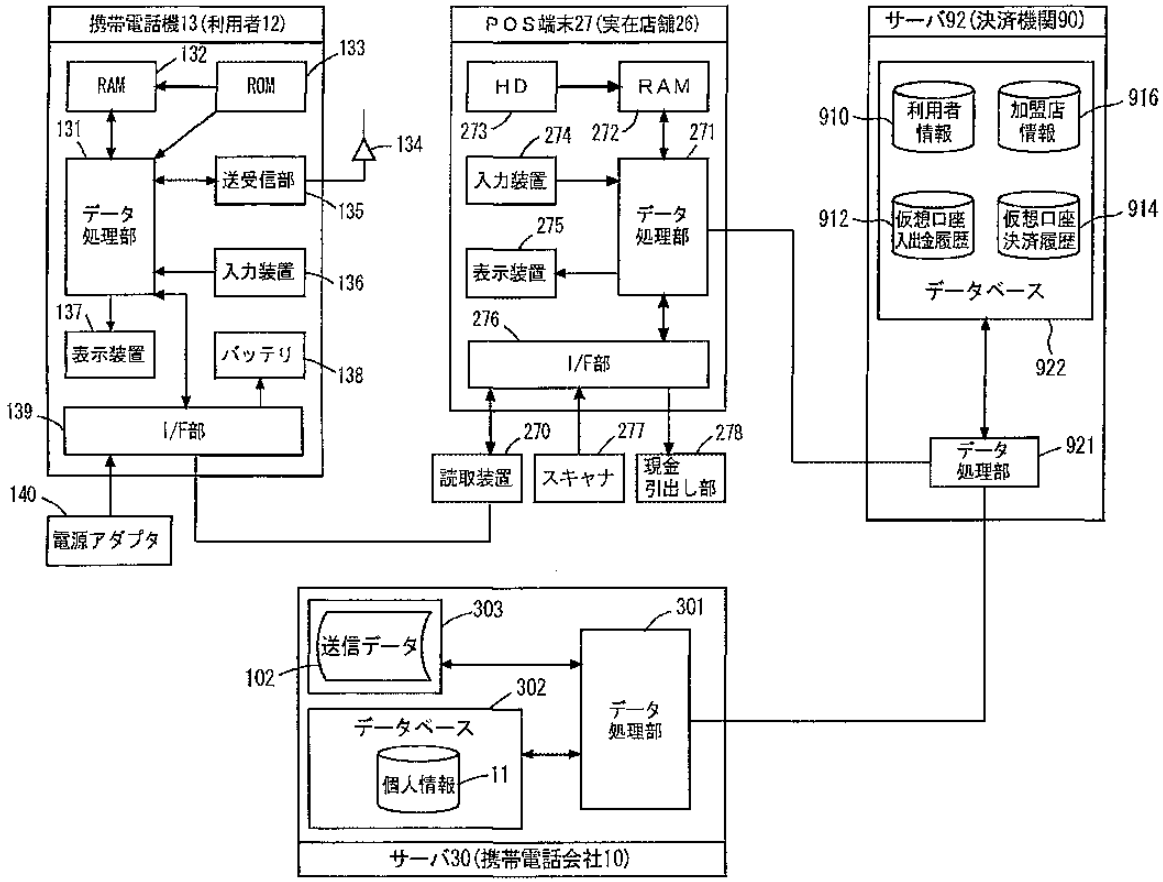
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 511 of 1360

FIG. 56



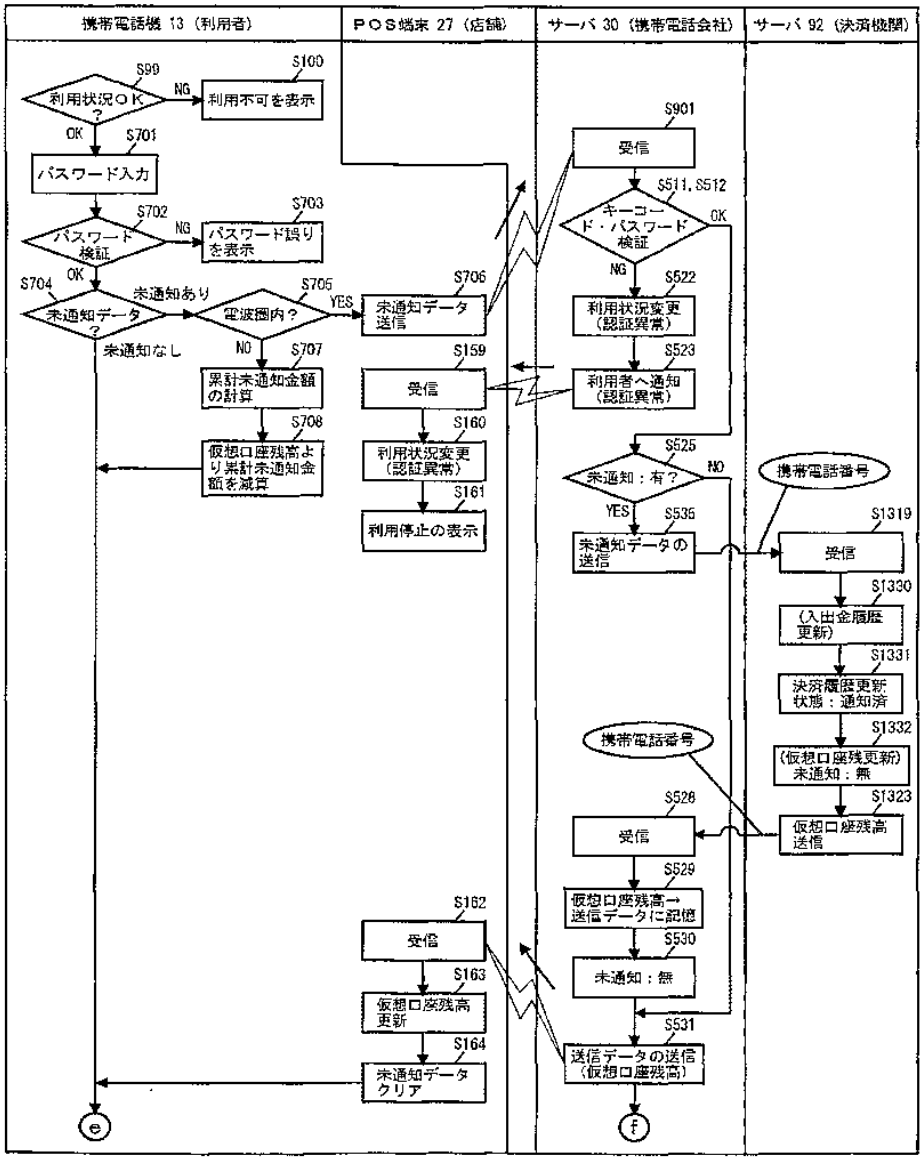
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 512 of 1360

FIG. 57



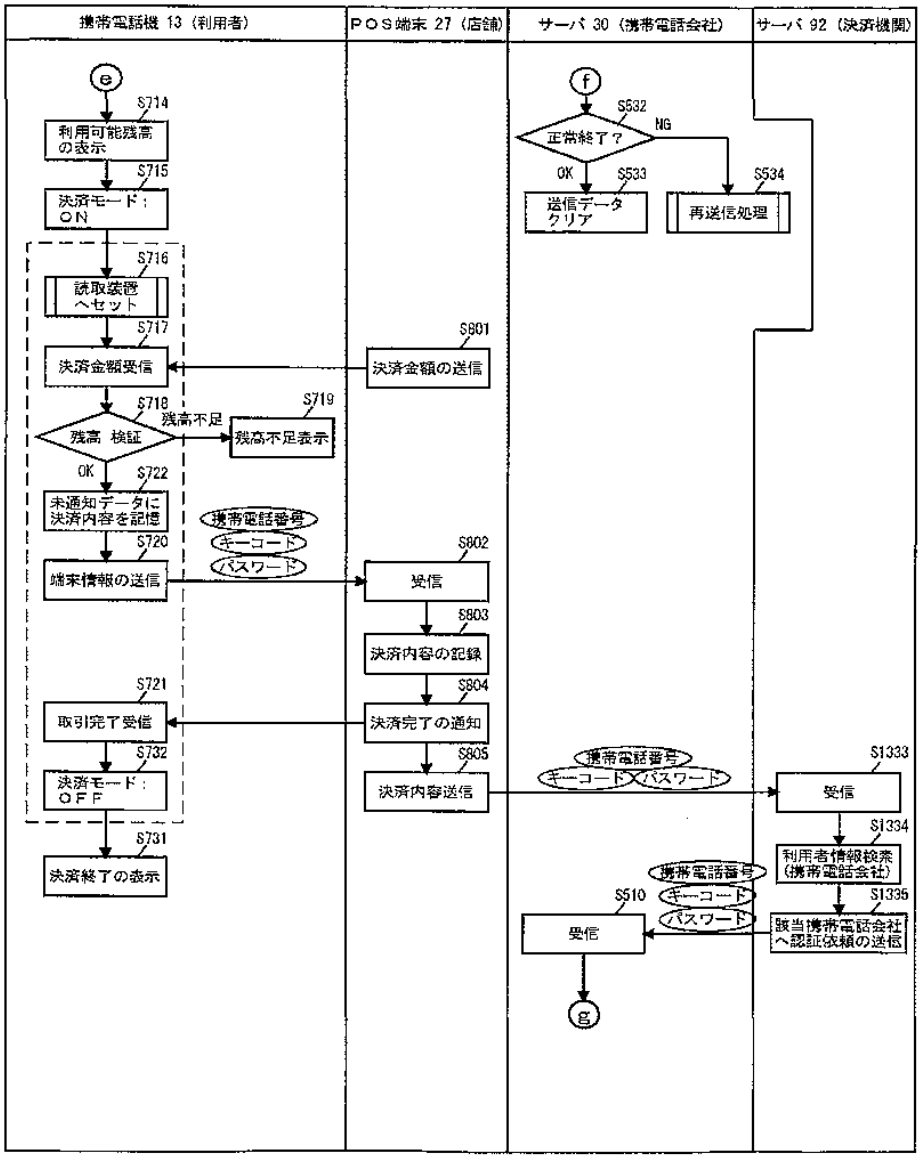
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 513 of 1360

FIG. 58



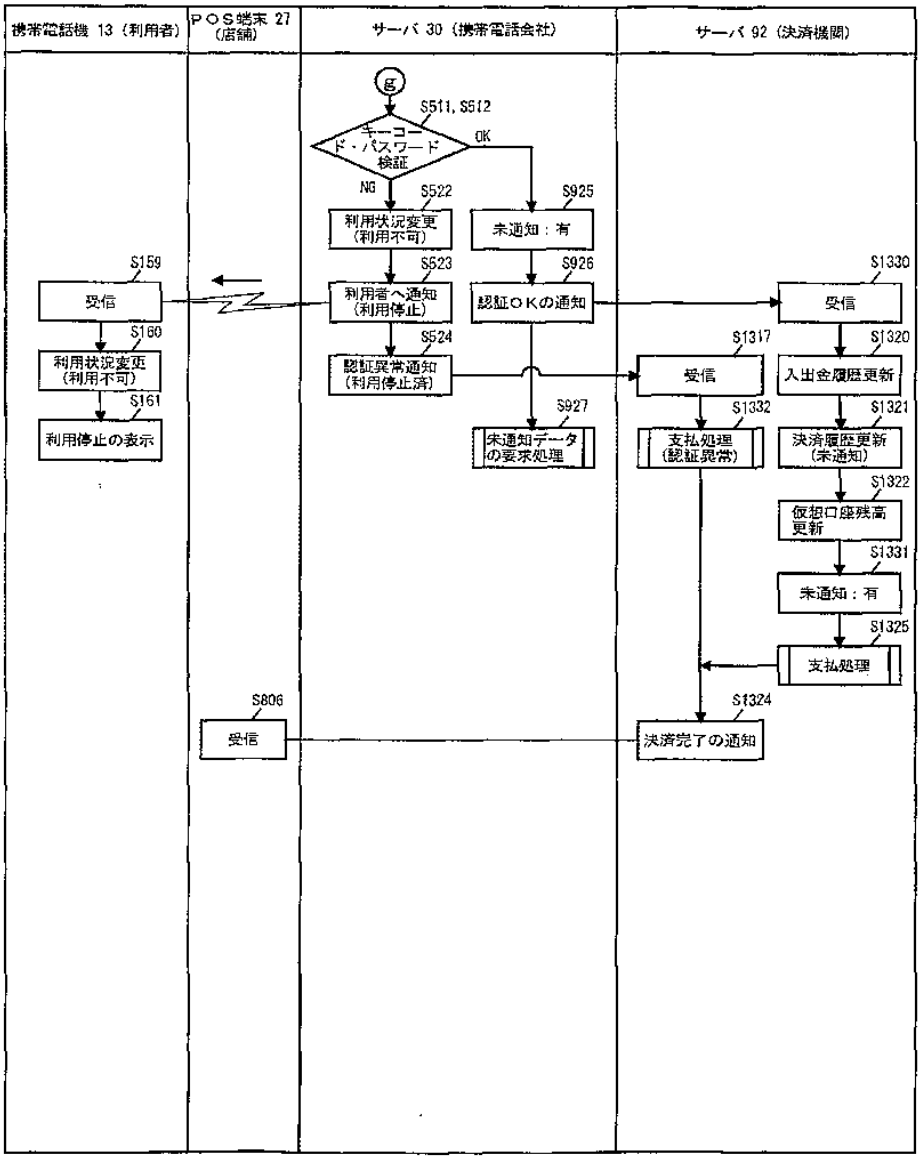
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 514 of 1360

FIG. 59



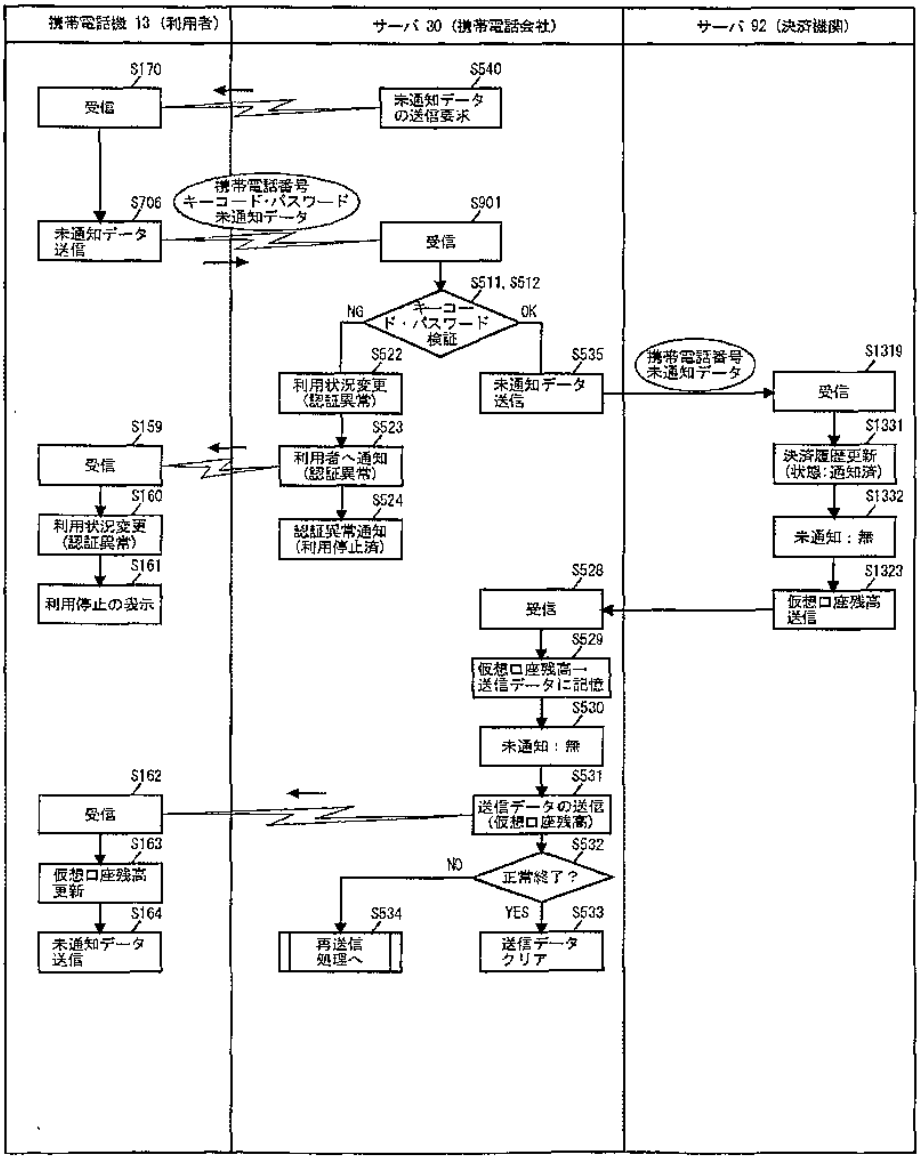
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 515 of 1360

FIG. 60



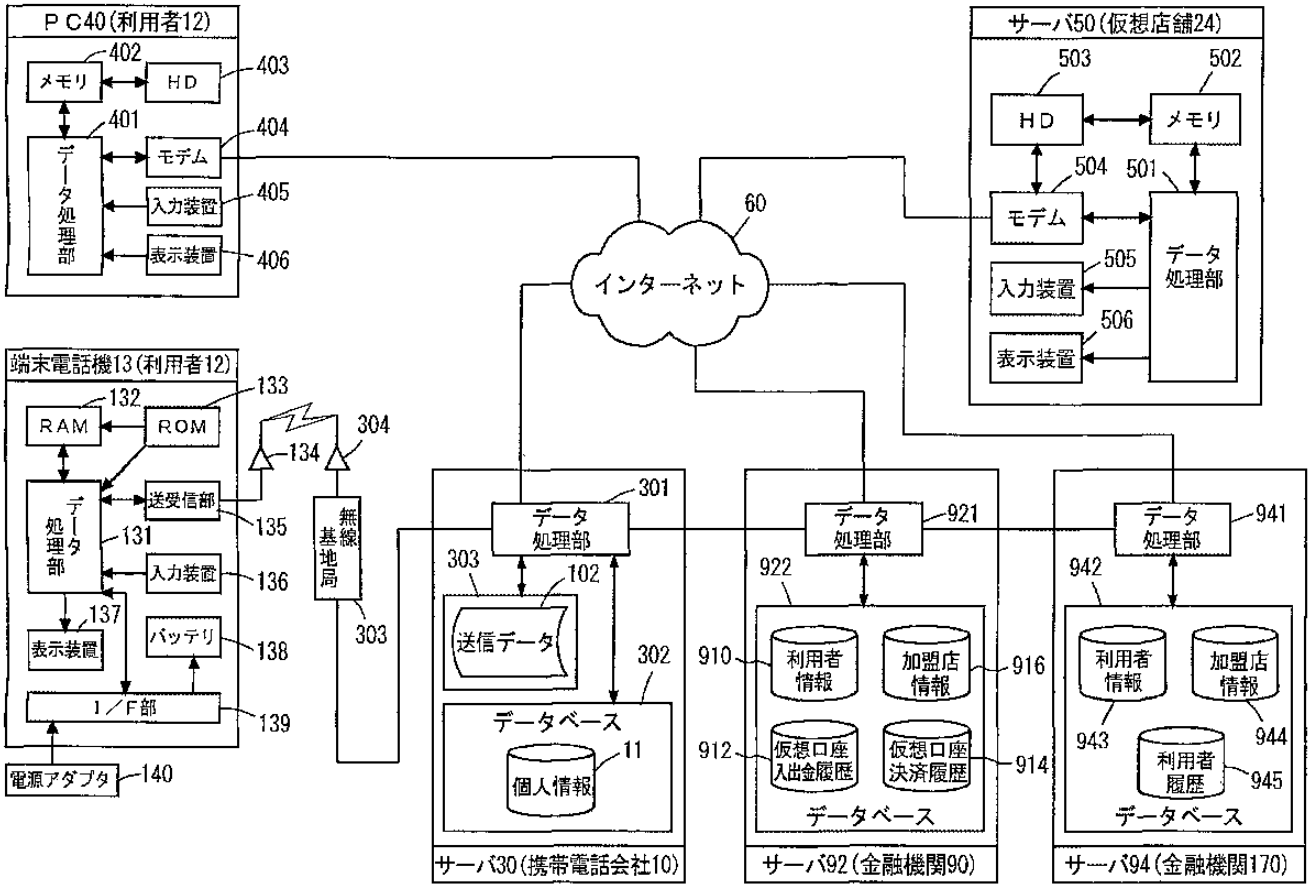
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 516 of 1360

FIG. 61



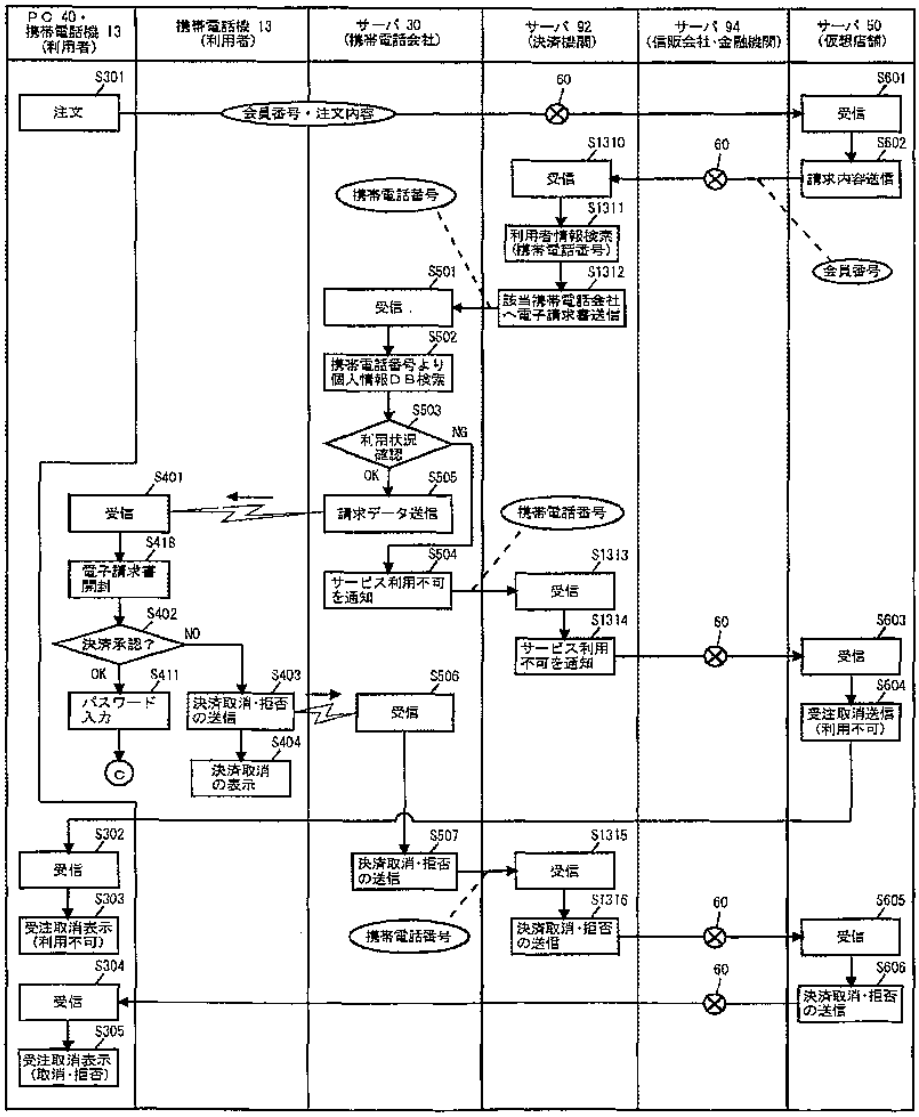
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 517 of 1360

FIG. 62



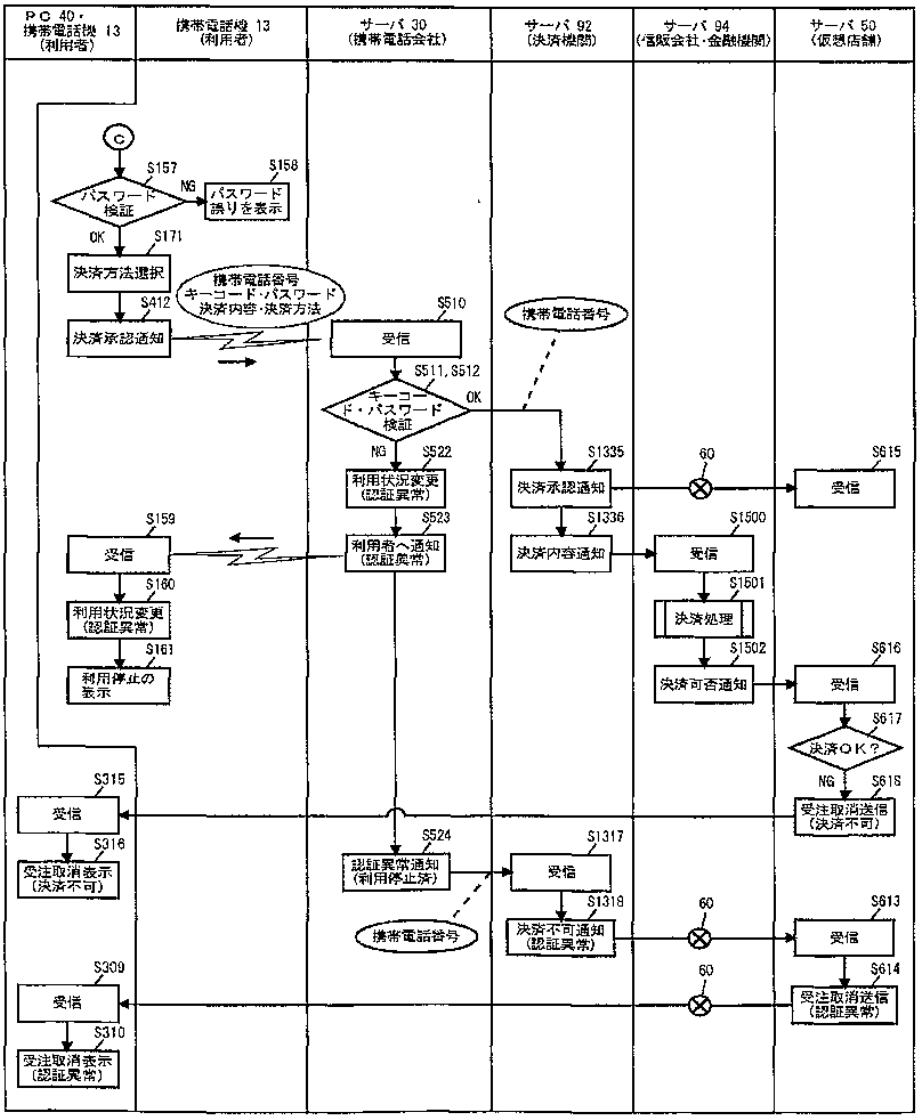
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 518 of 1360

FIG. 63



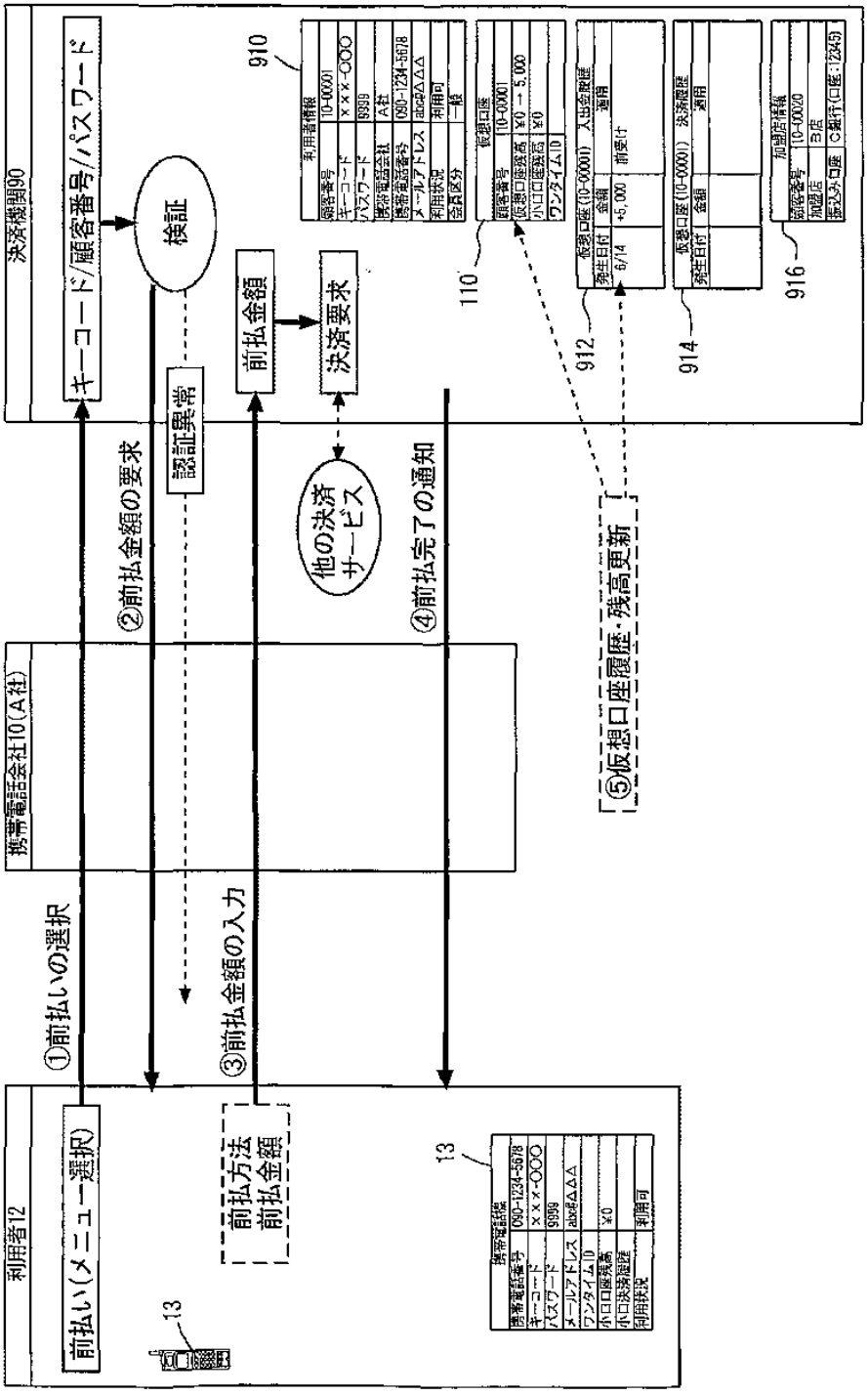
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 519 of 1360

FIG. 64



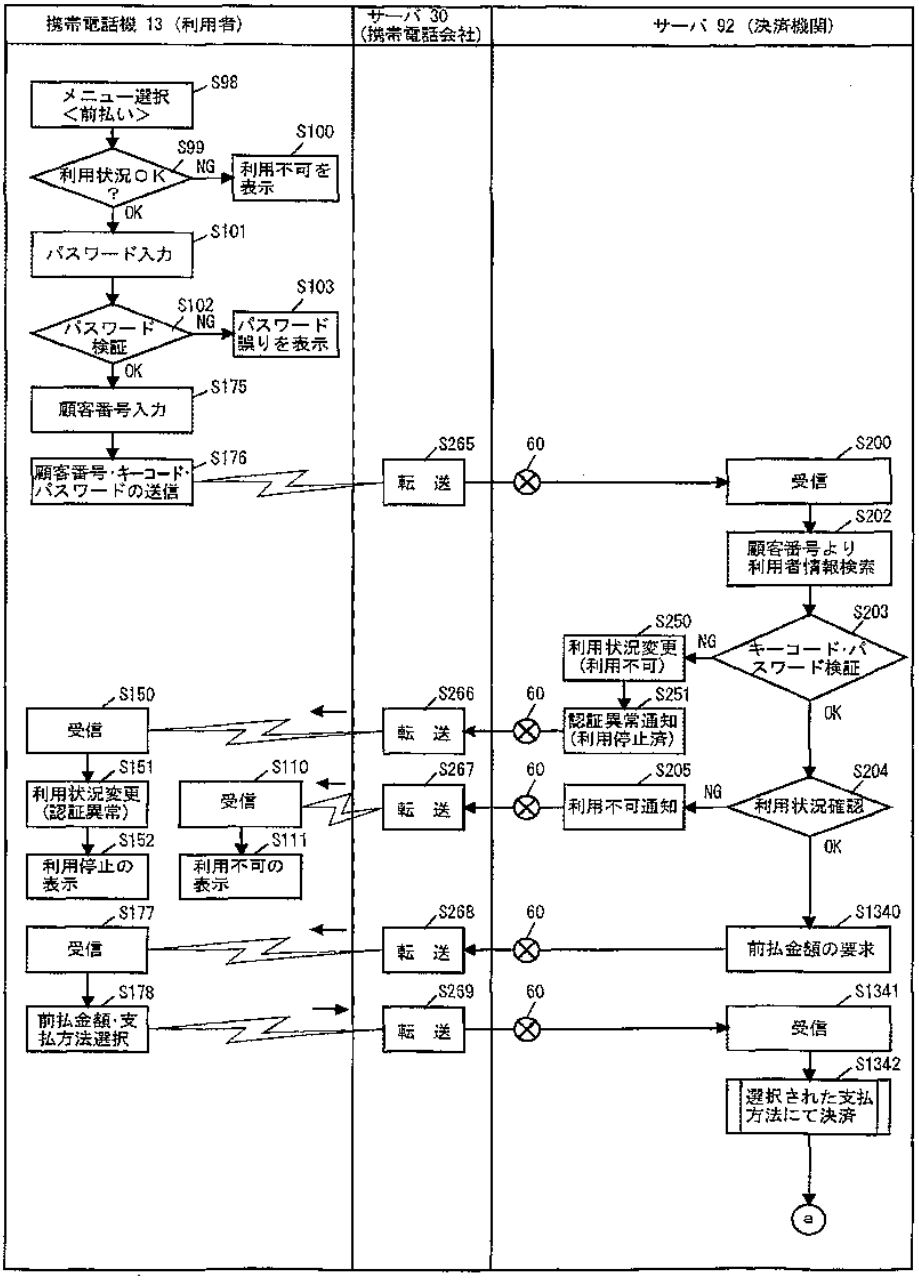
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 520 of 1360

FIG. 65



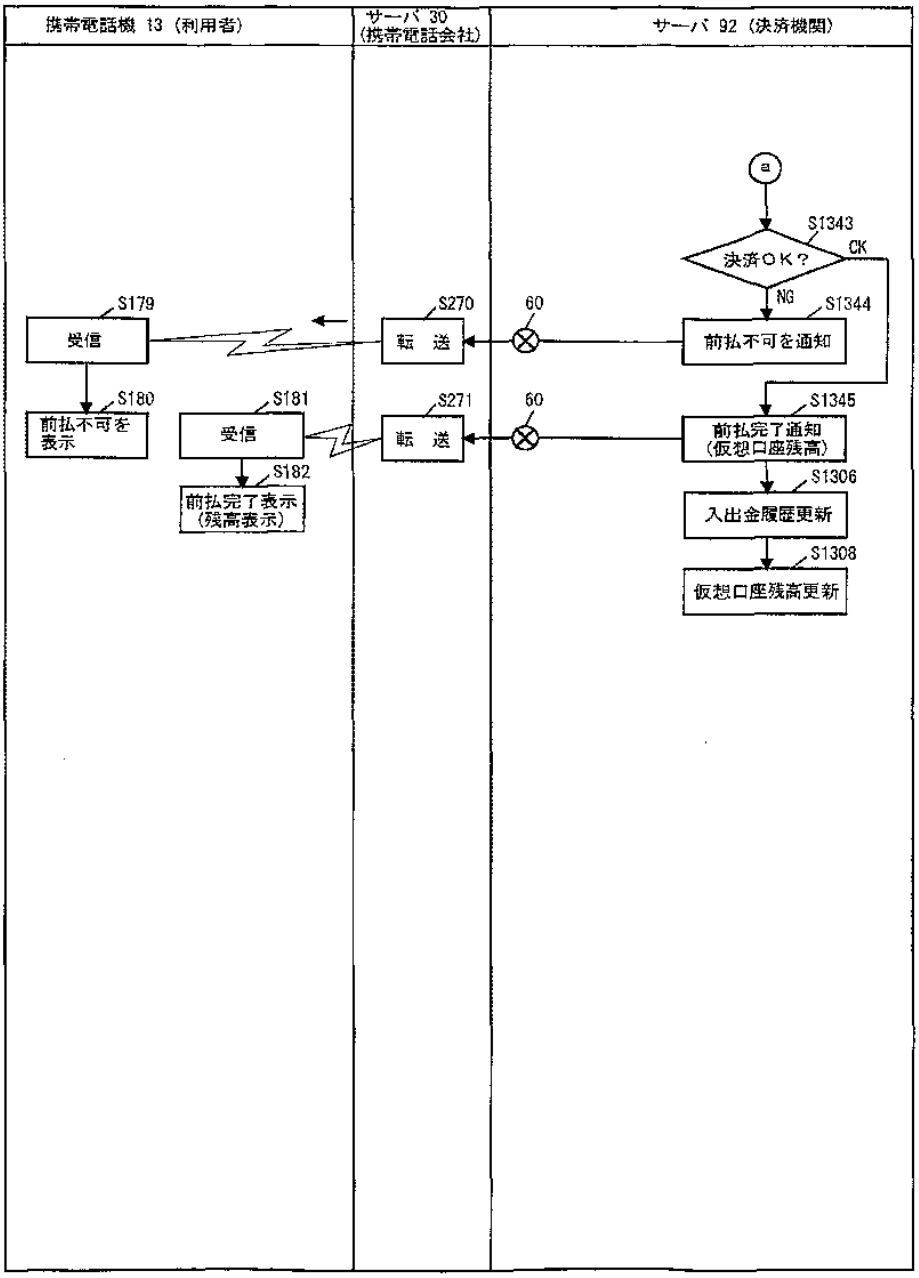
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 521 of 1360

FIG. 66



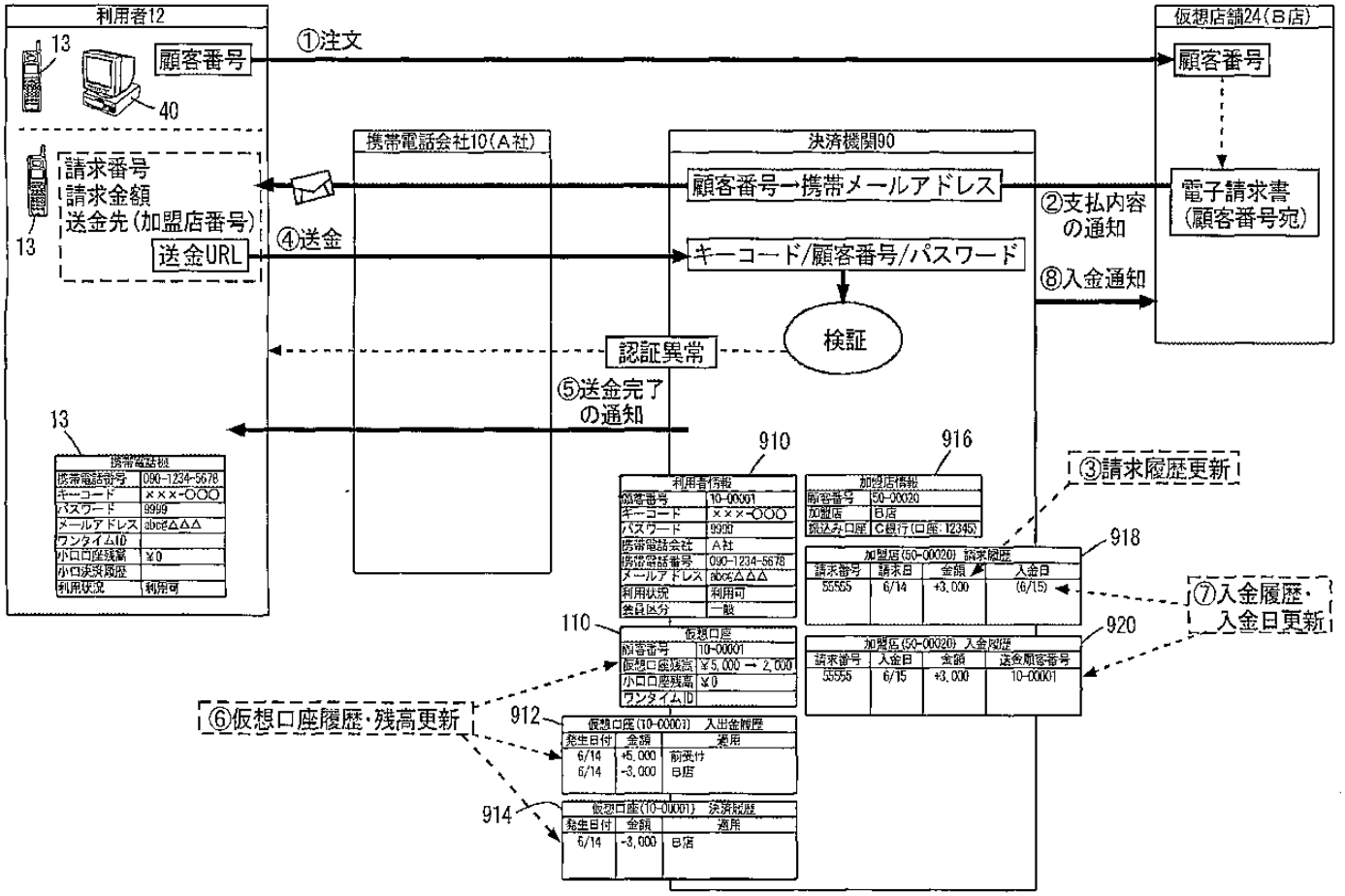
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 522 of 1360

FIG. 67



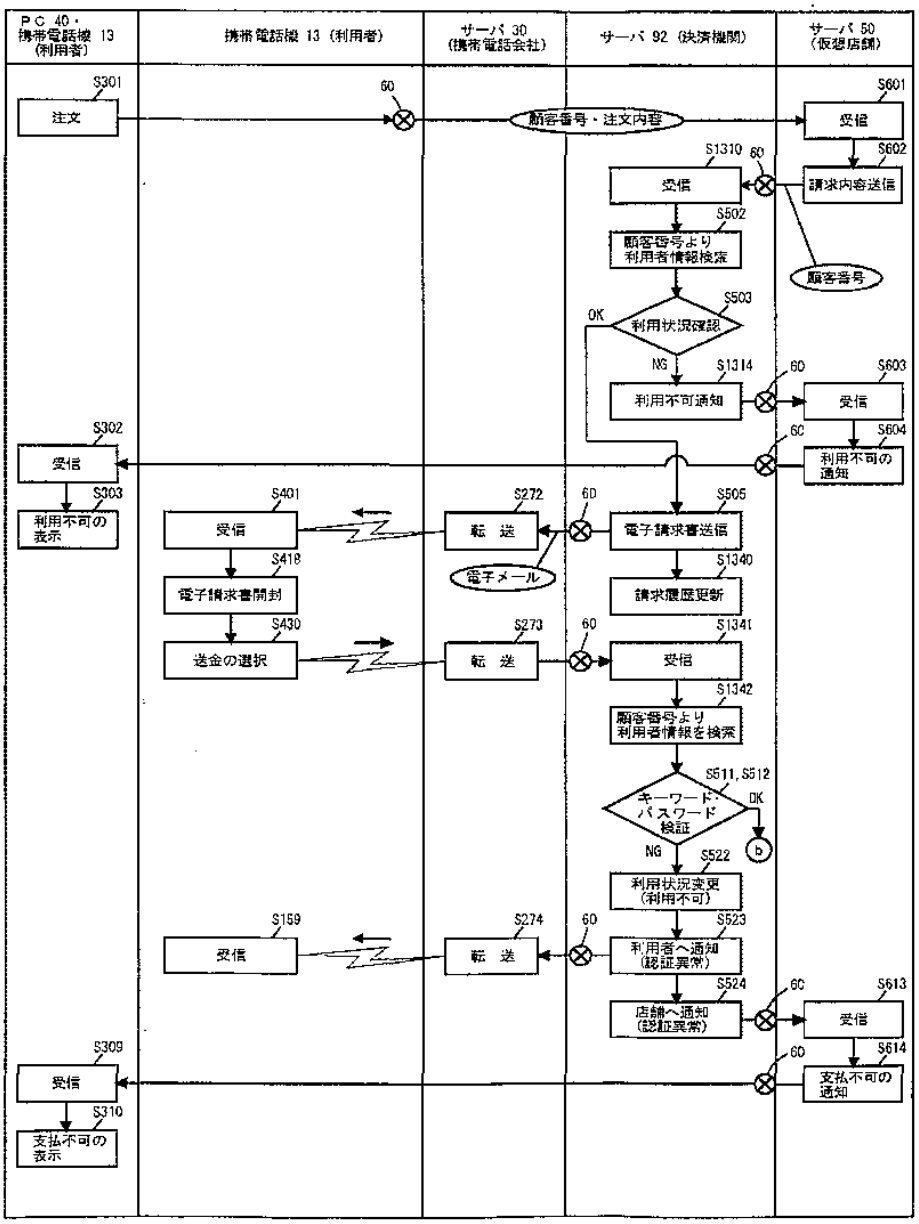
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 523 of 1360

FIG. 68



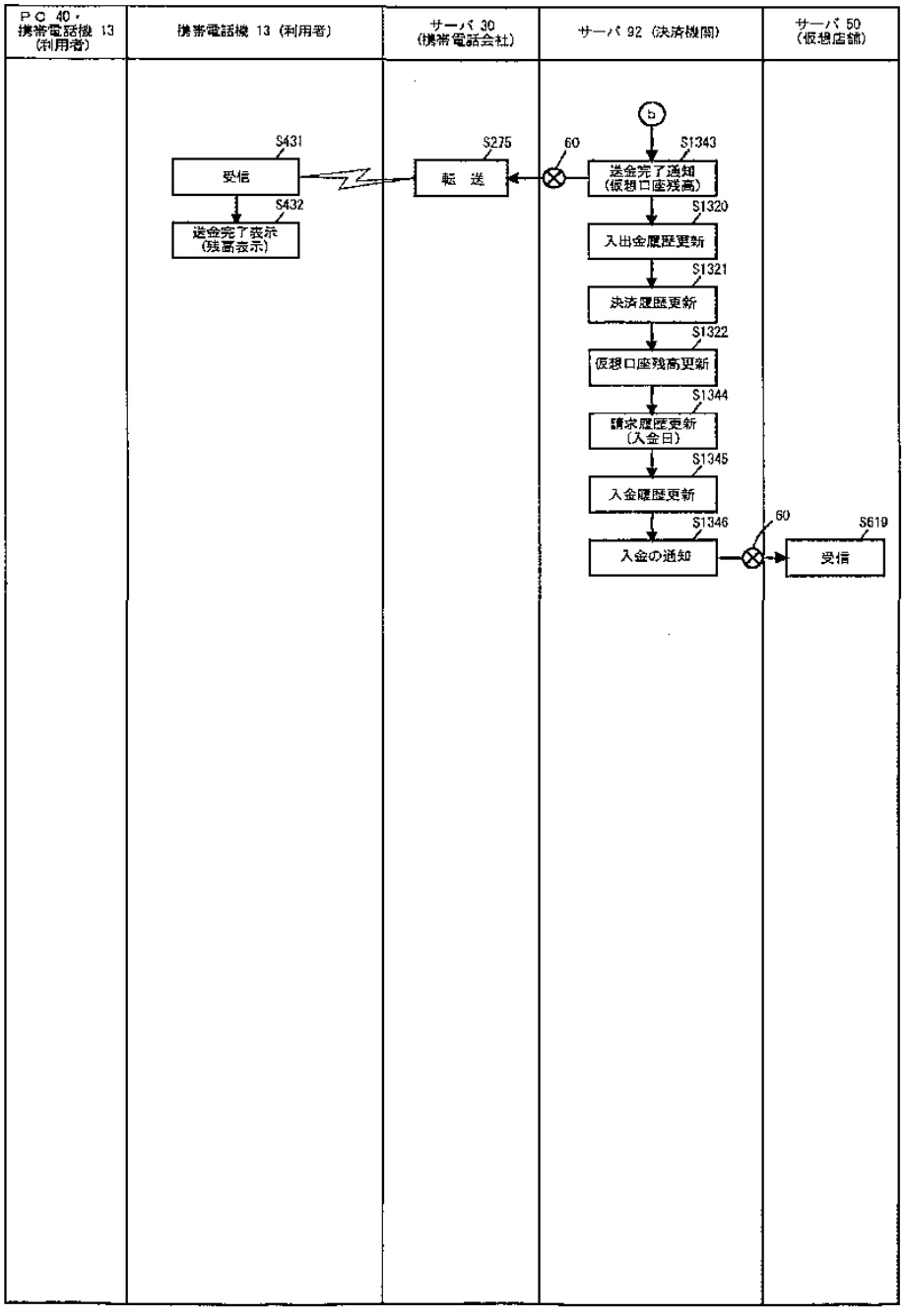
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 524 of 1360

FIG. 69



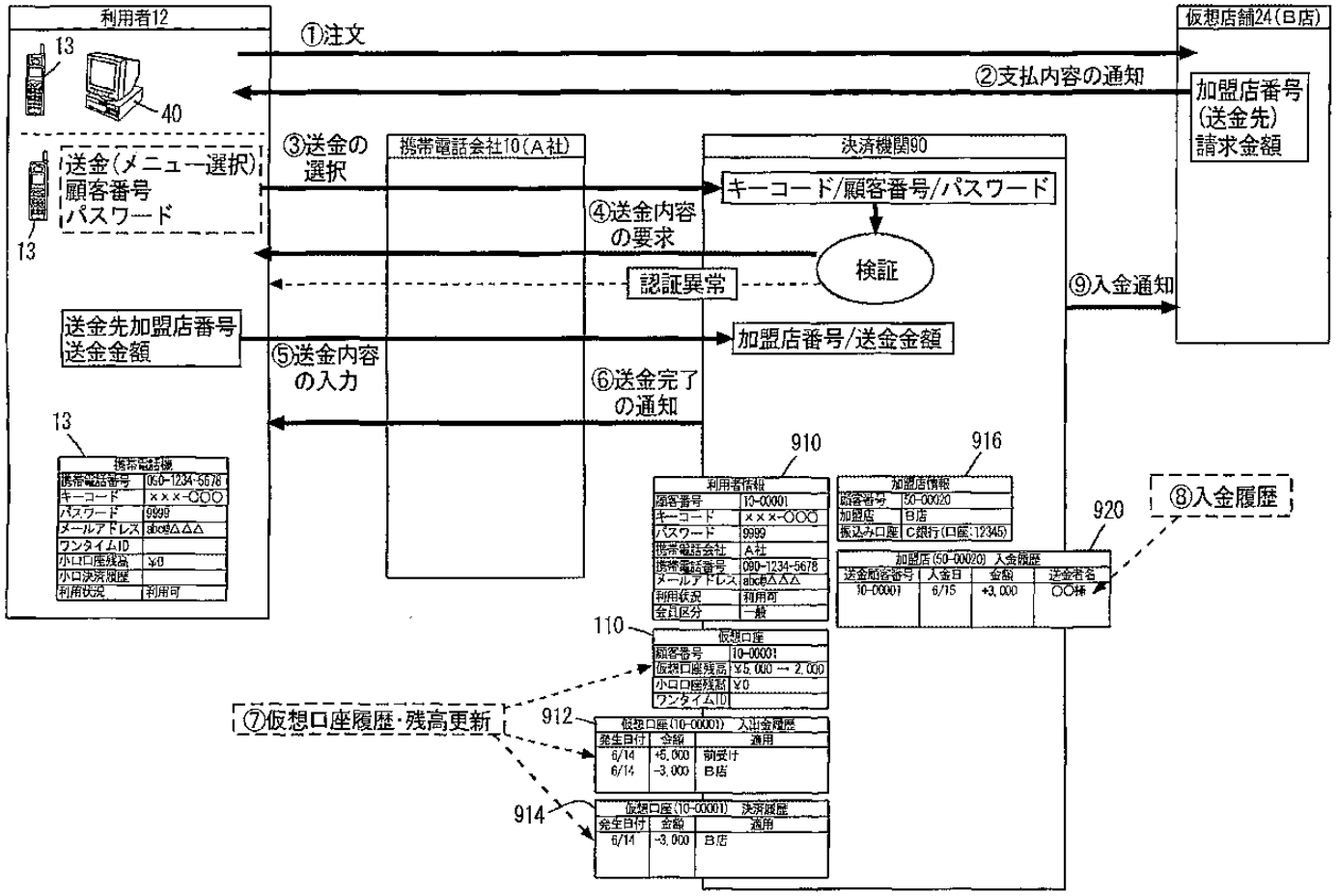
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 525 of 1360

FIG. 70



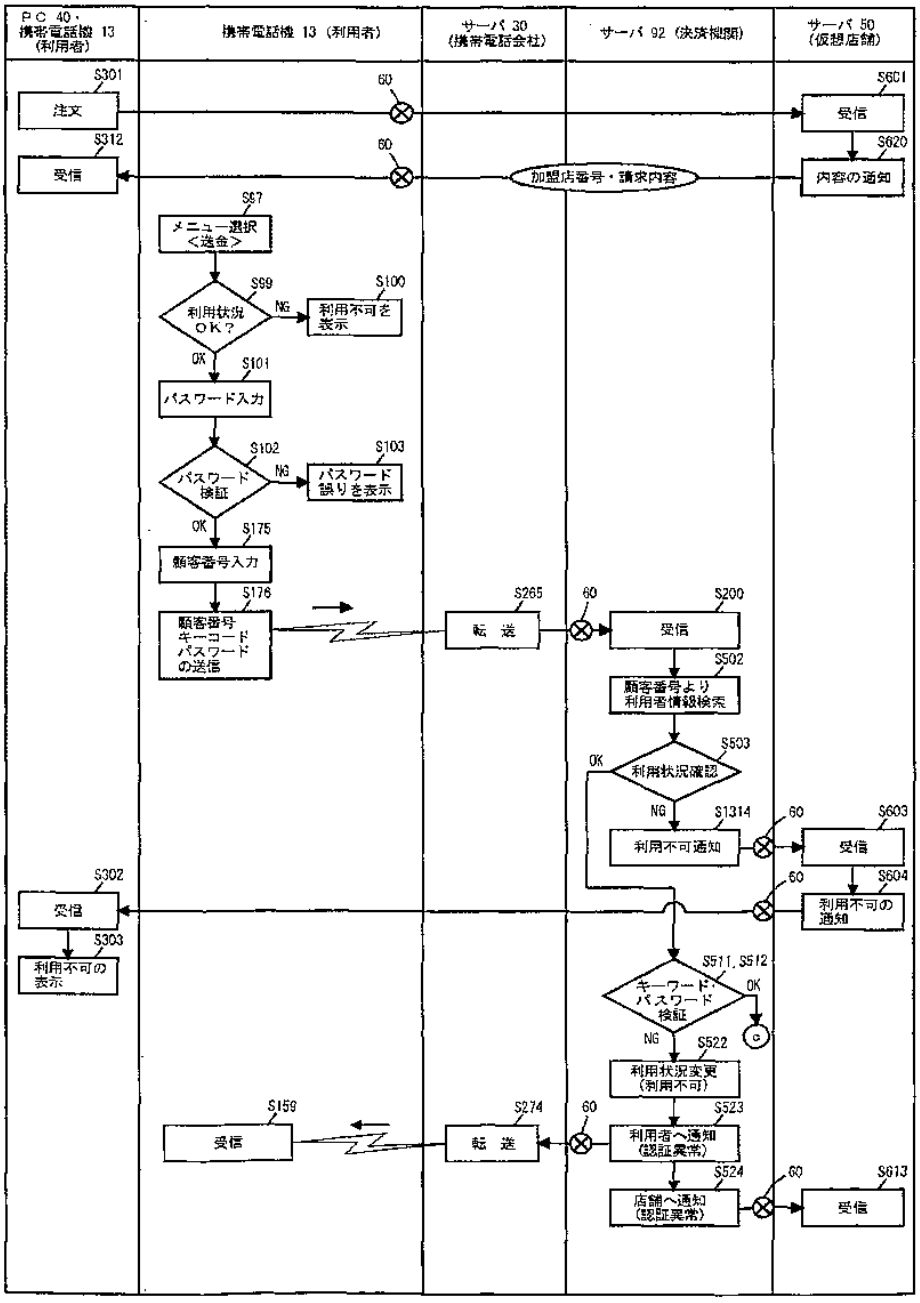
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 526 of 1360

FIG. 71



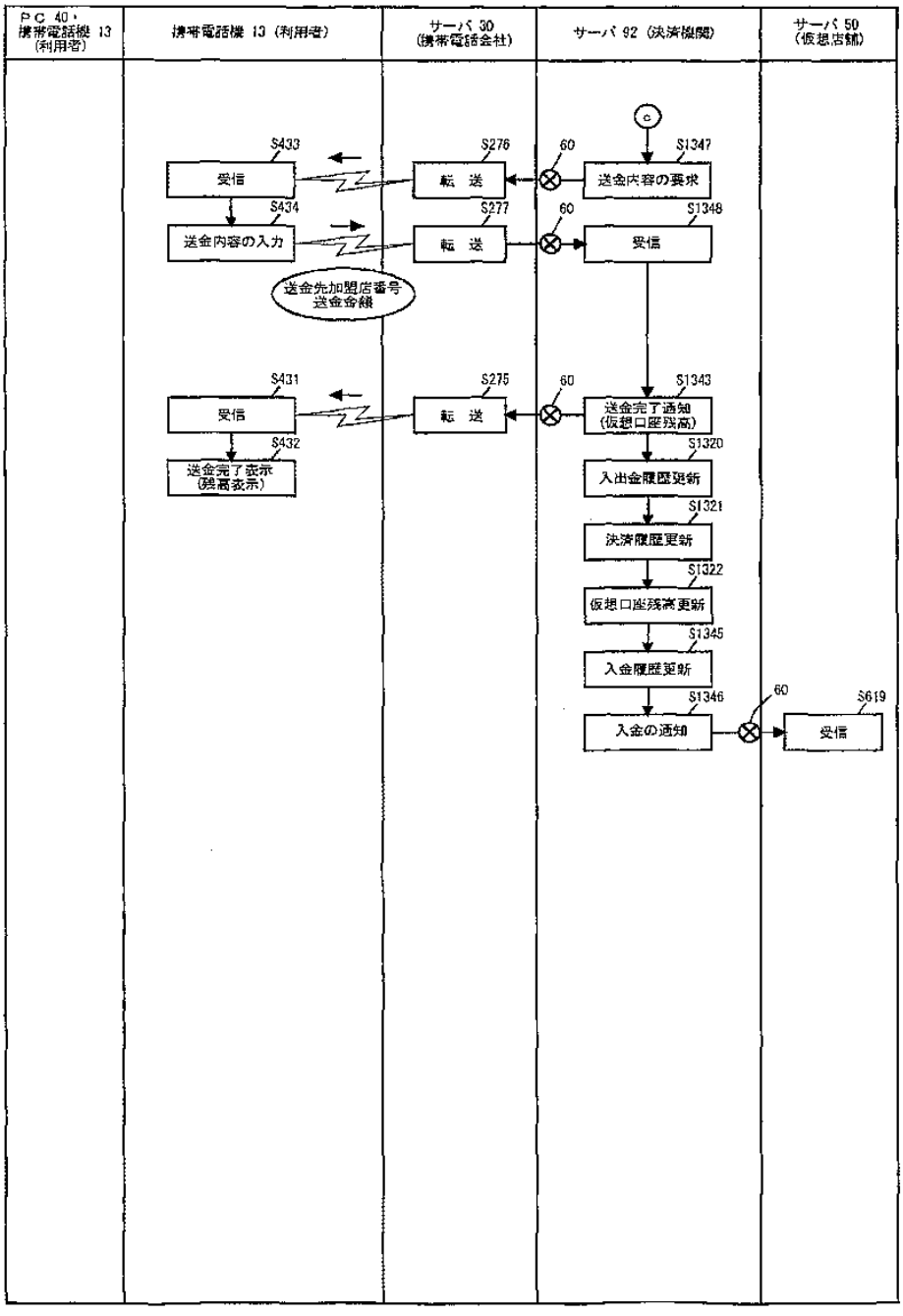
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 527 of 1360

FIG. 72



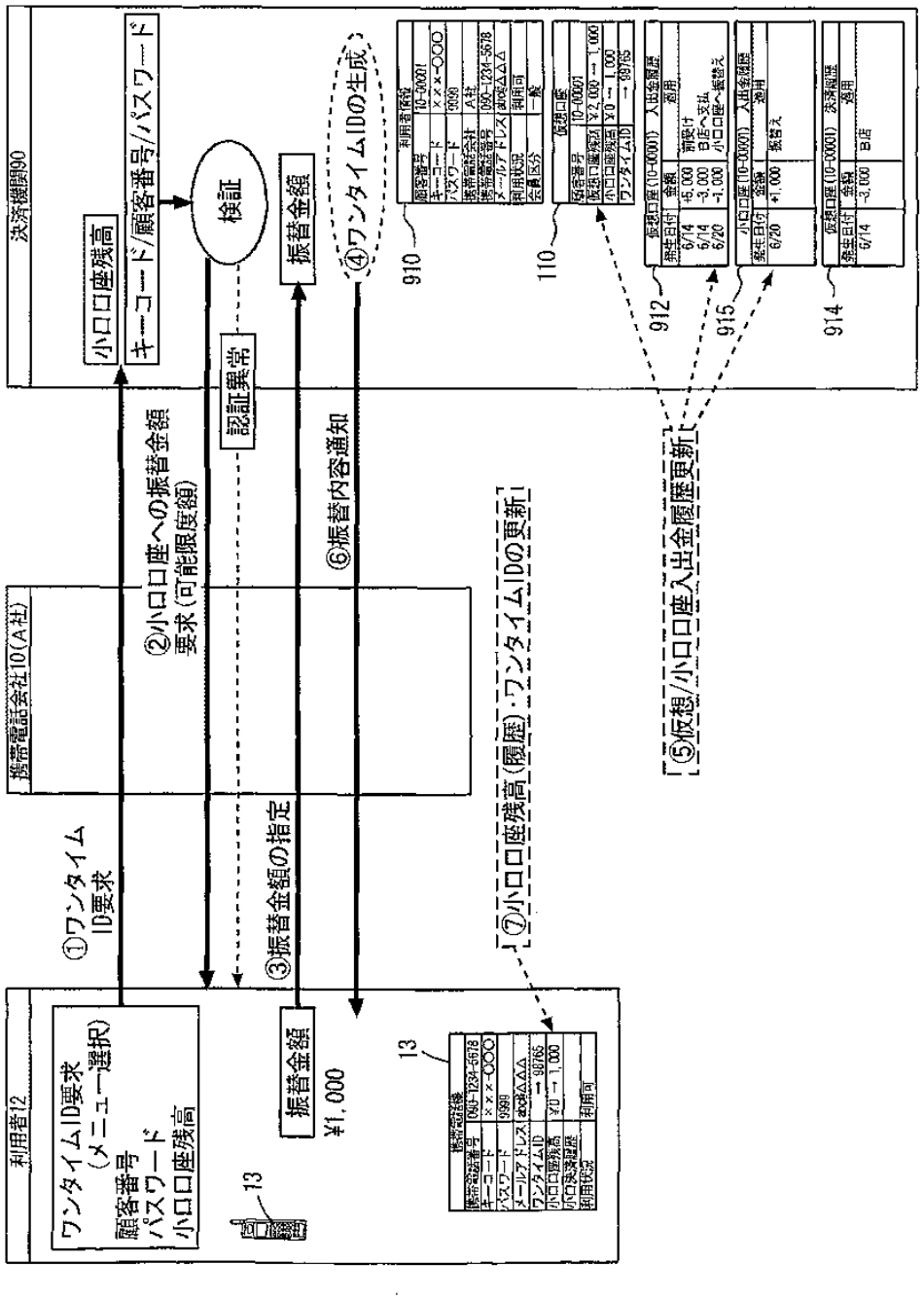
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 528 of 1360

FIG. 73



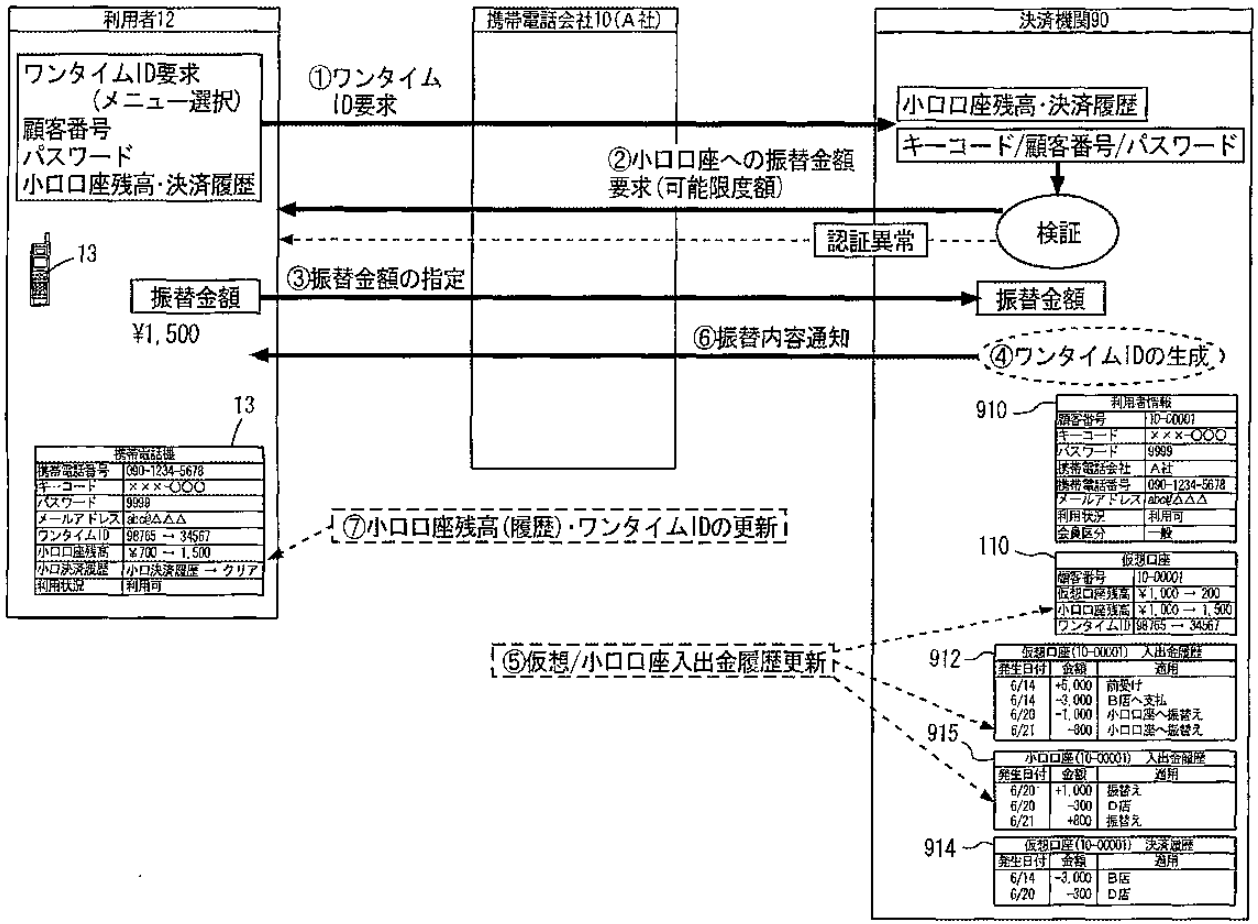
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 529 of 1360

FIG. 74



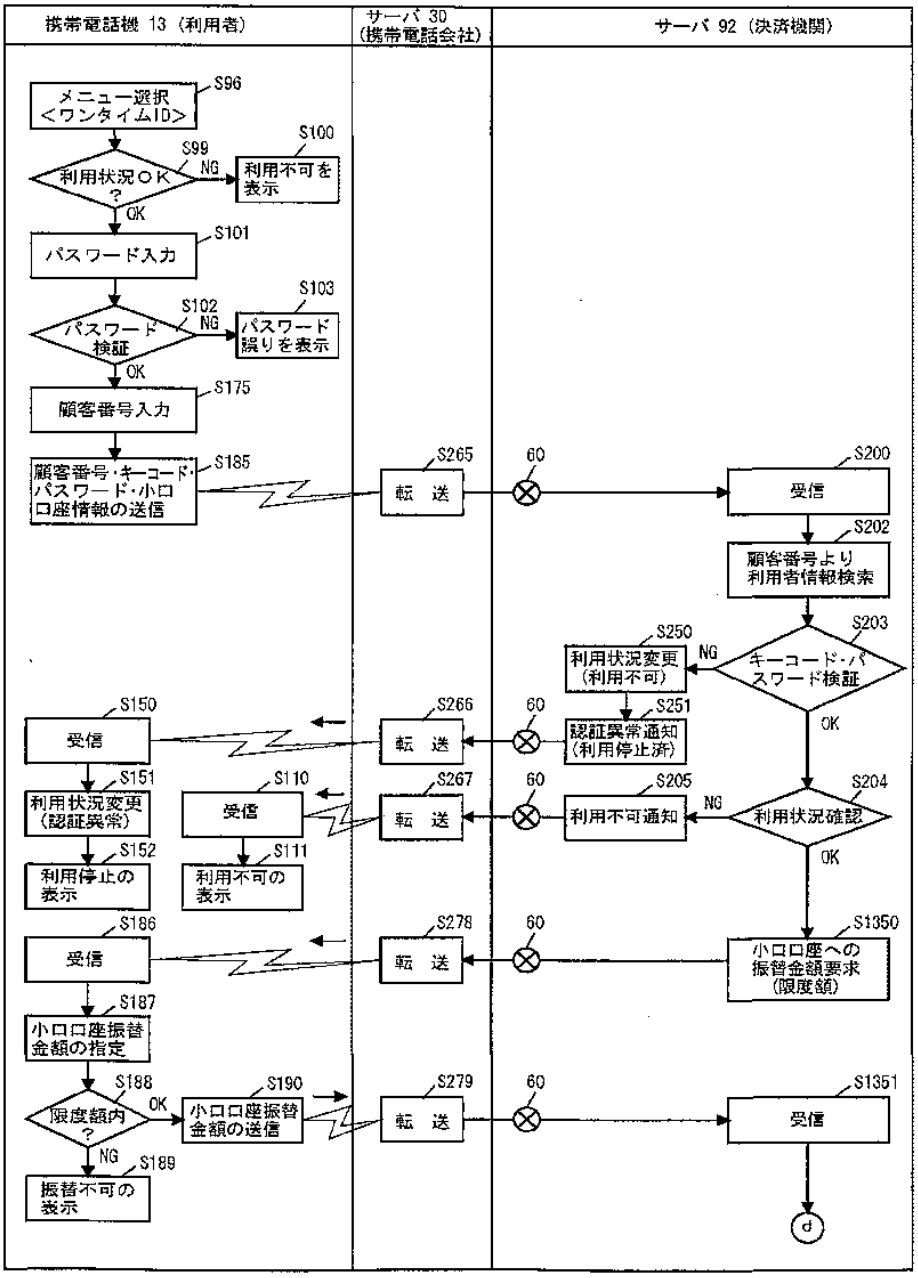
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 530 of 1360

FIG. 75



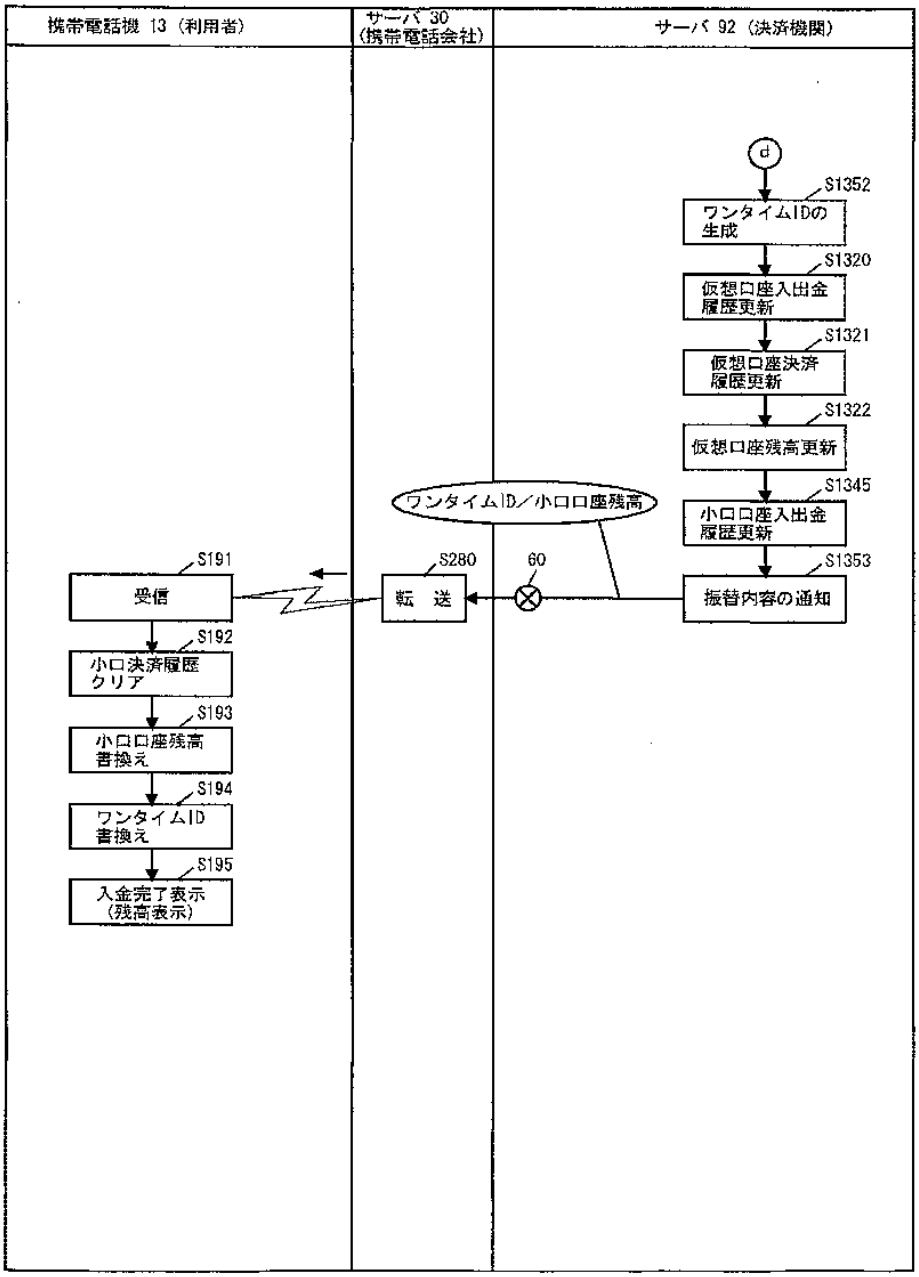
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 531 of 1360

FIG. 76



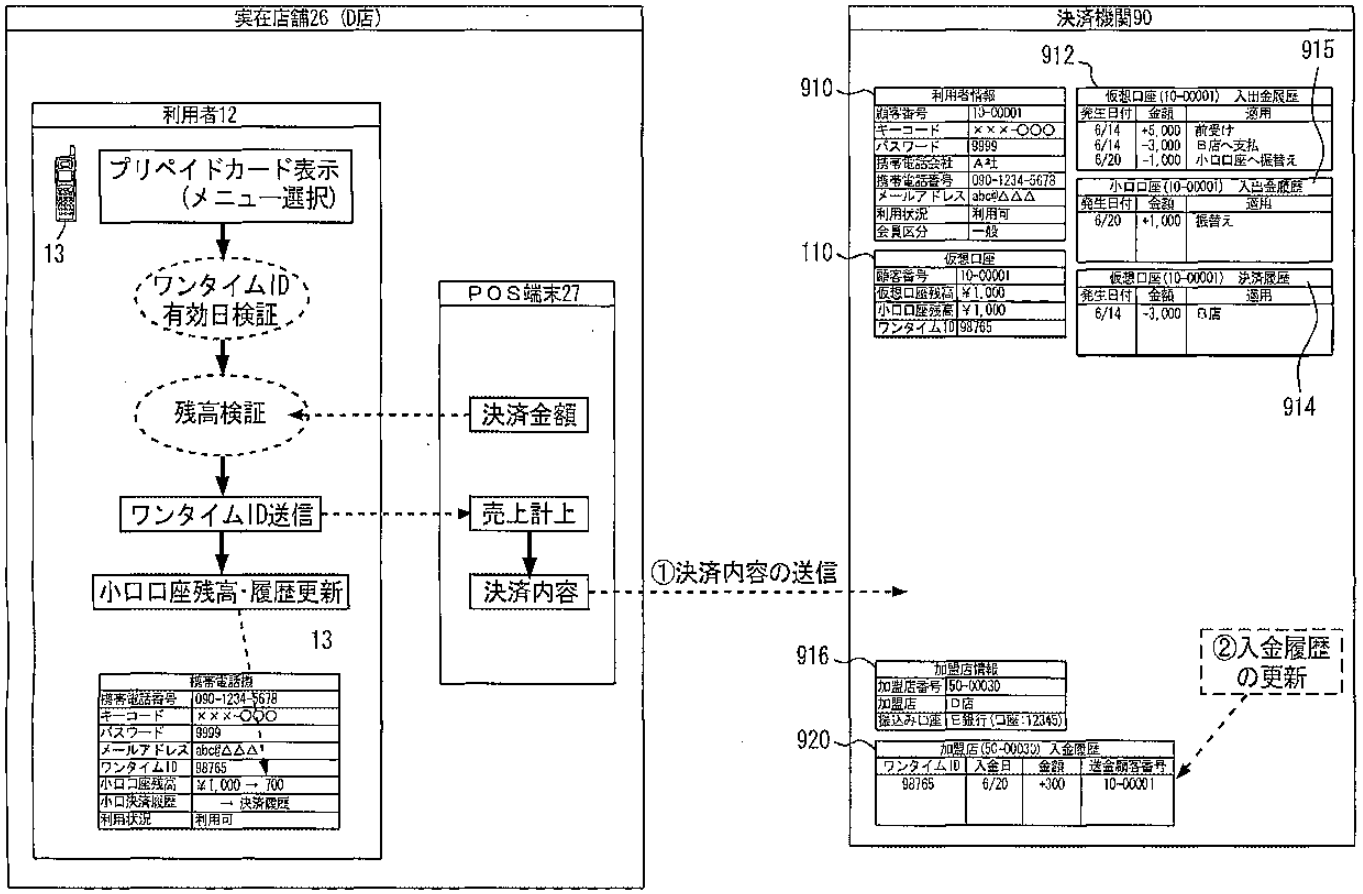
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 532 of 1360

FIG. 77



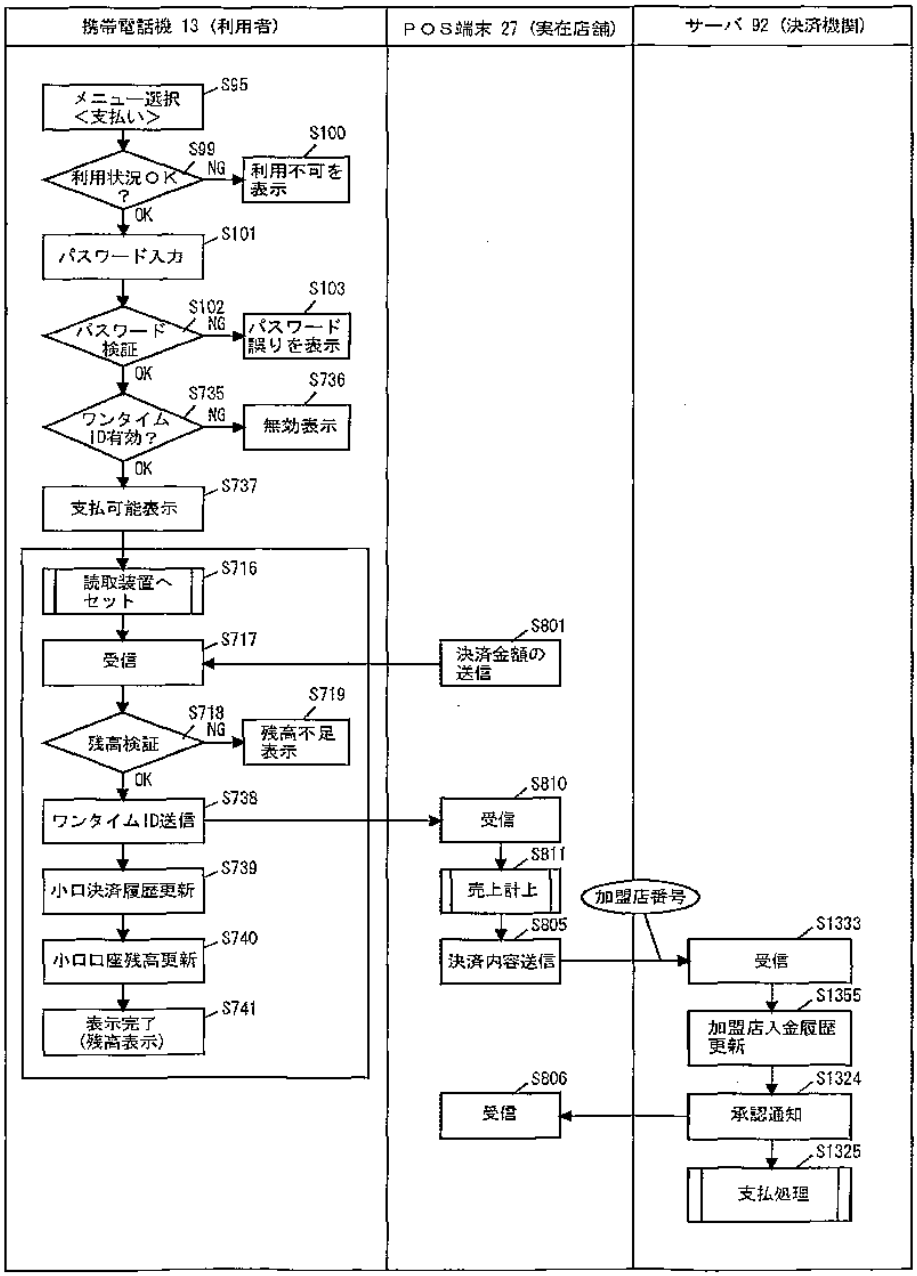
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 533 of 1360

FIG. 78



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 534 of 1360

FIG. 79



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 535 of 1360

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05039

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60, G06F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60, G06F19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 96/25828 A1 (Nokia Mobile Phones, Ltd.), 22 August, 1996 (22.08.96), page 16, lines 18 to 26; page 18, lines 22 to 25 & AU 46247/96 A & AU 696876 B & CN 1174648 A & EP 809916 A1 & FI 950685 A & FI 99071 B & JP 11-501424 A & US 5887266 A	1-33
Y	WO 92/11598 A1 (Motorola, Inc.), 09 July, 1992 (09.07.92), Figs. 5(A) to 5(E) & AT 188562 E & CA 2096730 A & DE 69131897 T & EP 564469 A1 & EP 940760 A1 & ES 2141092 T & GR 3032864 T & KR 97-07003 B1 & JP 6-501329 A & JP 3010069 B2 & US 5221838 A	1-33
Y	JP 6-121075 A (Nippon Telegr. & Teleph. Corp. <NTT>), 28 April, 1994 (28.04.94), Par. Nos. [0026] to [0027] (Family: none)	1-33

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 September, 2001 (11.09.01)	18 September, 2001 (18.09.01)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 536 of 1360

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05039

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2-061786 A (NEC Corporation), 01 March, 1990 (01.03.90), Fig. 1 (Family: none)	1-33
Y	EP 416916 A2 (Fujitsu Ltd.), 13 March, 1991 (13.03.91), Column 23, line 54 to Column 24, line 6 & DE 69033207 T & ES 2136057 T & JP 3-092966 A & JP 3184196 B2 & KR 9607940 A	1-33
Y	WO 99/24892 A1 (Citicorp Development Center, Inc.), 20 May, 1999 (20.05.99), page 11, lines 5 to 29; page 14, lines 18 to 24 & AU 92346/98 A & EP 917120 A2 & JP 11-232348 A & SG 78323 A	1-33
Y	WO 98/026381 A1 (Nixu OY), 18 June, 1998 (18.06.98), Figs. 6, 7; page 16, lines 1 to 6 & AU 52246/98 A & AU 729844 B & CN 1245574 A & DE 69603971 T & EP 848361 A1 & JP 2001-507487 A & NO 992776 & US 6029151 A	1-33
Y	JP 2000-113085 A (Sony Corporation), 21 April, 2000 (21.04.00), Fig. 1 (4, 5, 8) (Family: none)	1-33
A	DUKACH, Semyon, "SNPP: A Simple Network Payment Protocol", In: *Proceedings of the Eighth Annual Computer Security Applications Conference*, 30 November, 1992 (30.11.92), pages 173 to 179	1-33

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ０１／０５０３９

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F17／60, G06F19／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F17／60, G06F19／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO 96/25828 A1 (NOKIA MOBILE PHONES LTD) 22. 8月. 1996 (22.08.96) *16 ページ, 18–26 行; 18 ページ, 22–25 行* & AU 46247/96 A　& AU 696876 B & CN 1174648 A　& EP 809916 A1 & FI 950685 A　& FI 99071 B & JP 11-501424 A　& US 5887266 A	1–33

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
11.09.01	18.09.01

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	阿波　進	５Ｌ	９１６８
	電話番号　０３－３５８１－１１０１　内線　３５６１		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 538 of 1360

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO 92/11598 A1 (MOTOROLA INC) 9. 7月. 1992 (09.07.92) *図5A–5E* & AT 188562 E　& CA 2096730 A & DE 69131897 T　& EP 564469 A1 & EP 940760 A1　& ES 2141092 T & GR 3032864 T　& KR 97-07003 B1 & JP 6-501329 A　& JP 3010069 B2 & US 5221838 A	1–33
Y	JP 6-121075 A（日本電信電話株式会社） 28. 4月. 1994 (28.04.94) *段落[0026]–[0027]* （ファミリーなし）	1–33
Y	JP 2-061786 A（日本電気株式会社） 1. 3月. 1990 (01.03.90) *図1* （ファミリーなし）	1–33
Y	EP 416916 A2 (FUJITSU LTD) 13. 3月. 1991 (13.03.91) *コラム23, 54行 — コラム24, 6行* & DE 69033207 T　& ES 2136057 T & JP 3-092966 A　& JP 3184196 B2 & KR 9607940 A	1–33
Y	WO 99/24892 A1 (CITICORP DEVELOPMENT CENTER INC) 20. 5月. 1999 (20.05.99) *11ページ, 5–29行; 14ページ, 18–24行* & AU 92346/98 A　& EP 917120 A2 & JP 11-232348 A　& SG 78323 A	1–33

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 539 of 1360

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO 98/026381 A1 (NIXU OY) 18. 6 月. 1998 (18.06.98) 図 6, 7; 16 ページ, *1–6 行* & AU 52246/98 A　& AU 729844 B & CN 1245574 A　& DE 69603971 T & EP 848361 A1　& JP 2001-507487 A & NO992776　& US 6029151 A	1–33
Y	JP 2000-113085 A (ソニー株式会社) 21. 4 月. 2000 (21.04.00) *図 1（4, 5, 8 を見よ）* (ファミリーなし)	1–33
A	DUKACH, Semyon, SNPP: A Simple Network Payment Protocol, in *Proceedings of the Eighth Annual Computer Security Applications Conference*, 30 November 1992 (30.11.92), pp 173–179.	1–33

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 540 of 1360

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 19/00, H04M 17/00 — A1

(11) International Publication Number: **WO 98/34203**

(43) International Publication Date: 6 August 1998 (06.08.98)

(21) International Application Number: PCT/US98/01391

(22) International Filing Date: 27 January 1998 (27.01.98)

(30) Priority Data:
791,530 30 January 1997 (30.01.97) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 6455 Lusk Boulevard, San Diego, CA 92121 (US).

(72) Inventors: JACOBS, Paul, E.; 9075 La Jolla Shores Lane, La Jolla, CA 92037 (US). BELK, Jeffrey, K.; 13967 Arbolitos Drive, Poway, CA 92064 (US).

(74) Agents: OGROD, Gregory, D. et al.; Qualcomm Incorporated, 6455 Lusk Boulevard, San Diego, CA 92121 (US).

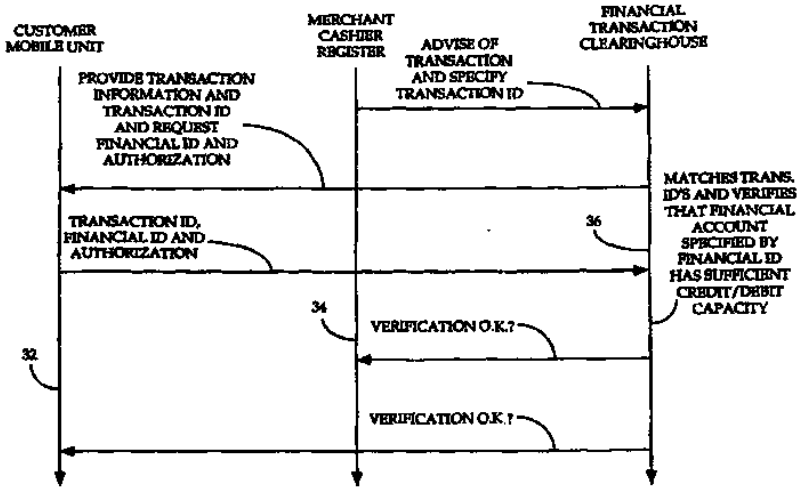
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR PERFORMING FINANCIAL TRANSACTIONS USING A MOBILE COMMUNICATION UNIT



(57) Abstract

Financial identification codes (ID's) are stored directly within a mobile communications unit (12) such as a mobile telephone or other device provided with wireless telephony capability such as a personal data assistant, a laptop computer, a dedicated Internet access device, or electronic organizer. The financial ID's represent credit or debit accounts, digital money or other financial entities. Storage of financial ID's within such devices allows the various financial ID's of credit (28) and debit accounts (30) of a customer or of digital money to be consolidated and used efficiently. The ID's are transmitted by radio or infrared signals to a merchant (14) or other party to enable quick and efficient transactions such as purchase transactions. Radio transmission is particularly advantageous for conducting transactions during a mobile telephone call which might otherwise require verbally reciting the financial ID of a credit or debit account.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND APPARATUS FOR PERFORMING FINANCIAL TRANSACTIONS USING A MOBILE COMMUNICATION UNIT

BACKGROUND OF THE INVENTION

I. Field of the Invention

The invention generally relates to mobile communication units such as mobile telephones and to devices for implementing financial transactions.

II. Description of the Related Art

Consumers increasingly use credit cards, debit cards (such as automated teller machine (ATM) cards), and the like for performing financial transactions with merchants to purchase goods or services. Typically, the consumer provides the credit or debit card to the merchant who runs it through a card scanner to read out a financial identification (ID) associated with the card. The financial ID and the cost of the goods or services are forwarded over a telephone network (such as the public switched telephone network PSTN)) to the bank or other entity providing the credit for the credit card or maintaining the money associated with the debit card. The bank verifies that there is sufficient credit or debit capacity for the transaction and forwards verification to the merchant. The consumer then is typically asked to sign a receipt for the purchase and the transaction is thereby completed and the goods or services are conveyed to the consumer.

Among the advantages of this common type of financial transaction is that the consumer need not carry significant amounts of cash for making purchases and may take advantage of any credit granted to him or her. Disadvantages, however, remain. Consumers typically carry numerous credit and debit cards which can be lost or stolen and are often left accidentally with the merchant. Moreover, the financial ID associated with the card is typically recorded on a magnetic strip on the back of the card which can be accidentally erased or otherwise rendered unreadable. Often, purchases are made using credit or debit accounts over the telephone. In such case, the customer must read the financial ID for the account aloud and the merchant must transcribe the financial ID. This is, at best, a tedious and time consuming process and frequent errors occur in reading or transcribing the financial ID's. Moreover, the financial ID may be captured by

unauthorized parties by eavesdropping. Indeed, the party representing itself as the merchant may merely be fraudulently obtaining financial ID's without intending to provide any goods or services. If the purchase is initiated over the Internet, the financial ID is typically conveyed over the Internet via computer transmission signals which again are subject to eavesdropping.

Accordingly, it would be desirable to consolidate all of the financial ID's associated with all of the credit and debit cards of a consumer in a single device not subject to magnetic erasure thereby minimizing the likelihood of misplacing one of the cards and eliminating the risk of having the financial ID accidentally erased. It would also be desirable to consolidate the financial ID's in a device allowing the ID's to be transmitted efficiently such that the financial ID need not be read and transcribed verbally and allowing the financial ID's to be transmitted in an encrypted or otherwise protected form to minimize the risk that the financial ID's may be captured by eavesdropping. Aspects of the invention are directed to solving these and other problems.

To partially address some of these problems, it has been proposed to store the financial ID of a particular credit or debit account on a Smart Card. A Smart Card is similar to a credit card in size and shape but includes electronic circuitry, perhaps in the form of a small microprocessor, for controlling operation of devices receiving the Smart Card and for storing information such as financial ID's. In one possible implementation, the Smart Card is configured to enable telephony operations of the mobile telephone and is also configured to store the financial ID of a single credit or debit account. To effectuate a financial transaction, the Smart Card is removed from the mobile telephone and provided to a merchant for insertion into a Smart Card reader for reading the financial ID therefrom. Although, the use of such a Smart Card has the advantages that the financial ID cannot be easily erased and may be output subject to appropriate encryption, many of the other disadvantages of conventional credit and debit cards remain. For example, depending upon the implementation, a separate Smart Card may be required for each separate credit and debit account and the separate cards are thereby subject to being lost or stolen. Moreover, the consumer may need to terminate a telephone call to allow the Smart Card to be removed from mobile telephone to effectuate the transaction. Finally, because the Smart Card must be inserted into a reader provided by the merchant, no clear advantages are gained for financial transactions conducted over the telephone or using the Internet.

Accordingly, it would be desirable to provide a more effective integration of mobile telephony and financial ID transactions and it is to that end that further aspects of the invention are drawn.

Finally, there is an movement toward enabling the use of digital money for purchase transactions. Digital money constitutes packets of data containing financial ID's defining certain quantities of money that can be transferred from computer to computer. Digital money differs from credit or debit money in that it is not tied to any external real world account. Rather, digital money is the cyberspace equivalent of cash. It would be desirable to provide the aforementioned integration of mobile telephony and financial ID transactions in a manner that enables and facilitates digital money transactions and it is to that end that still further aspects of the invention are drawn.

SUMMARY OF THE INVENTION

In accordance with one aspect of the invention, financial ID's are stored directly within a mobile communications unit such as a mobile telephone or other device provided with wireless telephony capability such as a personal data assistant (PDA), a laptop computer, a dedicated Internet access device, or an electronic organizer. The financial ID's represent credit or debit accounts, digital money or other financial instruments. Storage of financial ID's within such devices allows the various financial ID's of credit and debit accounts of a customer or of digital money to be consolidated and used efficiently. The ID's are transmitted by radio or infrared signals to a merchant or other party to enable quick and efficient transactions such as purchase transactions. Radio transmission is particularly advantageous for conducting transactions during a mobile telephone call which might otherwise require verbally conveying the financial ID of a credit or debit account. Moreover, by storing the financial ID's in the mobile communications unit, the ID's are therefore not as easily subject to inadvertent magnetic erasure as with magnetic strip cards, and the risks associated with misplacing individual credit or debit cards are avoided. The financial ID's may be transmitted in an encrypted form to minimize the risk of unauthorized capture. Almost any form of transaction otherwise conventionally handled with credit or debit accounts or digital money may be performed.

In one embodiment, the invention is implemented within a mobile communications unit by a providing a means for storing a financial

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 545 of 1360

identification code and a means for transmitting the financial identification code to effectuate a financial transaction. A means for receiving a signal representative of a requested financial transaction is also provided along with means for retrieving the financial ID in response to the received request signal. To receive selections from the customer, the mobile communications unit is further provided with a means for providing an indication representative of the financial identification codes to a customer and for requesting selection of one to effectuate transaction; and a means for receiving a selection signal representative of one of the financial identification codes. To receive authorization from the customer to complete a transaction, the mobile communications unit further includes a means for providing an indication of the requested financial transaction to a customer and for requesting approval to effectuate the transaction; a means for receiving an authorization signal representative of whether approval is granted for effectuating the transaction; and a means for transmitting the authorization signal.

Depending upon the implementation, the means for receiving signals and the means for transmitting signals may be an infrared receiver/transmitter, a cellular telephone receiver/transmitter for communicating with a cellular base station, or a mobile telephone receiver/transmitter for communicating with a satellite. Means for encrypting signals prior to transmission and for decrypting received signals may also be employed.

In other embodiments, the invention is implemented as a method.

BRIEF DESCRIPTION OF THE DRAWINGS

The features, objects, and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings in which like reference characters identify correspondingly throughout and wherein:

FIG. 1 is a block diagram of a financial transaction system configured in accordance with an exemplary implementation of the invention wherein the mobile telephone of a customer has financial ID's stored therein and wherein signals relevant to a purchase transaction are transmitted between the mobile telephone and a merchant cashier register via a cellular telephone system;

FIG. 2 is a flowchart illustrating the steps performed by the system of **FIG. 1** to effectuate a financial transaction in accordance with a first method

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 546 of 1360

wherein a financial ID is transmitted from the mobile telephone to a financial transaction clearinghouse;

FIG. 3 is a block diagram illustrating the mobile telephone of **FIG. 1** and showing a financial ID selection display;

FIG. 4 is a block diagram illustrating the mobile telephone of **FIG. 1** and showing an authorization display;

FIG. 5 is a timing diagram summarizing, at a high level, steps performed by the system of **FIG. 1**;

FIG. 6 is a timing diagram summarizing, at a high level, a second method wherein the financial ID is transmitted from the mobile telephone to the merchant cashier register;

FIG. 7 is a block diagram of a financial transaction system configured in accordance with a first alternative implementation of the invention wherein signals relevant to the financial transaction are transmitted between the mobile telephone and the merchant cashier register via a satellite-based mobile telephone system;

FIG. 8 is a block diagram of a financial transaction system configured in accordance with a second alternative implementation wherein signals relevant to the transaction are transmitted between the mobile telephone and the merchant cashier register via infrared signals;

FIG. 9 is a block diagram of a financial transaction system configured in accordance with a third alternative implementation and wherein signals relevant to a transaction initiated during a telephone call are transmitted between the mobile telephone and the merchant cashier register via a cellular telephone system;

FIG. 10 is a timing diagram summarizing, at a high level, steps performed by the system of **FIG. 9** to effectuate a financial transaction in accordance with a first method wherein a credit or debit account is accessed;

FIG. 11 is a timing diagram illustrating, at a high level, steps performed by the system of **FIG. 9** to effectuate a financial transaction in accordance with a second method wherein digital money is transferred;

FIG. 12 is a block diagram of a financial transaction system configured in accordance with a fourth alternative implementation of the invention wherein signals relevant to a transaction initiated via the Internet are transmitted between the mobile telephone and a merchant computer via a cellular telephone system connected to the Internet;

FIG. 13 is a timing diagram summarizing, at a high level, steps performed by the system of **FIG. 12** to effectuate a financial transaction in

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 547 of 1360

accordance with a method wherein digital money is transferred via the Internet.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

With reference to the figures, preferred and exemplary implementations of the invention will now be described. Initially, techniques of the invention will described with reference to **FIGS. 1 - 5** which illustrate a system employing a mobile telephone wherein signals appropriate for implementing an in-person purchase via a credit or debit account are transmitted between a mobile unit and a merchant cashier register or other point of sale unit via a cellular telephone. The transaction is coordinated by a financial transaction clearinghouse with the financial ID of a credit or debit account selected by the customer being transmitted from the mobile telephone to the clearinghouse, rather than to the merchant cashier register. An alternative method for in-person purchases wherein the financial ID is transmitted from the mobile telephone to the merchant cashier register will be described with reference to **FIG. 6**. Then, alternative systems employing satellite-fleet mobile communications or direct infrared communications between the mobile unit and the merchant cashier register for in-person purchases will be described with reference to **FIGS. 7 - 8**. Next, with reference to **FIGS. 9 - 11**, a system for implementing a purchase wherein the purchaser and merchant are remote from one another will be described both for a credit or debit account purchase and for a digital money purchase. Finally, with reference to **FIGS. 12 - 13** a system for implementing a digital money purchase via the Internet using a lap-top computer with mobile telephony capability will be described.

FIG. 1 shows a system **10** for performing a purchase based upon a credit or debit account between a customer (not shown) using a mobile telephone unit **12** and a merchant (also not shown) using a point of sale cashier register **14**. **FIG. 2** illustrates a method performed by the system of **FIG. 1**. **FIGS. 1** and **2** will be described together with the steps of **FIG. 2** provided in parentheses. After the customer verbally indicates a desire to purchase goods or services, the merchant enters purchase transaction information including the amount of the purchase and the telephone number (provided by the customer) of mobile unit **12** into cashier register **14** (**FIG. 2**, step **102**). The cashier register generates a transaction ID and transmits transaction information and the mobile unit telephone number

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 548 of 1360

over a land line **16** connected to the PSTN **17** to a financial transaction clearinghouse (clearinghouse) **18** (**FIG. 2,** step **104**). The transaction information includes, for example, a transaction ID, the identity and cost of the goods or services and an identification of the merchant. Clearinghouse **18** receives and records the information (**FIG. 2,** step **106**), then calls mobile unit **12** using the provided telephone number via a cellular system **20** having a base station **22** in the vicinity of the mobile unit **12** (**FIG. 2,** step **108**).

The purchaser answers the incoming telephone call to mobile unit **12** and thereby allows the mobile unit **12** to receive signals transmitted by the clearinghouse **18** (**FIG. 2,** step **110**). Depending upon the implementation, clearinghouse **18** may transmit signals to the mobile unit **12** via the cellular system specifying the amount of the transaction, the identity of the goods or services, and the identity of the merchant. Clearinghouse **18** also transmits a request for either digital money or a financial ID specifying a credit or debit account and approval to charge the account. The mobile unit **12** receives the signals and presents appropriate displays to the customer to display information received from clearinghouse **18** and to request selection of a credit or debit account or digital money (**FIG. 2,** step **112**). To this end, mobile unit **12** retrieves pre-stored financial information from a memory unit (not shown) within the mobile unit identifying the credit and debit accounts of the customer of mobile unit **12** and any digital money stored therein.

An exemplary display is provided in **FIG. 3** within a display screen **24** of mobile unit **12**. As can be seen, the exemplary display identifies the merchant, the goods or services and the amount of the purchase and provides three credit card accounts and two ATM (debit) accounts for selection. The credit card accounts may be, for example, VISA, MASTER CHARGE, and AMERICAN EXPRESS accounts and may be identified by appropriate icons in display screen **24**. (VISA, MASTER CHARGE and AMERICAN EXPRESS are trademarks of their respective companies.) The ATM debit card accounts may be checking accounts maintained at different banks and may be identified by the bank name or other appropriate icons in display screen **24**. The display also shows that the purchase may be made using digital money and specifies the amount of digital money available. Examples involving a digital money purchase will be described below with reference to **FIGS. 11 - 13**.

The customer enters a selection by, for example, pressing the appropriate button on keypad **26** corresponding to the number of the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 549 of 1360

selected account (**FIG. 2**, step **114**). In the present example the customer selects credit card no. 2 and is presented with the display of **FIG. 4** requesting authorization to bill the amount of the purchase to the selected credit account (**FIG. 2**, step **116**). The customer responds by pressing the appropriate buttons, such as by pressing 1 for YES or 2 for NO. If NO, an appropriate refusal signal is sent to clearinghouse **18** (**FIG. 1**) via cellular system **20** refusing authorization. The refusal is forwarded to the cashier register and the transaction is terminated. Assuming however, that the customer grants approval by selecting YES, the mobile unit retrieves the financial ID for the selected credit account from an internal memory and forwards the financial ID and an authorization signal to the clearinghouse along with transaction ID (**FIG. 2**, step **120**) via cellular system **20**. Although not separately shown, the customer may be required to first enter a personal identification number (PIN) before authorizing the transaction. Also, depending upon the implementation the financial ID may be encrypted, perhaps using a public key encryption system, the details of which are well known to those skilled in the art and will accordingly not be described herein.

Clearinghouse **18** receives the authorization and the selected financial ID from mobile unit **12** along with the transaction ID and contacts the appropriate bank or credit card company to verify that the selected account has sufficient capacity to cover the purchase (**FIG. 2**, step **122**). In **FIG. 1**, an exemplary set of credit card companies **28** and debit card companies **30** are shown. Communications between clearinghouse **18** and the credit and debit card companies may be via PSTN **17** or any other appropriate communications medium. Assuming that the selected account has sufficient capacity for the purchase, the selected credit account company records the amount of the purchase and the transaction ID and sends a verification signal to clearinghouse **18** for forwarding to the cashier register **14** and to mobile unit **12** (**FIG. 2**, step **124**). Hence, both the customer and the merchant are advised simultaneously of the verification (**FIG. 2**, steps **126** and **128**). Both mobile unit **12** and the cashier register **14** provide an appropriate verification display. The telephone call between clearinghouse **18** and the mobile unit **12** is then terminated. The merchant then conveys the goods or services to the customer and the transaction is completed. Ultimately, the credit card company forwards a bill to the customer for the amount of the purchase and forwards funds to the merchant to cover the purchase.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 550 of 1360

Thus, the system of **FIG. 1** allows for a purchase transaction using, for example, a credit or debit account to be completed easily without requiring the financial ID of the purchasers account to be provided to the merchant and without the use of conventional credit or debit cards which, as noted above, are subject to being lost, stolen or damaged. All of the financial ID's for all of the customers accounts are consolidated in within mobile unit **12** for easy access. Depending upon the implementation, the memory unit of the mobile unit may additionally store the amount of credit or debit remaining, i.e. the account balance, for each credit and debit account. This information may be updated following each transaction. Assuming that all purchases are handled using mobile unit **12**, the account balance information stored therein thereby remains correct. If purchases are made separately perhaps using a conventional credit or debit card, the information for a particular account can be updated following each transaction involving that account by transmitting the current account balance from the appropriate credit or debit card company to the mobile unit via the financial transaction clearinghouse. Additions to the amount of money available in a debit account as a result of a deposit may be tracked in much the same manner.

Depending upon the implementation, the signals transmitted to and from mobile unit **12** may be entirely digital and may be embedded in any on-going voice conversation the purchaser may be having using the mobile unit. For example, for cellular telephone systems employing Code Division Multiple Access (CDMA) technology, which encodes all voice signals digitally, the appropriate digital financial transaction signals may be embedded or interleaved in data packets along with voice signals. In this manner, the purchaser need not terminate an on-going voice telephone call. Rather, the purchaser merely pauses briefly during the conversation to review the information displayed regarding the transaction and to press the appropriate buttons for selecting the credit/debit account and for authorizing the purchase.

Also, depending upon the implementation, no financial transaction clearinghouse is required. Rather, merchant cashier register **14** may communicate directly with the appropriate credit card and debit card companies **28** and **30**.

The messages exchanged during the performance of the steps of the method implemented by the system of **FIG. 1** are summarized at a high level as shown in **FIG. 5** which provides separate time lines **32**, **34** and **36** showing, respectively, the steps performed by mobile unit **12**, merchant

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 551 of 1360

cashier register **14** and financial transaction clearinghouse **18** of **FIG. 1**. The steps performed during the generation of the messages shown in **FIG. 5** have already been described with reference to **FIGS. 1** and **2**, and will not be re-described.

With the system and method thus far described, the selected financial ID is transmitted directly from the mobile unit to the financial transaction clearinghouse. Hence the merchant never receives the financial ID. This helps maintain the privacy of the financial ID, particularly from unauthorized use by possible unscrupulous merchants. **FIG. 6** summarizes a somewhat simpler, alternative method wherein the financial ID is transmitted to the merchant cashier register **14**. After the customer indicates a desire to purchase goods or services and provides the telephone number of the mobile unit, the cashier register **14** calls the mobile unit using the telephone number and transmits signals to mobile unit **12** via the cellular system of **FIG. 1**, at step **20**, advising of the transaction and requesting either the financial ID of a credit/debit account or digital money and requesting authorization to complete the transaction. The advise of transaction information includes an identification of the goods or service to be purchased and the cost thereof.

Mobile unit **12** provides appropriate displays such as those illustrated in **FIGS. 3 - 4**, inputs the appropriate selections from the customer and then, assuming that a credit or debit account is selected, transmits the financial ID of the credit or debit account and an authorization signal to the merchant cashier register, step **202**. The cashier register then transmits signals to the financial transaction clearinghouse, step **204**, perhaps using land lines as illustrated in **FIG. 1**, advising of the transaction and providing the financial ID and the authorization signal received from the mobile unit. Again the advice of transaction information includes the cost of the goods or services to be purchased. Clearinghouse **18** forwards the financial ID to the appropriate credit account or debit account company and requests verification that the selected account has the capacity to cover the purchase. Assuming that the selected account has sufficient capacity, a verification signal is received by clearinghouse **18** and then forwarded to the cashier register **14** for completion of the transaction. One particular advantage of performing the method of **FIG. 6** is that the telephone number of the mobile unit need not be provided to the merchant for inputting into the cashier register because no telephone calls are made to the mobile unit.

What has been described thus far is a system wherein communication between the cashier and the financial transaction clearinghouse is

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 552 of 1360

performed using the PSTN and wherein communications between the mobile unit and clearinghouse is performed using a cellular telephone system. In general, however, any appropriate forms of communication may alternatively be employed. For example, communication between the cashier register and the clearinghouse may also be via a cellular telephone system. Alternatively, communications may be performed using a satellite-based mobile communications system. Also, communications between the mobile unit and cashier may be performed using an infrared system.

FIG. 7 illustrates a satellite-based system **310** having a mobile unit **312**, a cashier register **314**, a financial transaction clearinghouse **318**, and credit account and debit account companies **320** and **322** all interconnected via a satellite mobile communications system represented by a single satellite **324**. The satellite system may include ground stations not separately shown. All communications between the various units are performed using the satellite system thereby eliminating the need for any land line communications. Any of the transaction methods described above with respect to **FIGS. 1 - 6** may be performed using the system of **FIG. 7** and the methods will not be re-described.

FIG. 8 illustrates an infrared-based system **410** having a mobile unit **412**, a cashier register **414**, PSTN **417**, a financial transaction clearinghouse **418**, and credit account and debit account companies **428** and **430**. As with the system of **FIG. 1** the cashier register, the clearinghouse and the credit and debit account companies are interconnected via the PSTN. However, communication between the mobile unit and the cashier is performed using infrared signals. More specifically, mobile unit **412** has an infrared receiver/transmitter **424** and cashier register **414** has an infrared receiver/transmitter **426**.

In an exemplary transaction performed in accordance with the method of **FIG. 6**, the cashier transmits to the mobile unit via infrared signals the amount of the transaction and an identification of the goods or services. The mobile unit inputs the customers selection of a credit or debit account, receives explicit authorization from the customer, then transmits the financial ID of the selected account and an authorization signal to the cashier register **414** via infrared signals. Transmission and reception of the infrared signals may be entirely in accordance with conventional infrared techniques which are well understood by those skilled in the art and will not be described herein. In an alternative embodiment of the invention, the method of **FIG. 2** is performed using the system of **FIG. 8** whereby the telephone number of mobile unit **12** is exchanged using the infrared link.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 553 of 1360

Thus far, in-person transaction methods have been described wherein the customer with mobile unit is in the vicinity of the merchant cashier register. In the following, transactions are described wherein the customer is remote from the merchant and initiates the transaction either via a mobile telephone call to the merchant or via an Internet or similar computer network connection. Also, transactions are described wherein digital money is conveyed.

FIG. 9 illustrates a system **510** having a customer mobile unit **512** and a merchant cashier register **514** with telephone **515**. The mobile unit is located remote from the cashier and telephone as indicated by a dashed line interposed between them. Cashier register **514** and telephone **515** are connected via a land line **516** to PSTN **517** which, in turn, is connected to a financial transaction clearinghouse **518**, cellular system **520** having base station **522**, and credit and debit account companies **528** and **530**. The customer initiates a purchase transaction by calling the merchant telephone **515** using mobile unit **512** and indicates a desire to purchase goods or services. The merchant enters the selected transaction into cashier register **514** which communicates directly with mobile unit **512** via the open mobile telephone call connection to digitally provide the amount and nature of the transaction to the mobile unit and to digitally requests a financial ID and an authorization signal for completing the transaction. This assumes that a mobile system is employed that allows embedding of digital signals within voice telephone conversation signals such as the aforementioned CDMA system. The customer pauses briefly during his conversation with the merchant to select a credit or debit account and to authorize the transaction in the same manner as described above with reference to **FIGS. 3 - 4**. Mobile unit **512** retrieves the financial ID of the selected account and transmits the financial ID and an authorization signal digitally to cashier register **514** again via the same mobile telephone call. Cashier register **514** immediately forwards the financial ID and authorization signal to the financial transaction clearinghouse over a second PSTN line (not separately shown). Clearinghouse **518** operates in the same manner as described above to obtain verification that the selected account has sufficient capacity of the purchase. A verification signal is forwarded back to the cashier **514** which displays the verification to the merchant who verbally conveys the verification to the customer using telephone **515**. Verification may additionally be transmitted from the cashier register to the mobile unit via the open mobile telephone call. The telephone call is then terminated and the transaction is thereafter completed by providing the goods or services to the customer.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 554 of 1360

The steps of the method implemented by the system of **FIG. 9** are summarized at a high level within **FIG. 10** which provides separate time lines **532**, **534** and **536** showing, respectively, the steps performed by the mobile unit **512**, the cashier register **514** and the financial transaction clearinghouse **518** of **FIG. 9**.

Hence, a system is provided wherein digital signals pertaining to a purchase transaction are transmitted between a customer mobile unit and a merchant cashier register during a voice mobile telephone conversation between the customer and merchant. This is similar to otherwise conventional telephone purchase transactions using credit or debit accounts, but with the system of **FIG. 9 - 10** the customer need not verbally convey the financial ID of a credit/debit account to the merchant during the telephone call. This has the advantage of speeding up the transaction because the customer need not read aloud the financial ID, name and expiration date from a credit card and the merchant need not record that information. Also, mistakes that can commonly occur in reading and transcribing the digits of the financial ID are avoided. Moreover, the unauthorized capture of the financial ID by eavesdropping is minimized. As with previous embodiments, the financial ID may encrypted to further reduce the risk of unauthorized access.

Thus far, all example transactions described have involved the purchase of goods or services using a credit or debit account selected by the customer. As noted above, however, any of the various transaction methods and systems also allow payment for the goods or services using digital money stored within the mobile unit.

FIG. 11 summarizes a digital money transaction using the system of **FIG. 9**. **FIG. 11** provides separate time lines **632** and **634** showing, respectively, the steps performed by the mobile unit **512** and the point of sale cashier register **514** of **FIG. 9**. No time line is provided for the financial transaction clearinghouse because no credit or debit account is used and hence account verification is required. Rather digital money is conveyed for the customer mobile unit to the merchant cashier register.

The customer initiates a purchase transaction with the merchant during a voice mobile telephone call from the mobile unit to the merchant telephone, step **636**. The merchant enters the purchase transaction information into the cashier register and, in the same manner as described above without reference to **FIG. 9**, the cashier register transmits digital signals to the mobile unit advising of the transaction and requesting a financial ID and an authorization signal, step **638**. The customer is then

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 555 of 1360

presented with a display such as is shown in FIG 3. However, rather than selecting a credit or debit account, the customer presses the appropriate buttons to select the digital money option and to authorize the purchase. Assuming the customer has sufficient digital money stored within the mobile telephone to cover the purchase, the financial ID or ID's of the digital money is transmitted to the cashier register as digital signals embedded within the mobile telephone voice conversation signals, step 640. The cashier register receives and stores the digital money. Hence, the digital money account of the mobile unit is decreased and the digital money account of the cashier register is increased. The completion of the digital money transaction is confirmed by transmitting appropriate verification and receipt signals from the cashier register back to the mobile unit, step 642. The telephone call is then ended and the goods or services are ultimately conveyed to the customer. If the goods or services are for some reason not conveyed, the verification and receipt signals received by the mobile unit of the customer provide proof of the transaction.

Thus far all transactions have been described with reference to systems employing mobile telephones capable of voice conversation telephone calls. As noted above however, purchase transactions can be performed in accordance with the invention using other types of mobile communications units such as laptop computers and PDA's configured with mobile transmitter/receivers. FIG. 12 provides an example of a system employing a laptop computer wherein a purchase transaction is performed over the Internet. FIG. 13 illustrates a method using the system of FIG. 12 wherein the purchase is made with digital money.

FIG. 12 illustrates a system 710 having a mobile laptop computer unit 712 and a merchant computer 714 located remote from one another. Merchant computer 714 is connected via a land line 716 to a PSTN 717 which is in turn connected to a financial transaction clearinghouse 718, the Internet 719 and a cellular system 720 having a base station 722. The clearinghouse is additionally connected to various credit account and debit account companies 728 and 730.

The customer initiates a purchase transaction by contacting the merchant computer via the cellular system and the Internet. In this regard, the laptop computer employs a modem (not separately shown) in connection with a mobile receiver/transmitter (also not separately shown) to contact the merchant computer via base station 722, cellular system 720, Internet 719 and PSTN 717 perhaps to access World Wide Web page maintained by the merchant. In any case, the customer selects goods or

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 556 of 1360

services to be purchased by entering the appropriate commands into laptop 712 for transmission to merchant computer 714.

The merchant computer receives the customers purchase selection and transmits appropriate signals confirming the purchase selection and requesting a financial ID and an authorization signal. As with the other embodiments described above, the customer may select a credit or debit account or a quantity of digital money. If the former, the financial ID of the account is transmitted via the Internet, preferably encrypted, to the merchant computer for forwarding to the financial transaction clearinghouse, perhaps also via the Internet, for verification of adequate credit or debit account capacity. Appropriate, verification signals are sent to the merchant computer and forwarded to the customers laptop computer. If the purchase is via digital money, the financial ID defining the needed quantity of digital money is transmitted over the Internet to the merchant computer, again preferably encoded in some manner to prevent unauthorized capture, and appropriate verification and receipt signals are sent back to the customer. With the digital money transaction, no signal need be sent to the clearinghouse.

FIG. 13 summarizes the digital money transaction using the system of **FIG. 12**. **FIG. 13** provides separate time lines **732** and **734** showing, respectively, the steps performed by the laptop **712** and merchant computer **714** of **FIG. 12**. Again, no time line is provided for the financial transaction clearinghouse because no credit or debit account is used and hence account verification is required.

Various exemplary systems and methods for performing financial transactions such as purchase transactions using a mobile telephone or other mobile communications unit configured to store the financial ID's of various credit and debit accounts and/or quantities of digital money have been described. In accordance with the principles of the invention, a wide variety of other financial transactions may be performed as well including, in general, almost any transaction otherwise handled with credit or debit cards or digital money. Although the examples provided wherein relate to mobile telephone or laptops computers, principles of the invention can be applied to almost any type of mobile communications unit including, the aforementioned PDA's, mobile Internet access devices, etc.

The exemplary embodiments have been primarily described with reference to block diagrams illustrating apparatus elements and timing diagrams and flow charts primarily illustrating method steps. As to the timing diagrams and flowcharts, each block or step therein represents both a

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 557 of 1360

method step and an apparatus element for performing the recited step. Depending upon the implementation, each apparatus element, or portions thereof, may be configured in hardware, software, firmware or combinations thereof. It should be appreciated that not all components necessary for a complete implementation of a practical system are illustrated or described in detail. Rather, only those components necessary for a thorough understanding of the invention have been illustrated and described.

Moreover, the previous description of the preferred embodiments is provided to enable any person skilled in the art to make or use the present invention. The various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without the use of the inventive faculty. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

WE CLAIM:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 558 of 1360

CLAIMS

1. In a mobile communications unit, a system for performing a financial transaction comprising:

means for storing a financial identification code; and

means for transmitting said financial identification code to effectuate a financial transaction.

2. The system of claim 1 further including

means for receiving a signal representative of a requested financial transaction; and

means for retrieving the stored financial identification code in response to reception of the signal representative of the requested financial transaction.

3. The system of claim 1 wherein said mobile communications unit is selected from a group consisting of a mobile telephone, a personal data assistant with mobile telephony capability, a laptop computer with mobile telephony capability, an Internet access device with mobile telephony capability, and an electronic organizer with mobile telephony capability.

4. The system of claim 1 wherein said financial identification code is representative of digital money.

5. The system of claim 1 wherein said financial identification code is representative of a debit account.

6. The system of claim 1 wherein said financial identification code is representative of a credit account.

7. The system of claim 1 wherein said means for storing a financial identification code stores a plurality of financial identification codes.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 559 of 1360

8. The system of claim 7 wherein said system further includes -

means for providing an indication representative of said financial identification codes and for requesting selection of one to effectuate transaction; and

means for receiving a selection signal representative of one of said financial identification codes.

9. The system of claim 2 further comprising:

means for providing an indication of said requested financial transaction and for requesting approval to effectuate transaction;

means for receiving an authorization signal representative of whether approval is granted for effectuating said requested transaction; and

means for transmitting said authorization signal.

10. The system of claim 9 wherein said means for receiving an authorization signal operates to receive a personal identification number code.

11. The system of claim 4 further including

means for receiving a signal indicative of a completed financial transaction; and

means for modifying said digital money financial identification code to reflect the completed financial transaction.

12. The system of claim 2

wherein said means for receiving the signal representative of the requested financial transaction includes an infrared receiver.

13. The system of claim 1

wherein said means for transmitting said financial identification code includes an infrared transmitter.

14. The system of claim 2

wherein said means for receiving the signal representative of the requested financial transaction includes a cellular telephone receiver.

15. The system of claim 1

wherein said means for transmitting said financial identification code includes a cellular telephone transmitter.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 560 of 1360

16. The system of claim 2
wherein said means for receiving the signal representative of the requested financial transaction includes a wireless telephone receiver for receiving signals from a satellite.

17. The system of claim 1
wherein said means for transmitting said financial identification code includes a wireless telephone transmitter for transmitting signals to a satellite.

18. The system of claim 1 wherein said means for transmitting said financial identification code includes a means for encrypting the financial identification code prior to transmission.

19. In a mobile communications unit, a system for performing a financial transaction comprising:
a memory unit storing a financial identification code;
a receive unit receiving a signal representative of a requested financial transaction;
a control unit retrieving the financial identification code in response the received signal; and
a transmit unit transmitting said financial identification code to effectuate said requested financial transaction.

20. A system for performing a financial transaction comprising:
a point of sale unit comprising
means for transmitting a signal representative of a requested financial transaction, and
means for receiving a financial identification code for effectuating said requested financial transaction;
a mobile communications unit comprising
means for storing a financial identification code,
means for receiving the signal representative of the requested financial transaction, and
means for transmitting said financial identification code to effectuate said requested financial transaction.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 561 of 1360

21. In a mobile communications unit, a method for performing a financial transaction comprising the steps of:

storing a financial identification code; and

transmitting said financial identification code to effectuate a financial transaction.

22. The method of claim 21 further including the steps of

receiving a signal representative of a requested financial transaction; and

retrieving the stored financial identification code for transmission in response to reception of the signal representative of a requested financial transaction.

23. The method of claim 21 wherein said mobile communications unit is selected from a group consisting of a mobile telephone, a personal data assistant with mobile telephony capability, a laptop computer with mobile telephony capability, an Internet access device with mobile telephony capability, and an electronic organizer with mobile telephony capability.

24. The method of claim 21 wherein said financial identification code is representative of digital money.

25. The method of claim 21 wherein said financial identification code is representative of a debit account.

26. The method of claim 21 wherein said financial identification code is representative of a credit account.

27. The method of claim 21 wherein said step of storing a financial identification code is performed to store a plurality of financial identification codes.

28. The method of claim 27 wherein said method further includes the steps of

providing an indication representative of said financial identification codes and for requesting selection of one to effectuate said transaction; and

receiving a selection signal representative of one of said financial identification codes.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 562 of 1360

29. The method of claim 23 further comprising the steps of:
providing an indication of said requested financial transaction and for requesting approval to effectuate said transaction;
receiving an authorization signal representative of whether approval is granted for effectuating said transaction; and
transmitting said authorization signal.

30. The method of claim 21 wherein said step of receiving a authorization signal is performed to receive a personal identification number code.

31. The method of claim 24 further including the steps of
receiving a signal indicative of a completed financial transaction; and
modifying said digital money financial identification code to reflect the completed financial transaction.

32. The method of claim 22
wherein said step of receiving the signal representative of the requested financial transaction includes the step of receiving an infrared signal.

33. The method of claim 21
wherein said step of transmitting said financial identification code includes the step of transmitting an infrared signal.

34. The method of claim 22
wherein said step of receiving the signal representative of the requested financial transaction includes the step of receiving a cellular telephone signal.

35. The method of claim 21
wherein said step of transmitting said financial identification code includes the step of transmitting a cellular telephone signal.

36. The method of claim 22
wherein said step of receiving the signal representative of the requested financial transaction includes the step receiving signals from a satellite.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 563 of 1360

37. The method of claim 21

2 wherein said step of transmitting said financial identification code includes the step of transmitting signals to a satellite.

38. The method of claim 21 wherein said step of transmitting said

2 financial identification code includes the step of encrypting the financial identification code prior to transmission.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 564 of 1360

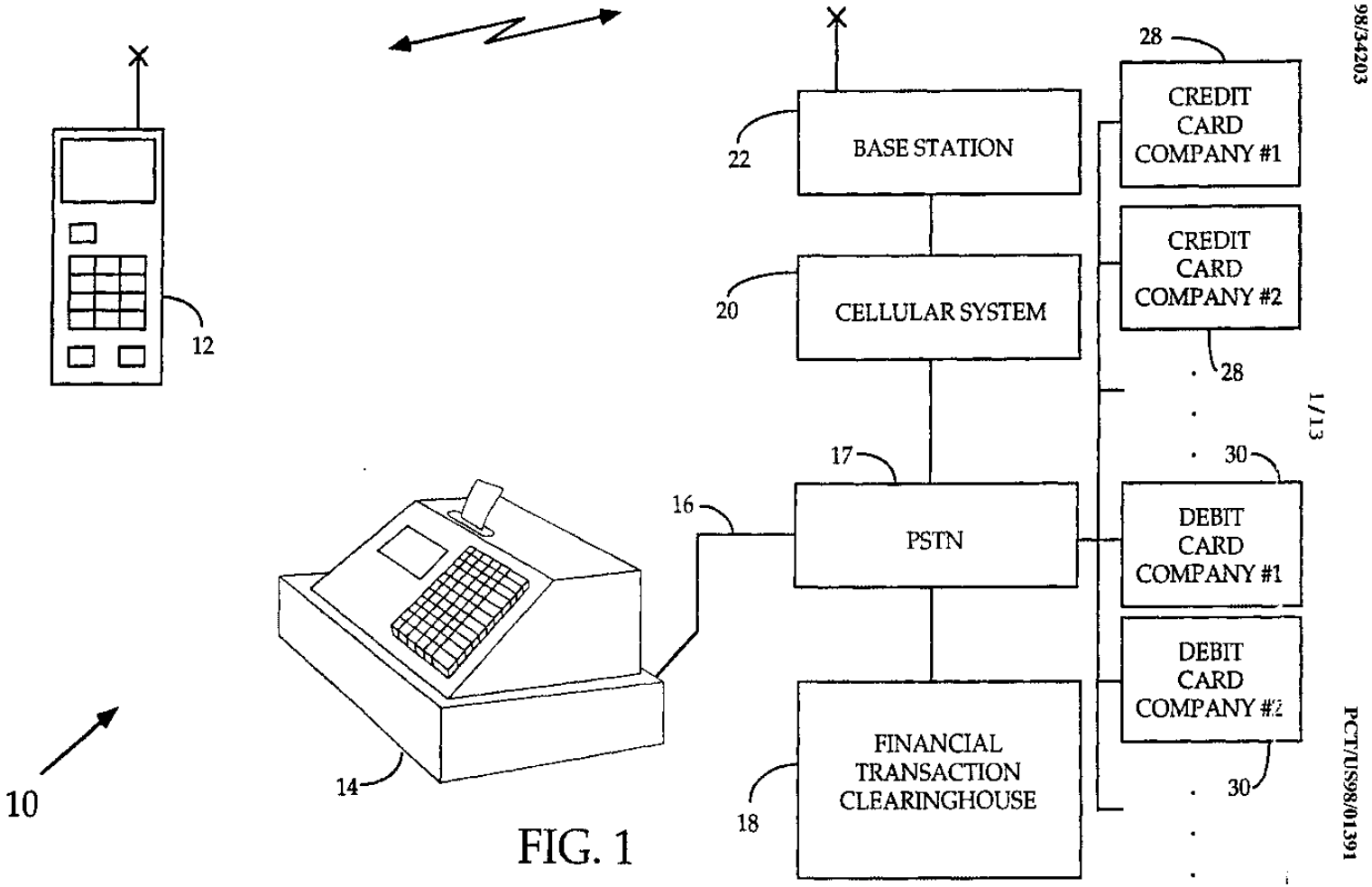


FIG. 1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 565 of 1360

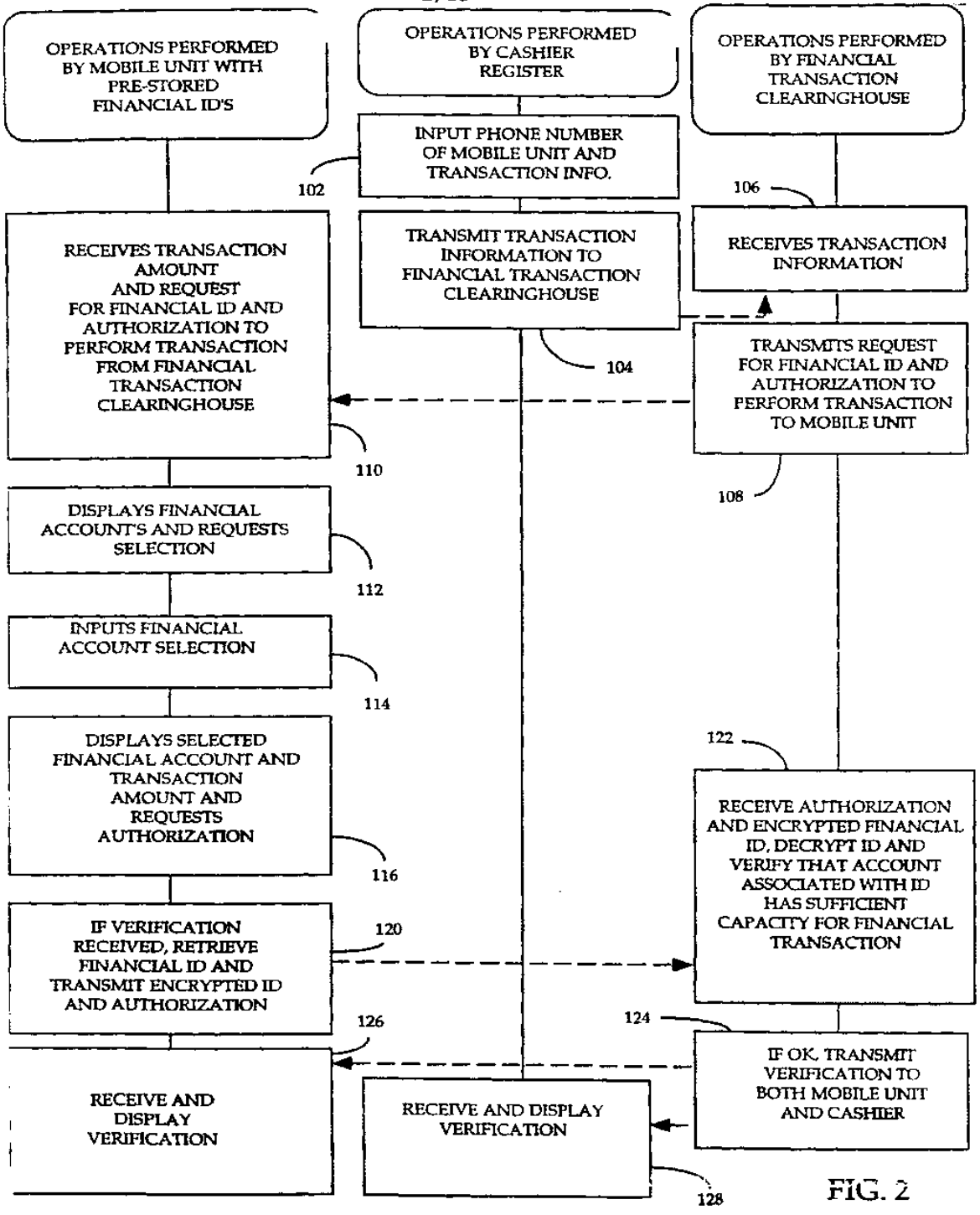

OPERATIONS PERFORMED BY MOBILE UNIT WITH PRE-STORED FINANCIAL ID'S
OPERATIONS PERFORMED BY CASHIER REGISTER
OPERATIONS PERFORMED BY FINANCIAL TRANSACTION CLEARINGHOUSE
INPUT PHONE NUMBER OF MOBILE UNIT AND TRANSACTION INFO.
102
106
RECEIVES TRANSACTION AMOUNT AND REQUEST FOR FINANCIAL ID AND AUTHORIZATION TO PERFORM TRANSACTION FROM FINANCIAL TRANSACTION CLEARINGHOUSE
TRANSMIT TRANSACTION INFORMATION TO FINANCIAL TRANSACTION CLEARINGHOUSE
RECEIVES TRANSACTION INFORMATION
104
TRANSMITS REQUEST FOR FINANCIAL ID AND AUTHORIZATION TO PERFORM TRANSACTION TO MOBILE UNIT
110
108
DISPLAYS FINANCIAL ACCOUNT'S AND REQUESTS SELECTION
112
INPUTS FINANCIAL ACCOUNT SELECTION
114
DISPLAYS SELECTED FINANCIAL ACCOUNT AND TRANSACTION AMOUNT AND REQUESTS AUTHORIZATION
116
122
RECEIVE AUTHORIZATION AND ENCRYPTED FINANCIAL ID, DECRYPT ID AND VERIFY THAT ACCOUNT ASSOCIATED WITH ID HAS SUFFICIENT CAPACITY FOR FINANCIAL TRANSACTION
IF VERIFICATION RECEIVED, RETRIEVE FINANCIAL ID AND TRANSMIT ENCRYPTED ID AND AUTHORIZATION
120
124
126
IF OK, TRANSMIT VERIFICATION TO BOTH MOBILE UNIT AND CASHIER
RECEIVE AND DISPLAY VERIFICATION
RECEIVE AND DISPLAY VERIFICATION
128

FIG. 2

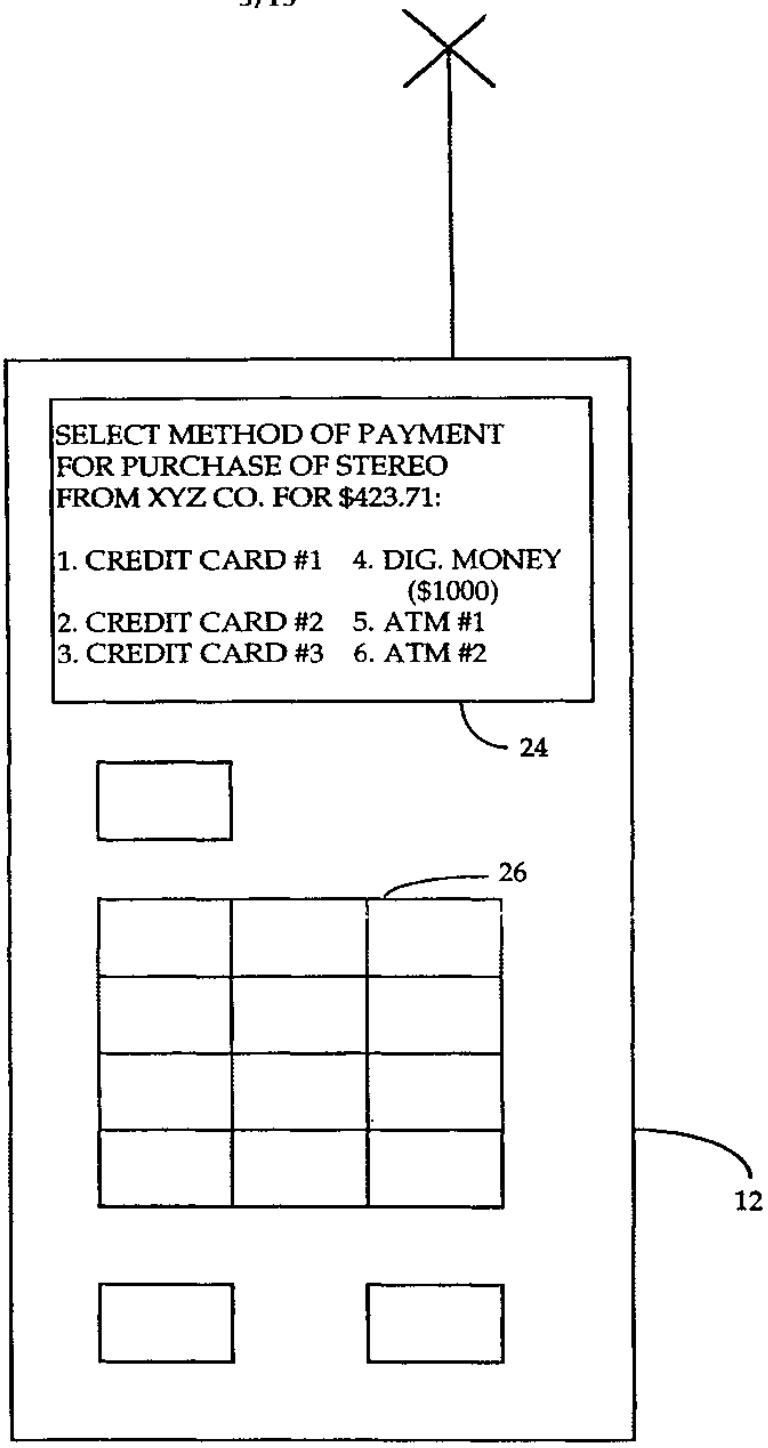

SELECT METHOD OF PAYMENT
FOR PURCHASE OF STEREO
FROM XYZ CO. FOR $423.71:
1. CREDIT CARD #1
2. CREDIT CARD #2
3. CREDIT CARD #3
4. DIG. MONEY ($1000)
5. ATM #1
6. ATM #2
24
26
12

FIG. 3

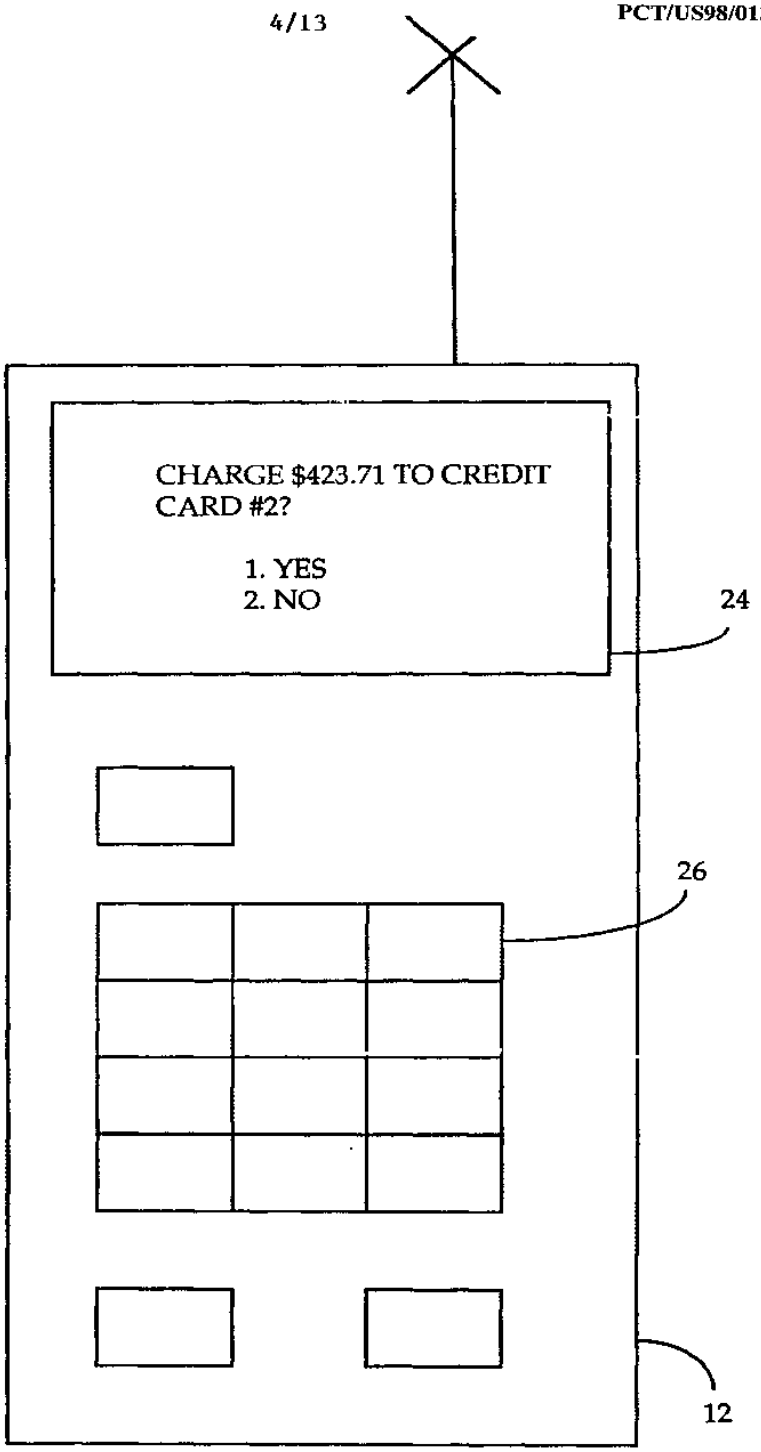


FIG. 4

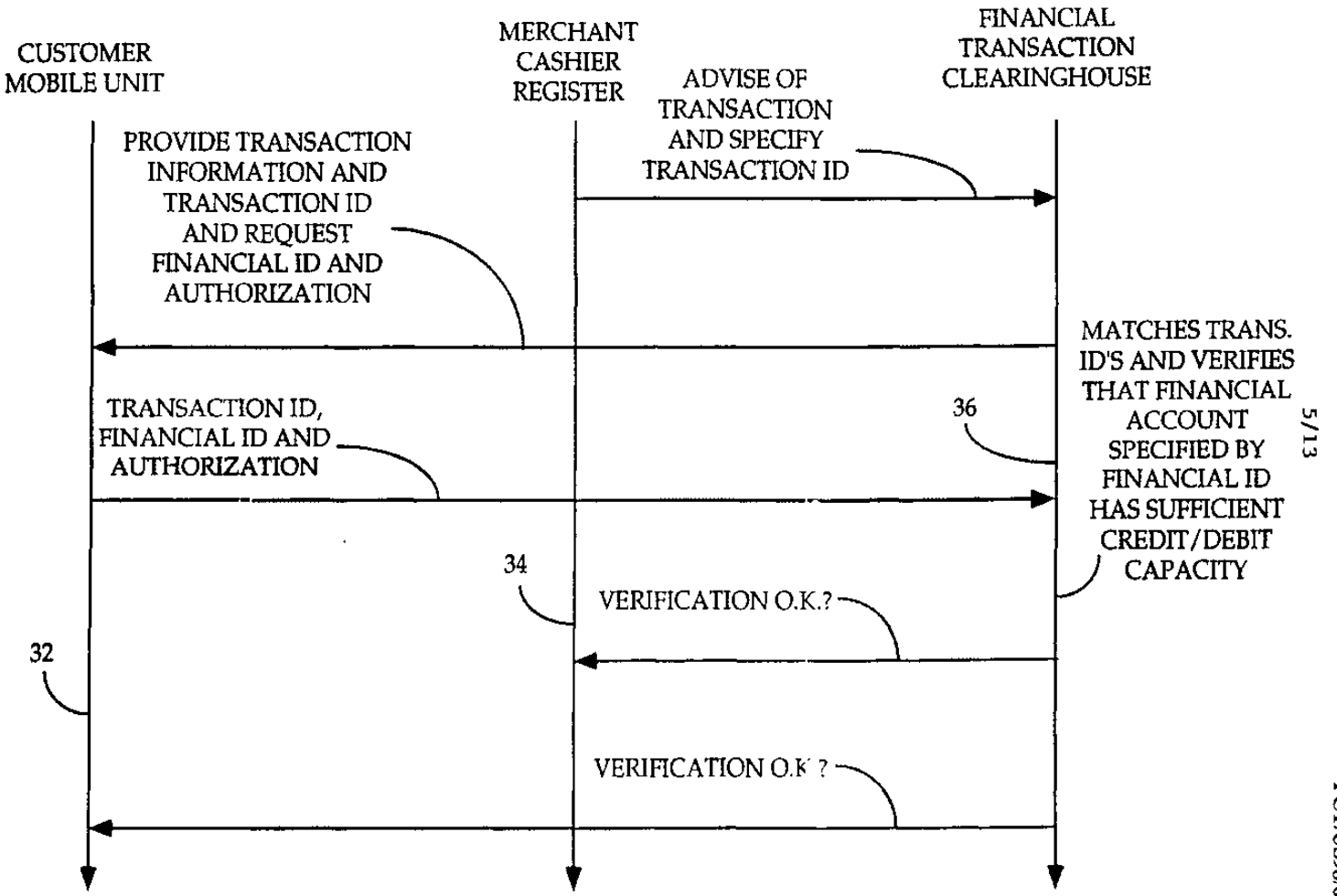


FIG. 5

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 569 of 1360

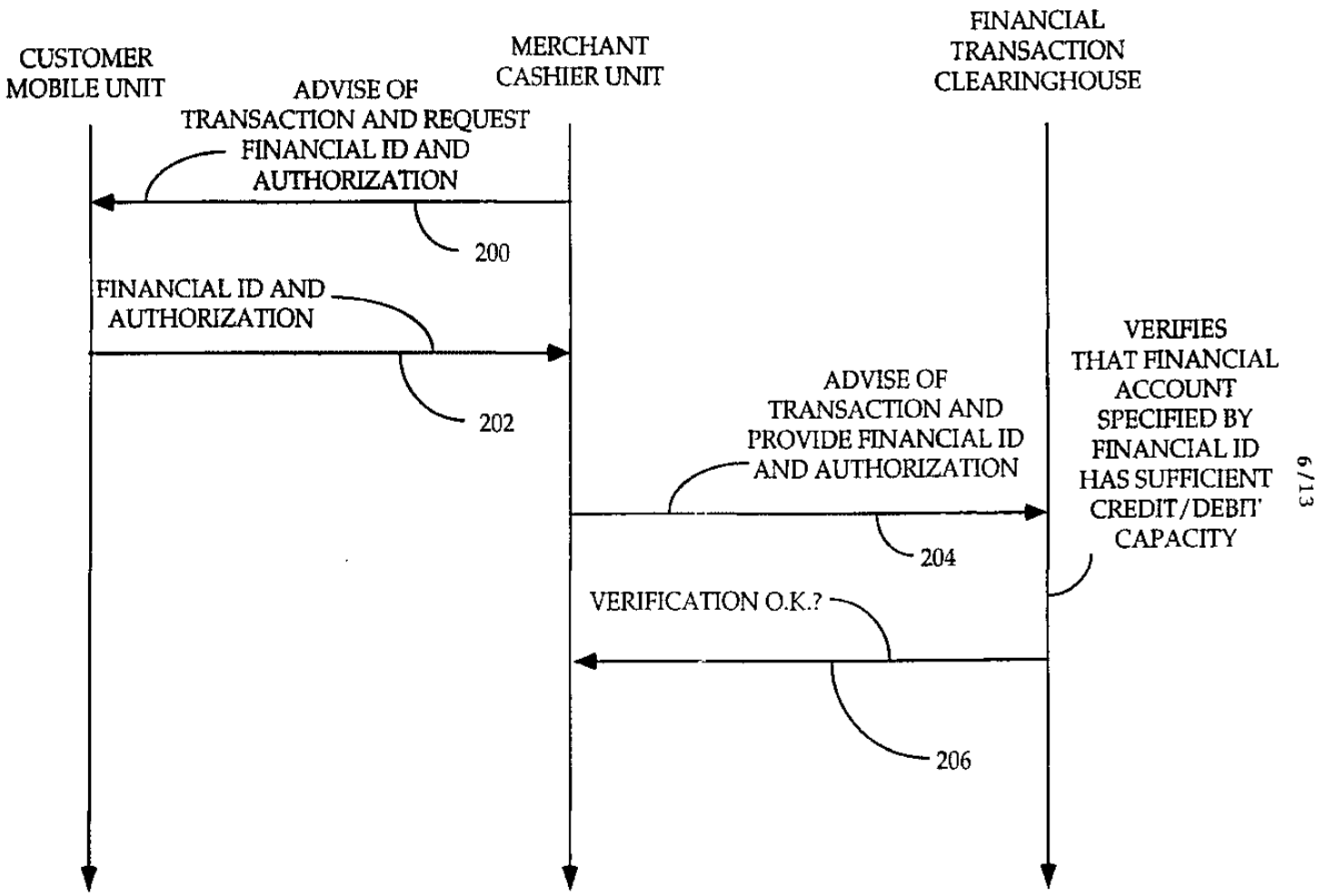


FIG. 6

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 570 of 1360

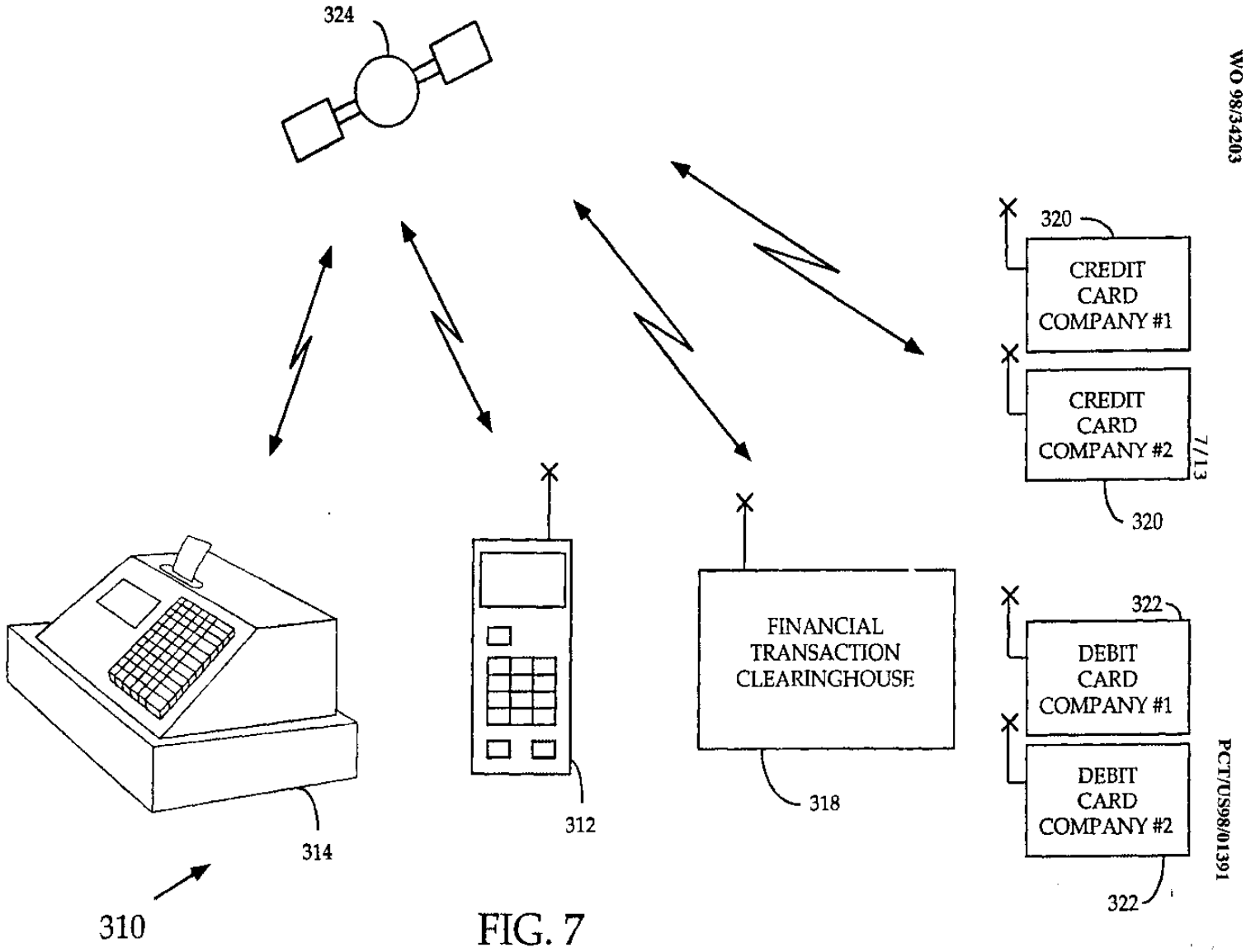


FIG. 7

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 571 of 1360

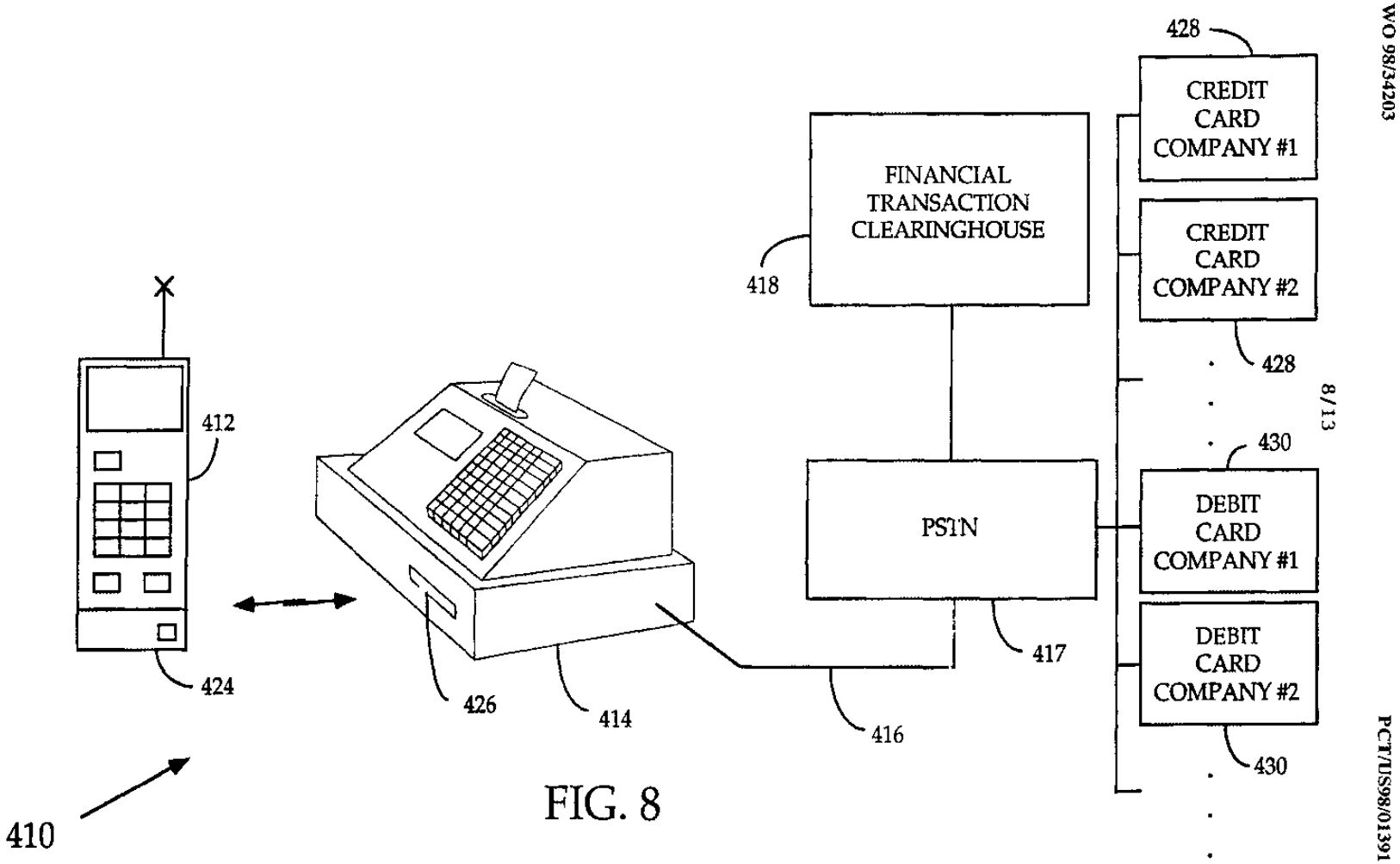


FIG. 8

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 572 of 1360

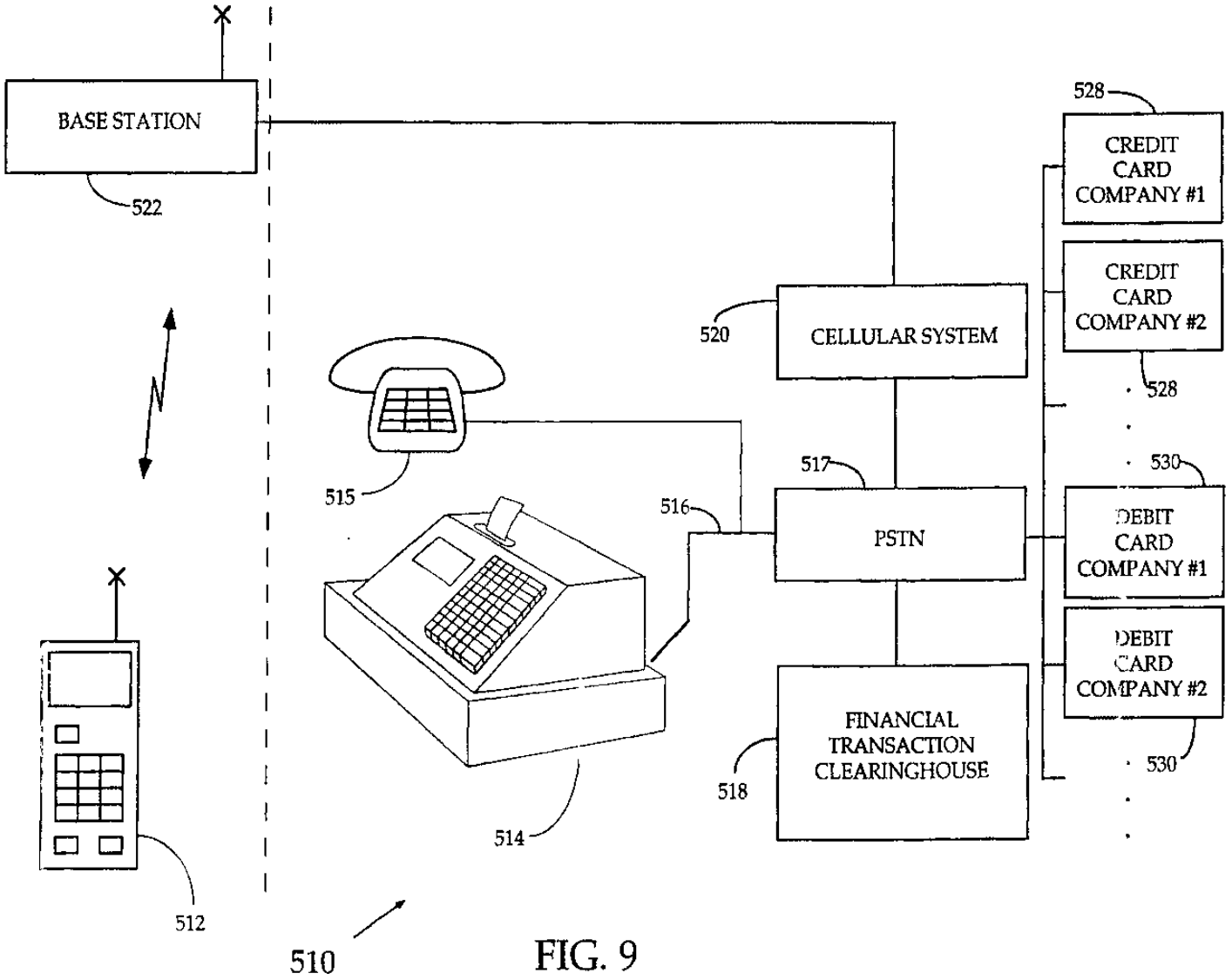


FIG. 9

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 573 of 1360

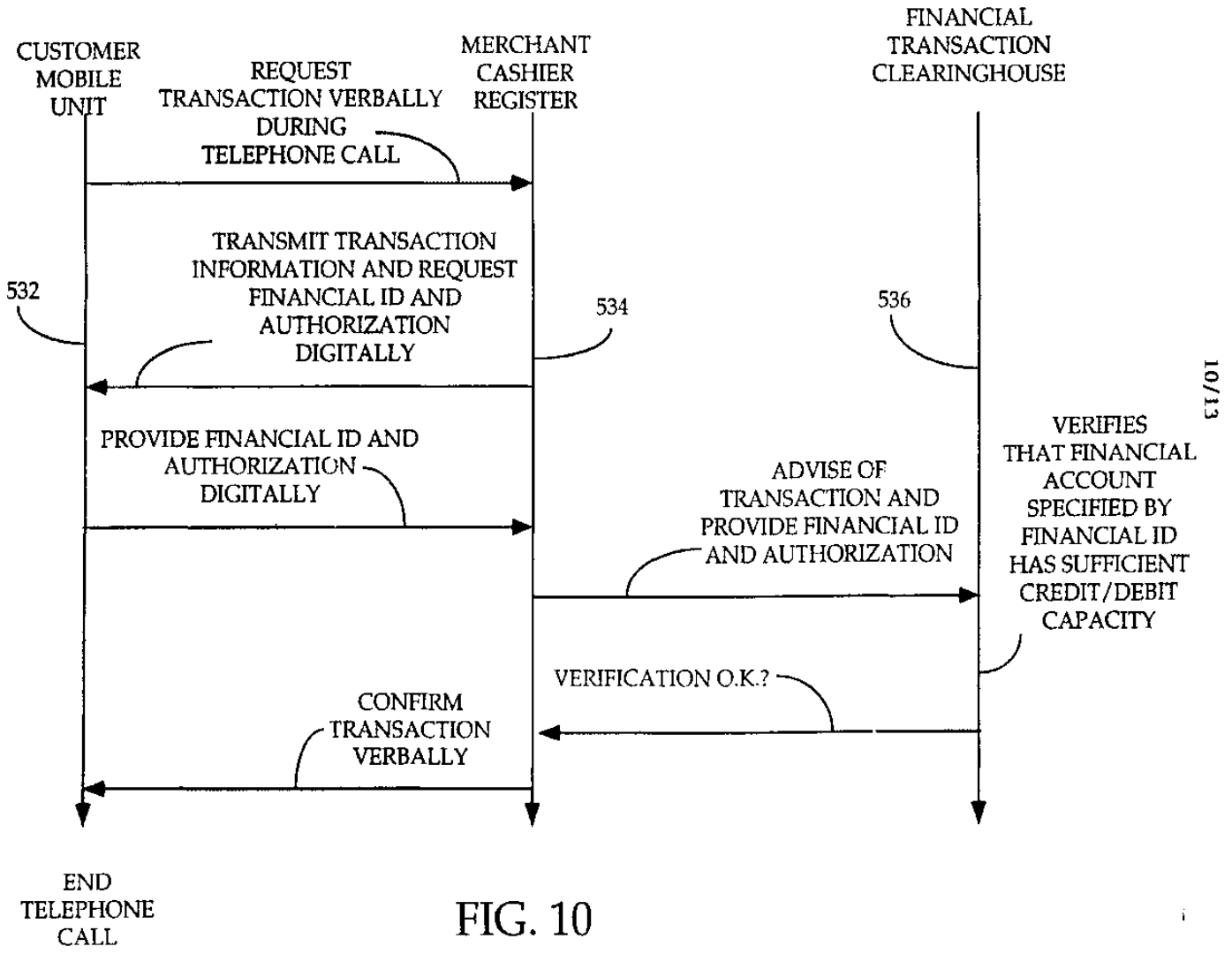


FIG. 10

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 574 of 1360

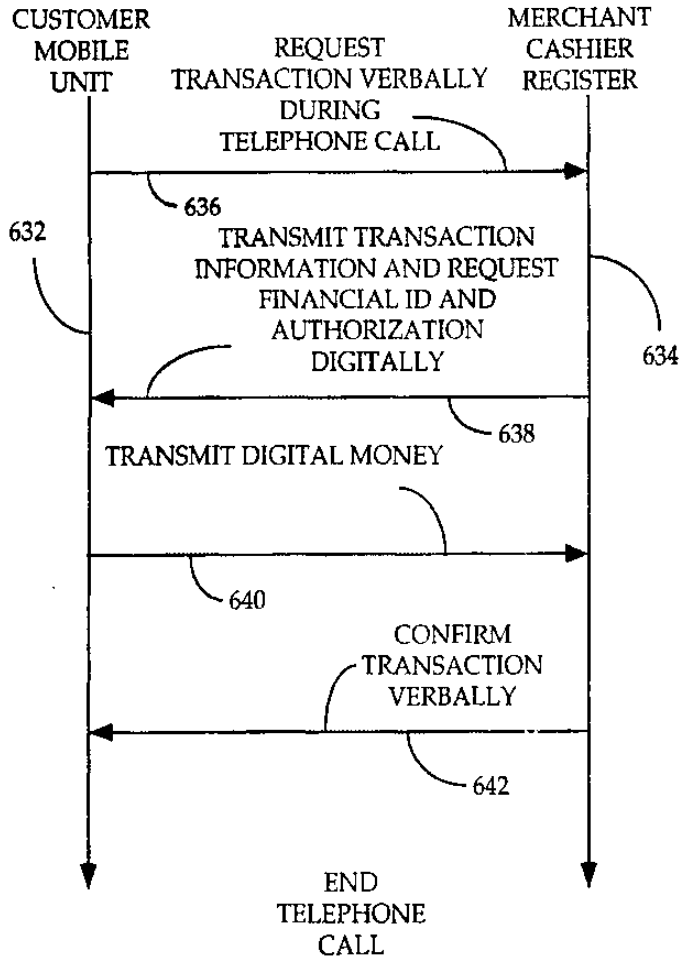


FIG. 11

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 575 of 1360

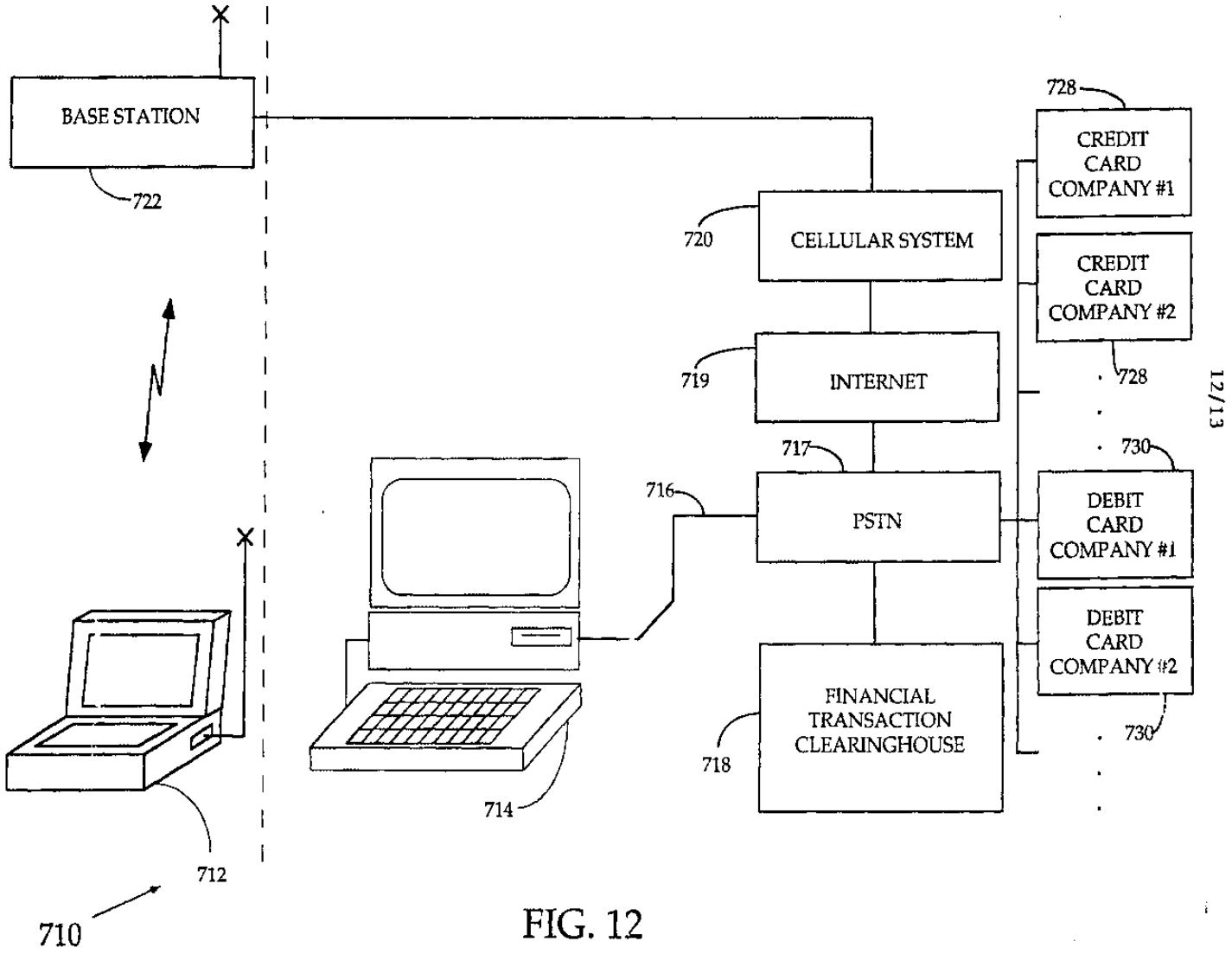


FIG. 12

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 576 of 1360

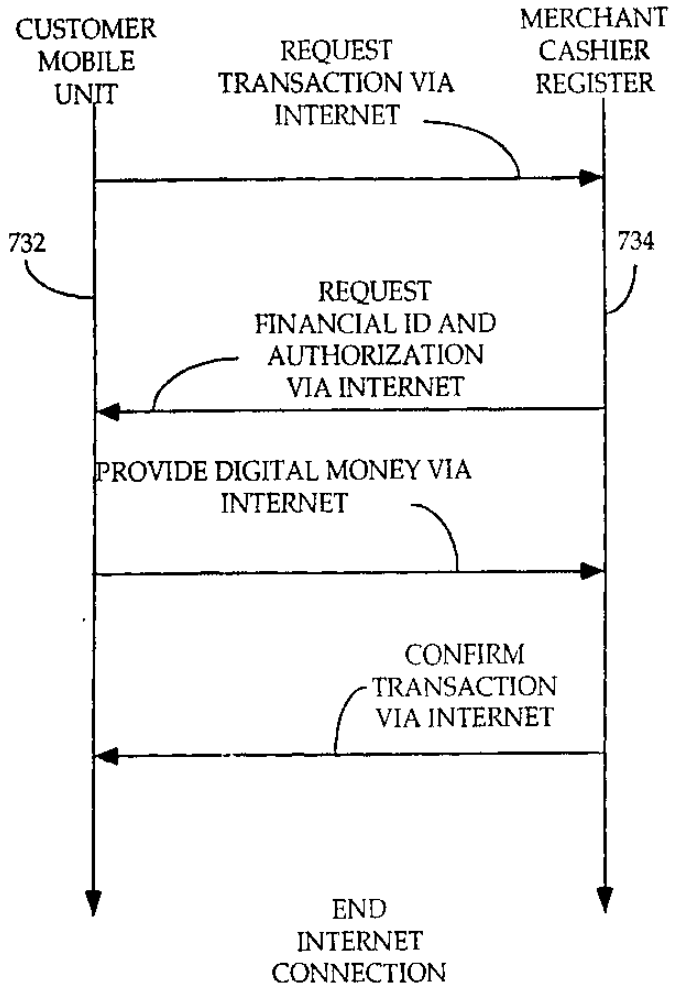


FIG. 13

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 577 of 1360

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/01391

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F19/00 H04M17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	WO 96 25828 A (NOKIA MOBILE PHONES) 22 August 1996 see abstract; claims; figures 1,6,7 see page 13, line 3 - page 19, line 28	1,3-7, 21,23-27 8,10-15, 19,20, 28,30-35
A	WO 94 11849 A (H.T. VATANEN) 26 May 1994 see abstract; claims; figures see page 5, line 36 - page 11, line 10	1,3,5,6, 9,10, 12-15, 19-21, 23,25, 26,29, 30,32-35
A	EP 0 708 547 A (AT & T) 24 April 1996	

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate 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 theinternational search	Date of mailing of the international search report
7 July 1998	15/07/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

1

Form PCT/ISA/210 (second sheet) (July 1992)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 578 of 1360

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/01391

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 13814 A (B. VAZVAN) 9 May 1996	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 579 of 1360

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/01391

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9625828 A	22-08-1996	FI 950685 A	16-08-1996
		AU 4624796 A	04-09-1996
		EP 0809916 A	03-12-1997
WO 9411849 A	26-05-1994	FI 925135 A	12-05-1994
		FI 934995 A	12-05-1994
		AT 159602 T	15-11-1997
		DE 69314804 D	27-11-1997
		EP 0669031 A	30-08-1995
		ES 2107689 T	01-12-1997
		NO 951814 A	09-05-1995
EP 0708547 A	24-04-1996	US 5608778 A	04-03-1997
		CA 2156206 A	23-03-1996
		JP 8096043 A	12-04-1996
WO 9613814 A	09-05-1996	FI 945075 A	29-04-1996
		EP 0739526 A	30-10-1996
		FI 962553 A	25-11-1997
		FI 962961 A	28-08-1996
		FI 971009 A	26-04-1997
		FI 971248 A	26-04-1997
		FI 971848 A	30-04-1997

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 580 of 1360

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 September 2005 (01.09.2005)

PCT

(10) International Publication Number
WO 2005/079254 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/004049

(22) International Filing Date: 10 February 2005 (10.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/544,300	17 February 2004 (17.02.2004)	US
60/549,148	3 March 2004 (03.03.2004)	US
60/575,835	2 June 2004 (02.06.2004)	US
11/045,484	31 January 2005 (31.01.2005)	US

(71) Applicant *(for all designated States except US)*: **FUJITSU LIMITED** [JP/JP]; 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 (JP).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LABROU, Yannis** [GR/US]; 519 West Pratt Street, #410, Baltimore, MD 21201 (US). **JI, Lusheng** [CN/US]; 15 Berry Lane, Randolph, NJ 07869 (US). **AGRE, Jonathan, Russell** [US/US]; 800 Brighton Knolls Drive, Brinklow, MD 20862 (US). **MOLINA TERRIZA, Jesus** [ES/US]; 1000 6th Street, Southwest, #704, Washington, DC 20024 (US). **CHEN, Wei-Lun** [CN/US]; 440 Ridge Road, #4, Greenbelt, MD 20770 (US).

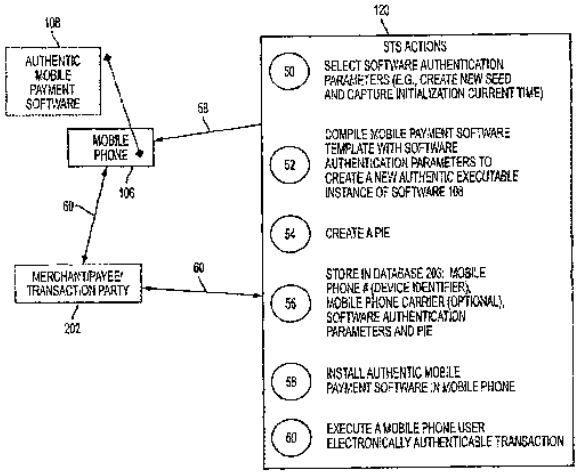
(74) Agent: **SHEIKERZ, Mehdi, D.**; Staas & Halsey LLP, Suite 700, 1201 New York Avenue, Washington, DC 20005 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: WIRELESS WALLET



(57) **Abstract:** A mobile phone system and method of initializing, at a secure transaction server (STS), a mobile payment software with a software authentication parameter, as an authentic mobile payment software; providing an STS correlation between a personal identification entry (PIE) and the authentic mobile payment software; installing, in a mobile phone, the authentic mobile payment software; and inputting, by a user, the PIE to the installed authentic mobile payment software to generate according to the PIE and the software authentication parameter a transformed secure authenticable mobile phone cashless monetary transaction over the mobile phone network, as a mobile phone wireless wallet of the user of the mobile phone. The mobile phone authenticable cashless monetary transaction is performed according to an agreement view(s) protocol.

WO 2005/079254 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 581 of 1360

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WIRELESS WALLET

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] This application is related to and is a continuation-in-part of US application no. 10/458,205, filed June 11, 2003, which claims the benefit of US provisional application no. 60/401,807, filed August 8, 2002; and also a continuation-in-part of US application no. 10/628,584 filed July 29, 2003, which claims the benefit of US provisional application no. 60/401,807 filed August 8, 2002; and also a continuation-in-part of US application no. 10/628,569 filed July 29, 2003, which claims the benefit of US provisional application no. 60/401,807 filed August 8, 2002; and also a continuation-in-part of US application no. 10/628,583 filed July 29, 2003, which claims the benefit of US provisional application no. 60/401,807 filed August 8, 2002.

[0002] This application is also related to and also claims the benefit of priority to, Provisional Application U.S. Serial Number 60/544,300, Attorney Docket No. 1634.1002P2, entitled A UNIVERSAL PERVASIVE TRANSACTION FRAMEWORK APPLICATION: WIRELESS WALLET ON A MOBILE PHONE, by Yannis Labrou, Jonathan Agre, Lusheng Ji, Jesus Molina Terriza, Wei-lun Chen, and, filed February 17, 2004 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0003] This application is also related to, and also claims the benefit of priority to, Provisional Application U.S. Serial Number 60/549,148, Attorney Docket No. 1634.1002P3, entitled WIRELESS WALLET, by Yannis Labrou, Jonathan Agre, Lusheng Ji, Jesus Molina Terriza, Wei-lun Chen, and, filed March 3, 2004 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0004] This application is also related to, and also claims the benefit of priority to, Provisional Application U.S. Serial Number 60/575,835, Attorney Docket No. 1634.1002P4, entitled A WIRELESS WALLET FOR PERSON-TO-PERSON TRANSACTIONS, by Yannis Labrou, Jonathan Agre, Lusheng Ji, Jesus Molina Terriza, Wei-lun Chen, and, filed June 2, 2004 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0005] This application is related to Provisional Application U.S. Serial Number 60/401,807, Attorney Docket No. 1634.1002P, filed August 8, 2002 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0006] This application is related to U.S. Serial Number 10/458,205, Attorney Docket No.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 583 of 1360

1634.1003, entitled SECURITY FRAMEWORK AND PROTOCOL FOR UNIVERSAL PERVASIVE TRANSACTIONS, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed June 11, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0007] This application is related to U.S. Serial Number 10/628,584, Attorney Docket No. 1634.1002, entitled METHODS FOR PURCHASING OF GOODS AND SERVICES, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed July 29, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0008] This application is related to U.S. Serial Number 10/628,569, Attorney Docket No. 1634.1004, entitled APPARATUSES FOR PURCHASING OF GOODS AND SERVICES, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed July 29, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0009] This application is related to U.S. Serial Number 10/628,583, Attorney Docket No. 1634.1005, entitled FRAMEWORK AND SYSTEM FOR PURCHASING OF GOODS AND SERVICES, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed July 29, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0010] The present invention is directed to wireless computing device authenticable transactions, for example, authenticable cashless monetary transactions. For example, a mobile phone wireless wallet.

2. Description of the Related Art

[0011] The future ubiquitous computing environment will consist of mobile users with information computing appliances (mobile devices), such as cellular phones or Personal Digital Assistants (PDA's), that will be wirelessly communicating and interacting with the varied services and devices encountered at any particular moment and place. Many applications that operate in such environments have been proposed from the research and business community, but there has not yet been a strong market pull for any particular one. It is apparent that a crucial enabler for ubiquitous computing to emerge into the marketplace is the ability to safely conduct financial transactions using mobile devices in this form of environment.

[0012] However, mobile devices, and, in particular, mobile phones, can present certain characteristics, such as limited capabilities (computation power, communication bandwidth,

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 584 of 1360

battery capacity, small display, limited keyboard, etc), a typical user who is not technically savvy and cannot be overly burdened with a complex application for executing transactions with other parties, and a wireless transport network that is deemed insecure at the network layer.

[0013] There have been many approaches and solutions proposed for the mobile commerce (m-commerce) problem. A few small manufacturers have offered Wireless Local-Area Network (WLAN)-enabled mobile phones and both MOTOROLA and NOKIA have made announcements of plans to offer such phones in 2004.

[0014] The current m-commerce practice involves Web Store-Front Payment, in which a consumer pays for goods or services offered by a retailer that has Internet presence. For web pages that are specially prepared for mobile devices, such as those that are WAP-enabled, one could use the mobile device to make a purchase as it is normally done in e-commerce transactions using a web browser on a personal computer. But, since payment typically requires logging in and typing a username and password, this approach is impractical and inefficient on a mobile device, even if the transaction uses Wireless Application Protocol (WAP) and has occurred through a secured network link such as through https or Secure Socket Layer (SSL). In many current web browsing applications, the consumer can pre-register one or more financial accounts with a merchant to save time and avoid repeatedly entering ones financial information, but this approach requires a consumer to register multiple user account information with multiple merchants. Further, in case of a physical point-of-sale (POS) case it is too complex to deploy from a business point of view because it frequently involves integration with the back-end store systems and some form of binding between the payer and the physical goods purchased.

[0015] From a data security perspective, existing m-commerce data security solutions rely on Public Key Infrastructure (PKI) technologies. However, PKI solutions suffer from poor computational performance in mobile device environments and complexity of the user experience. There are many different ways PKI can be used for mobile payments. One proposed PKI-based solution for mobile payments is by MET LIMITED, which is discussed at [www.mobiletransaction.org, retrieved on January 5, 2005]. Under existing m-commerce security solutions, a user signs a transaction (a purchase order) with a certificate that authenticates the identity of the user (it is unclear whether each user has a single such certificate or a variety of them, each for every eligible account). For example, handling of multiple security certificates from many vendors is confusing, at best, and can be dangerous if left up to the user. Since these certificates are stored on the mobile device, the certificate store needs to be protected and "unlocked" on a per use basis. If the certificate storage is

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 585 of 1360

implemented in software the key used to unlock the storage should be of sufficient length to protect this storage, or it can be instead implemented in hardware, which in case of a mobile phone would require the phone to be designed for this purpose. Such an approach requires an infrastructure for dissemination of certificates (including revocation), possibly specialized mobile phones and possibly some basic understanding by the user of certificates and their usage.

SUMMARY OF THE INVENTION

[0016] The embodiments described herein relate to wireless mobile computing device user electronically authenticable transactions, for example, mobile phone user authenticable cashless monetary transactions. For example, a user mobile phone wireless wallet.

[0017] A mobile phone system and method of initializing, at a secure transaction server (STS), a mobile payment software with a software authentication parameter, as an authentic mobile payment software; providing an STS correlation between a personal identification entry (PIE) and the authentic mobile payment software; installing, in a mobile phone, the authentic mobile payment software; and inputting, by a user, the PIE to the installed authentic mobile payment software to generate according to the PIE and the software authentication parameter a transformed, secure authenticable mobile phone cashless monetary transaction over a mobile phone network, as a mobile phone wireless wallet of the user of the mobile phone. The mobile phone authenticable cashless monetary transaction is performed according to an agreement view(s) protocol.

[0018] The above as well as additional aspects and advantages will be set forth in part in the description which follows and, in part, will be obvious from the description, or may be learned by practice of the described embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] These together with other aspects and advantages which will be subsequently apparent, reside in the details of construction and operation as more fully hereinafter described and claimed, reference being had to the accompanying drawings forming a part hereof, wherein like numerals refer to like parts throughout.

FIG. 1A is a flow chart of activating a mobile phone cashless monetary transaction capability, according to an embodiment of the present invention.

FIG. 1B is a flow chart of activating a mobile phone cashless monetary transaction capability, according to another embodiment of the present invention.

FIG. 1C is a diagram of mobile phone display screen user interface images to activate a mobile phone cashless monetary transaction, according to an embodiment of the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 586 of 1360

present invention.

FIG. 2 is a functional block diagram of Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) system architecture to execute a mobile device cashless monetary transaction, according to an embodiment of the present invention.

FIG. 3 is functional block diagram of a UPTF based system architecture to execute a mobile phone cashless monetary transaction with a physical point of sale (POS), according to an embodiment of the present invention.

FIG. 4 is a diagram of UPTF cashless monetary transaction messages based upon Secure Agreement Submission (SAS) protocol to execute a mobile phone cashless monetary transaction, according to an embodiment of the present invention.

FIG. 5 is a flow chart of a UPTF based mobile phone cashless monetary transaction with a merchant, according to an embodiment of the present invention.

FIG. 6 is a flow chart of a UPTF based mobile phone cashless monetary transaction to purchase a movie ticket, according to an embodiment of the present invention.

FIGS. 7A-B are mobile phone display screen user interface images to execute mobile phone cashless monetary transaction to purchase a movie ticket, and to obtain, store, and retrieve a transaction receipt, according to an embodiment of the present invention.

FIG. 8 is a flow chart based upon mobile phone display screen user interface images and message flow between a requestor device, a secure transaction server (STS) and a requestee to execute a person-to-person mobile phone cashless payment transaction, according to an embodiment of the present invention.

FIG. 9 is a flow chart based upon mobile phone display screen user interface images and message flow between a requestor device, a secure transaction server (STS) and a requestee to execute a person-to-person mobile phone cashless payment request transaction, according to an embodiment of the present invention.

FIG. 10 is overall mobile phone display screen user interface images and possible workflows available to an operator of a wireless wallet on a mobile phone to execute peer-to-peer cashless monetary transactions, according to an embodiment of the present invention.

FIGS. 11-12 are diagrams of mobile phone cashless monetary transaction message formats to execute various mobile phone person-to-person cashless monetary transactions, according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] Reference will now be made in detail to the present embodiments of the present invention, examples of which are illustrated in the accompanying drawings. The embodiments are described below to explain the present invention by referring to the figures.

[0021] Generally, there can be three classes of mobile commerce transactions, as follows:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 587 of 1360

[0022] 1. Person-to-person payments: A consumer can directly make an agreed upon payment to another consumer using their mobile devices.

[0023] 2. Web Store-Front Payment: A consumer pays for goods or services offered by a retailer that has an Internet presence. A user browses the retailer's web pages using a mobile device to identify the good or service to be purchased and then conducts payment. Examples of this case would be paying for a book or purchasing movie tickets through a web service.

[0024] 3. Physical Point-of-Sale (POS) purchase: A consumer pays a retailer at a check-out station using the mobile device, such as when making a payment at a "brick and mortar" store or restaurant.

[0025] The boundaries between these categories are malleable and their common properties can be exploited using the transaction agreement point of view. The embodiment(s) described herein accommodates these and/or other mobile commerce transactions.

[0026] In the described embodiments herein, a mobile device is any wireless handheld, or hand size, electronic computing device, including, without limitation, a mobile phone. The embodiment(s) described herein relate to wireless mobile computing device user electronically authenticable transactions based upon Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol, such as (without limitation) mobile phone user authenticable transactions that may or may not result in a financial settlement, and/or mobile phone user authenticable cashless financial/monetary transactions. For example, a user authenticable mobile phone wireless wallet. More particularly, according to an aspect of the embodiment(s) described herein, a wireless mobile computing device provides user electronically authenticable transactions according to time and software dependent secured (e.g., encrypted), matched (verified against each other), and transaction party anonymous, transaction view(s) of one or more parties (i.e., in a typical embodiment paired and/or more than two transaction views).

[0027] FIG. 1A is a flow chart of activating a mobile phone cashless monetary transaction capability, according to an embodiment of the present invention. A computer system and method for a wireless mobile computing device user electronically authenticable transactions (i.e., electronic authentication of a user and/or the user's transaction) comprises, at operations 50 and 52, initializing, at a secure transaction server (STS) 120, a mobile payment software template with software authentication parameter(s), as an authentic mobile payment software 108. At operations 54 and 56, correlating, at the STS

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 588 of 1360

120, a personal identification entry (PIE) and an identifier of a mobile phone 106 with the authentic mobile payment software 108. At operation 58, installing, in the mobile phone 106, the authentic mobile payment software 108. At operation 60, executing, at the mobile phone 106, the installed authentic mobile payment software 108 using the PIE to execute a mobile phone authenticable cashless monetary transaction as a mobile phone wireless wallet of a user of the mobile phone 106. More particularly, at operation 60, inputting by a user the PIE to the installed authentic mobile payment software to generate according to the PIE and the software authentication parameter, a transformed secure authenticable mobile phone cashless monetary transaction. According to an aspect of the embodiment described herein, at operation 50, one or more software authentication parameters are selected, which can be (without limitation) creation of a new seed, such as a new random seed number, and an initialization time. At operation 56, the STS 120 stores in a database 203, a unique identifier (referred to as Device ID, or DID) for the mobile phone 106, which can, for example, be a mobile phone number of the mobile phone 106 or some randomly generated globally unique identifier (GUID), a mobile phone carrier (as the case may be), the software authentication parameter(s) selected at operation 50, and the generated PIE. According to an aspect of the described embodiment, a mobile phone number can also be used as a device identifier for the mobile phone 106. The unique identifier (device ID (DID)) of the mobile phone 106 is used by the STS 120 to correlate a transaction message with authentic mobile phone payment software 108; to correlate the DID with the software authentication parameter(s) and the PIE stored at the STS 120 so that the STS 120 can generate a key that corresponds to a device 106 having the DID. The mobile phone number can be used to communicate (e.g., notifications, etc.) with the mobile phone 106 (e.g., Short Message Service (SMS) and/or Multimedia Message Service (MMS)). The mobile phone 106 can be an Internet enabled, according to known techniques, mobile phone. The PIE is described in more detail further below. The mobile phone authenticable cashless monetary transaction is performed according to an agreement view(s) protocol known as Universal Pervasive Transaction Framework (UPTF) (described in more detail below) and secured (e.g., encrypted) according to a protocol known as Secure Agreement Submission (SAS) (described in more detail below). According to an aspect of the embodiment(s) described herein, a transaction message is bound to a unique combination of a user and a device (e.g., mobile phone wireless wallet 106), the binding to the user is via the PIE and the binding to the device 106 is via the software authentication parameter(s) of the authentic mobile payment software 108. In particular, a transaction is an SAS based encrypted message and the encrypted message can be traced back to a combination of the user and the device 106 through the PIE and the software authentication parameter(s) of the authentic mobile payment software

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 589 of 1360

108.

[0028] FIG. 1B is a flow chart of activating a mobile phone cashless monetary transaction capability, according to another embodiment of the present invention. In FIG. 1B, a computer system and method comprises, at operation 100, providing to a user a mobile phone cashless monetary transaction activation link at a computing device 102 (sign-up application 102), at operation 104, registering a phone number of a mobile phone 106 of the user via the activation link, at operation 105, associating a mobile payment software 108 with software authentication parameters, as an authentic mobile payment software 108, and, at operation 110, providing a correlation between a personal identification entry (PIE) and the authentic mobile payment software 108, at the STS 120. At operation 112, a mobile phone download link to the mobile payment software 108 is transmitted to the mobile phone 106, using the registered phone number of the mobile phone 106. At operation 114, the mobile payment software 108 is downloaded to the mobile phone 106 via the download link. At operation 116, the user can activate the downloaded mobile payment software 108 using an optional activation code. After installation of the authentic mobile payment software 108, as a user mobile phone wireless wallet 106 of the mobile phone user (i.e., a mobile phone wireless wallet application 108), the user can execute a mobile phone user electronically authenticable cashless monetary transaction using the user mobile phone wireless wallet 106.

[0029] The mobile payment software 108 is implemented according to an application platform of the mobile phone 106. For example, the mobile payment software 108 can be implemented according to Java 2 Platform Micro Edition (J2ME). According to an aspect of the embodiment described herein, at operation 112, the mobile payment software downloaded link is transmitted to the mobile phone 106 using short message service (SMS) and/or multimedia message service (MMS).

[0030] In FIG. 1B, after operation 116, a mobile phone cashless monetary transaction may be performed according to Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol. The UPTF SAS protocol is discussed in related commonly assigned pending US patent application nos. 10/458,205, filed June 11, 2003; 10/628,584, filed July 29, 2003; 10/628,569, filed July 29, 2003; and 10/628,583, filed July 29, 2003, owned by FUJITSU LIMITED assignee of the present Application, the entire disclosures of all of which are hereby incorporated herein by reference.

[0031] In FIG. 1B, at operation 105, the associating of the mobile payment software 108 with the software authentication parameters comprises generating a UPTF random number identifier by a provider 122 of the mobile phone cashless monetary transaction activation, so

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 590 of 1360

that the UPTF random number can be associated with the user and transmitting the UPTF random number identifier and the registered phone number of the mobile phone 106 to a secure transaction server (STS) 120. For example, at operation 105, in case the provider 122 is a payment service 122 at which a transaction party (a user) registers financial account information, the payment service 122 can assign a UPTF random number identifier (abstracted identifier) 123 to identify the user when communicating with the STS 120. Accordingly, the STS 120 can communicate with the provider 122 to execute a UPTF based transaction based upon the provider 122 UPTF random number and without knowledge of actual transaction party account information. Further, operation 110, comprises generating, by the STS 120, an executable mobile payment software including the initialization parameters, as the authentic mobile payment software, and generating the PIE that is correlated in the STS with the authentic mobile payment software 108. At operation 112, the transmitting of the mobile payment software download link comprises transmitting, by the STS 120, via short message service (SMS) the mobile payment software 108 download link to the mobile phone 106 of the user; and providing, by the STS 120, the PIE to the user. The described embodiment is not limited to the above-described authentic mobile payment software 108 generation, activation, and installation, and, at operation 58, an authentic mobile payment software 108 can be installed or provided for a mobile phone 106 via mobile phone removable/installable (e.g., smart card) and/or embedded computer readable media, embedded in a mobile phone computing processor, via an emailed download link, emailed attachment, etc.

[0032] FIG. 1C is a diagram of mobile phone display screen user interface images to activate a mobile phone cashless monetary transaction, according to an embodiment of the present invention. User interface screen image 150 is displayed at operation 112, when the mobile phone 106 receives an SMS message from the STS 120 on behalf of the provider 122. User interface screen image 152 displays the received SMS message directing the mobile phone user to go to an Internet address to download the authentic wireless wallet software 108. The user interface screen image 154 is displayed after operation 114, when downloading of the authentic wireless wallet software 108 to the mobile phone 106 is completed. The user interface screen image 156 is displayed when installing the authentic wireless wallet software 108. The user interface screen image 158 is displayed at operation 116, when an optional activation code for the authentic wireless wallet software 108 has been provided to be input at the mobile phone 106. After input of the activation code via the user interface screen image 158, the user interface screen image 160 is displayed, confirming to the user that the authentic wireless wallet software 108 has been activated and ready for executing mobile phone user electronically authenticable cashless monetary

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 591 of 1360

transactions.

[0033] According to an aspect of the described embodiment herein, at operation 100, a provider 122, such as an online payment system/service, a merchant/service provider, a financial institution, etc., provides the mobile phone cashless monetary transaction activation link to a member of the provider 122 as the user. In case of an online payment system 122, the described embodiment provides member-to-member mobile phone cashless monetary transactions using the user mobile phone wireless wallet 108.

[0034] According to an aspect of the described embodiment herein, at operation 110, the STS 120 sends the PIE to the provider 122, and, at operation 111, the provider 122 receives the PIE and displays the PIE to the user at the computer 102. At operation 111, for additional security, the PIE might only be an image so that the provider 122 does not know the PIE, thereby allowing for anonymity of the transaction parties. The PIE can be delivered according to other secured ways, such as mail, email, a customer service representative, etc.

[0035] Therefore, with reference to FIGS. 1A and 1B, in an unlimiting example, the wireless wallet application 108 is implemented as a J2ME application than can be downloaded and executed on the mobile phone 106 and enables users to make purchases and payments leveraging Universal Pervasive Transaction Framework (UPTF). Currently, many mobile phones offered by carriers in the US are J2ME enabled and web-enabled, such that the wide-spread availability of J2ME on mobile phones enables new business models with respect to the delivery of content and services to mobile users. With J2ME, anyone can develop downloadable J2ME applications for custom content or service delivery to the mobile. This is the case of the wireless wallet application 108, which allows offering the service of secure payments using mobile phones 106.

[0036] The J2ME wireless wallet application is a relatively small application (typically according to the present invention less than 90 Kbytes) which combines the functionality of a web browser (for example, a cHTML web browser) and that of the purchasing application that implements the UPTF SAS framework and security protocol. It allows mobile users to enable or disable the payment functionality and to store receipts of purchase. The wireless wallet method can be offered by any retailer or payment service in order for consumers to make payments with their mobile phone. It is a completely software solution to the problem of secure payments using a mobile device. If the provider of the wireless wallet is a web store-front retailer, such as a movie ticket provider, the wireless wallet application 108 can be used to make payments with any of the accounts registered with the retailer. If the provider is an Online Payment Service, the wireless wallet software 108 can be used to make

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 592 of 1360

payments to other online payment service users (person-to-person) or to "brick and mortar" retailers that accept payment with this payment service or a central service/system that can interface a plurality of payment services. In the latter case, the merchant can use a merchant's version of the wireless wallet client 108 to specify transaction information, such as the payment amount. The issue of identifying what is being paid for by the consumer via a mobile phone 106 is addressed by having the consumer enter a receipt number (e.g., as printed in the receipt of the restaurant where the meal is paid for) and/or a merchant identifier (e.g., a phone number of the merchant, including merchant POS identifier, etc.) on their wireless wallet application 108 to interface with the merchant retail application software; the goal being to bind a virtual shopping cart to a specific consumer.

[0037] A more detailed mobile payment software 108 download and activation is described as follows:

[0038] 1. After a user logs into a Provider's 122 web site using a computer device, such as personal computer 102, the option of using one's mobile phone for payments is presented and the user is re-directed to a page where one is asked for a phone number of the mobile phone to be used for mobile phone cashless money payments.

[0039] 2. The Provider 122 generates a UPTF_ID (random number) for the already captured username and password (operation 105) and sends to the STS 120 the UPTF_ID and mobile number. Therefore, in this example, the Provider 122 does not have to share with the operator of the STS 120 real account information of the user, but the provider 122 and the STS 120 relate transactions to a user based upon a random identifier generated by the provider 122.

[0040] 3. The STS 120 then creates a new wireless wallet executable 108 (with "fresh" initialization parameters per the UPTF requirements), a link to download this executable, an optional activation code, and a personal identification entry (PIE), all of which are correlated at and maintained by the STS 120 (operations 50-56 and 110). The STS 120 can send the PIE to the Provider 122.

[0041] 4. If the STS 120 sends the PIE to the Provider 122, the PIE is received by the provider 122 and displayed to the user (operation 111). Optionally, the STS 120 can provide an activation code to the user via SMS (e.g., at operation 116) or via the provider 122 (e.g., at operation 111). Alternatively, the PIE and the activation code (as the case may be) can be communicated to the user through channels other than the provider 122 or SMS, for example, via mail, email, etc. Typically in the present invention, the activation code is a number (for easier user entry) and used as a one time password that encrypts the UPTF-

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 593 of 1360

related initialization parameters of the downloaded software 108, so that if a third party attacker intercepts the software while in transit, the attacker cannot have access to the device-specific initialization parameters.

[0042] 5. The STS sends a Short Message Service (SMS) message to the previously entered mobile's phone number with the download link (operation 112).

[0043] 6. The mobile user downloads the wireless wallet software 108 (e.g., at operation 114, the link can be easily followed directly from the SMS text itself) and subsequently uses the wireless wallet software 108 (operation 116). An initial activation can involve using the activation code. Otherwise, at operation 116, the user can subsequently use the wireless wallet software 108 to execute a mobile phone cashless monetary transaction by using only the PIE.

[0044] After operation 114 (after downloading wireless wallet application 108 into the mobile phone 106), the wireless wallet 108 is ready for use; purchases and/or financial transactions can be paid for with any of the accounts registered with the wireless wallet provider 122. This scheme for distributing the software ensures a secure distribution of the software, on request, and a safe dissemination of the PIE. A mobile phone wireless wallet software 108 distribution model has been implemented for downloading and installing a J2ME executable on the mobile phone 106. Operation of the software 108 is very easy and transaction time largely depends on the speed of the mobile phone carrier's network. Based on tests, a mobile phone cashless monetary transaction time can vary between 30 and 45 seconds, the differences due to a mobile carrier's network-related delays. The traffic generated by the mobile payment software application 108 (following the determination of what is purchased) is less than 1KByte (send/receive) for each transaction, as each mobile phone cashless monetary transaction message can be smaller than 256 bytes. In an unlimiting example, communication between the mobile phone 106 and the STS 120 during payment was routed either through a provider 122 or directly to the STS 120 (depending on the type of financial transaction and as will be described in more detail below) and was carried over Internet Hypertext Transfer Protocol (HTTP) on a mobile phone communication network. More particularly, because the UPTF SAS security is session-less based upon message view (as described in more detail below) encryption (i.e., not based upon communication session security), such as secure socket layer (SSL), secured transaction processing efficiency by the mobile phone 106 is substantially improved.

[0045] FIG. 2 is a functional block diagram of Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) system architecture to execute a mobile device cashless monetary transaction, according to an embodiment of the present

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 594 of 1360

invention. In FIG. 2, colors are used to highlight features/concepts described herein. The Universal Pervasive Transaction Framework (UPTF) defines a system architecture based upon independent and anonymous transaction agreement views and a communication security protocol called the Secure Agreement Submission (SAS) protocol to transmit the views. Essentially the UPTF offers a vessel, which is able to securely carry the individual views of a transaction agreement from each party involved in the transaction to a trusted third party for verification, using a communication network which may consist of insecure segments such as wireless LANs or cellular links. When used for financial applications, such as the electronic wireless wallet, the transaction parties are payer 200 and a payee 202, for example, a customer payer 200 and a merchant payee 202, and a typical example of an "agreement" may read: "Party A will pay Party B $X for item Y."

[0046] The UPTF SAS protocol encrypts/decrypts a transaction message using a symmetric, secret-key approach where the secret key is producible only by an individual party's device 106 and a trusted third party (e.g., implemented as STS 120) and without transmission of the secret key among the parties. In other words, the UPTF SAS provides an implicit user authentication, because decryption by a trusted third party, such as STS 120, of a sending party's encrypted message, authenticates the sending party. The SAS insures that the authenticity of the parties is verified and during delivery, the privacy of the information is preserved (transaction party anonymity), even when the parties distrust each other and the messages from one party may be forwarded by the other to the third party verification. The UPTF also provides the mechanism for the trusted third party to verify that the independent views of the agreement are consistent with each other.

[0047] After the agreement data is extracted from the transaction views received from the parties and the data is verified by the trusted third party, further actions may need to be taken to actually execute the agreement. This is realized by the trusted third party interacting with the financial institutions associated with the payer 200 and the payee 202 to cause the transfer of the specified funds between the customer payer 200 and the merchant payee 202.

[0048] The wireless wallet UPTF system architecture is shown in FIG. 2 and comprises: a Payer 200 operating a UPTF device (called a UPTD), such as a mobile phone 106 loaded with a mobile phone wireless wallet 108, a Payee 202 operating another UPTF device, a Secure Transaction Server (STS) 120, a number of financial institutions 204, and several communication channels among them. For example, the payer 200 operates the mobile phone wireless wallet 106 to interact with the Payee 202 to determine the details of a purchase transaction and executes the UPTF protocol and its corresponding security

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 595 of 1360

operations SAS. The mobile phone wireless wallet 106 can support wireless communication capability necessary for discovering/interfacing with the payees 202 via service spots of the payees 202 (a place where a signal can exist to connect to the mobile phone wireless wallet 106). The wireless communication capability of the mobile phone wireless wallet 106 to communicate with a service spot payee 202 and/or an STS 120 can be wireless local area network (WLAN) and/or mobile phone communication (cellular) network. The mobile phone wireless wallet 106 can also have a user interface for interacting with the payee 202 through some common application and to the STS 120 as needed. The Payee 202 can also operate a UPTD, such as a merchant transaction server (MTS) 302 that implements a retail application, and is responsible for interacting with the payer 200, executing the UPTF protocol and its corresponding security operations and interacting with the STS 120. In FIG. 1B, in case the provider 122 is an online payment system, the provider 122 would correspond to the financial institutions 204 of FIG. 2, which allows any type of UPTD person-to-person cashless monetary transactions via Channels A, B, and C as logical communication channels. Of course, the STS 120 and the financial institutions 204 might be implemented by a single entity or separate entities, as the case may be.

[0049] According to an aspect of the embodiment described herein, the STS 120 is a backend verification server on which both the payer 200 and the payee 202 have registered and provided identifying account information that is maintained in a secure STS database 203. The secret information used for encrypting the messages to/from each payer 200 and payee 202 are also stored in this DB 203. The STS 120 receives independently generated UPTF SAS transaction views (described in more detail further below) from both the payer 200 and the payee 202 regarding a financial transaction conducted between them. The STS 120 is able to decode both of the views using information from UPTF SAS cashless monetary transaction messages and the information stored in the STS 120 database 203. Following successful decoding, the STS 120 verifies that the view messages are original, authentic, involve the intended payer 200 and payee 202 and that the information fields in the agreement views are consistent with each other. The STS 120 will maintain a log of messaging activity for non-repudiation purposes.

[0050] In FIG 2, a generic set of communication channels are explicitly indicated. The indicated communication channels reflect anonymity of the transaction party communications (anonymous transaction party communication channels) according to the UPTF. Channel A (Ch A) logically represents the link between the payer 200 and the payee 202. This link is used to negotiate the details of a cashless payment transaction. This aspect is application dependent and is not considered to be part of the UPTF framework. Ch

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 596 of 1360

A may or may not exist, and if it exists it can be a wireless channel, for example, in case of a WLAN enabled mobile phone 106, and/or channel A can be oral communication between the payer 200 and payee 202 in case of a non-WLAN mobile phone 106 used in a point of sale financial transaction. Channels B and C, are example logical links among the Payer 200, the Payee 202, and the STS 120. In case of a mobile phone wireless wallet 106, Channels B and C are mobile phone communication networks that can carry Internet traffic. In most situations these are not direct links, but involve communicating through the mobile communications network and/or the Internet. In general, these are insecure channels. Channel D, from the STS 120 to the Financial Institutions 204 is a different type of channel and is assumed to be a highly secure communication path. In addition, STS 120 itself is assumed to be housed in a protected facility so that its database 203 is physically secure and inaccessible from the network.

[0051] The mobile phone wireless wallet 106 operations involved in an example transaction with reference to FIG. 2 is described. The payer (operator) 200 initiates the SAS protocol through an explicit action, enters the PIE generated in operation 110 by the STS 120. This allows the payer 200 to generate a view of the transaction and to encrypt this with its private key based upon the PIE and the software authentication parameter(s) and then to send the encrypted view as a message to the STS 120. Similarly, the payee (operator) 202 enters its PIE that is also generated in operation 110 by the STS 120 and generates it's own view of the transaction, encrypts the view with its private key based upon the PIE and the software authentication parameter(s) and then sends its view to the STS 120. The STS 120 receives both encrypted views and verifies the views, through a successful view decryption (i.e., a successful view decryption authenticates a user) and a successful comparison of two or more views (as the case may be) (i.e., a successful comparison of transaction party views authenticates a transaction). The STS 120 then uses the secure back channels D to interact with the financial institutions 204 of the payer 200 and the payee 202 for transferring the funds. The STS 120 sends receipts (or failure notices) back to the payer 200 and the payee 202 to complete the transaction. The response messages are also encrypted by the STS 120 for each intended destination.

[0052] Other examples described herein are particular instances of the FIG. 2 UPTF system architecture. In particular, the physical POS deployment represents a common variation of this scheme. For this situation, the Payer 200 is a customer device, such as the mobile phone 106 that executes the wireless wallet application 108, the Payee 202 is the merchant operated device. The merchant operated device is located at a fixed site and can be a more powerful computer and provide additional network services, such as an Internet

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 597 of 1360

connection. A direct payer 200 to STS 120 Ch B is not used, but rather the Payer 200 UPTF cashless monetary transaction messages are forwarded to the STS 120 through the merchant 202. In this case, channels A and B would be a mobile communication channel between the payer 200 and the merchant server 302 to bind the mobile phone user with transaction information of the merchant, such as the merchant products/services available for purchase and to forward, by the merchant server 302 to the STS 120, the payer 200 UPTF transaction messages (see FIGS. 3, 5 and 6). The properties of the protocol prevent the merchant from gathering personal information from the customer 200. Further details of the encryption procedures as part of the SAS are described further below.

[0053] Therefore, the mobile phone 106 wireless wallet application 108 is based on a general framework, called the Universal Pervasive Transaction Framework (UPTF), a generic architecture and a new security protocol for conducting secure multi-party agreements, using mobile devices over a wireless transport network. The framework is designed to address several key aspects specific to the envisioned pervasive environments.

[0054] FIG. 3 is functional block diagram of a UPTF based system architecture to execute a mobile phone cashless monetary transaction , according to an embodiment of the present invention. A universal pervasive transactions device (UPTD) is a wireless mobile computing device, such as mobile phones 106a-n, based upon the UPTF SAS to implement a wireless wallet by installing in the mobile phones 106a-n corresponding authentic mobile payment software 108a-n. A computer system and method of binding the mobile payment software 108a with transaction information of a transaction party (e.g., merchant online retail application 302); inputting the PIE by the user at the mobile phone 106a of the user; executing the authentic mobile payment software 108a and presenting, by the STS at the mobile phone 106a, a selectable list of abstracted relationship identifiers (identifiers that are a level removed from actual identifiers), corresponding to the registered financial entities of the user, that are correlated with the authentic mobile payment software 108a; and executing the mobile phone cashless monetary transaction with the transaction party 302 using the PIE and the software authentication parameter and according to UPTF transaction messages comprising an identifier of the mobile phone 106a, an identifier of the transaction party 302, and an identifier of the transaction, thereby providing the mobile phone wireless wallet based upon a combination of the authentic mobile payment software 108a at the mobile phone 106a and the STS 120 correlations of the authentic mobile payment software 108a with the PIE, the software authentication parameter, and the financial entities of the user, and independent, anonymous exchange of the UPTF transaction messages between the user, the transaction party and the STS. As described in more detail below, the authentic mobile

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 598 of 1360

payment software 108 and the STS 120 correlations result in generation of a security tool (e.g., an encryption key) to secure (e.g., encrypt) messages, and, thus, successfully decrypting each message authenticates a sender, and, in case of UPTF transaction messages, by decrypting and matching UPTF transaction views of one or more transacting parties authenticates the transaction.

[0055] A UPTD wireless wallet can be a WLAN enabled wallet-sized computing device, including a WLAN enabled mobile phone, able to detect UPTF-enabled physical points of sale (POS), to wirelessly connect to the POS using a wireless local area network/short range radio technology (e.g., 802.11, BLUETOOTH, Infrared, etc.), and to allow their owners to make purchases and or payments with the UPTD wireless wallet. A UPTD wireless wallet can also be a mobile phone without WLAN capability. UPTF authenticable transactions using a UPTD that is a WLAN enabled mobile phone is described in, and can also be understood, for example, by referring to, the pending US patent application no. 10/628,583 (attorney docket no. 1634.1002) filed July 29, 2003 and owned by FUJITSU LIMITED assignee of the present patent application, which is incorporated herein by reference. In a typical embodiment described herein, the UPTD wireless wallet is an Internet and/or web capable/enabled mobile phone 106 (hereinafter referred to as a mobile phone 106 or as a mobile phone wireless wallet 106). For example, a mobile phone wireless wallet 106 could be used to place an order at a restaurant and subsequently make payment, as follows: (1) the user consumer 200, through activating a UPTD mobile phone wireless wallet software 108 function, according to the processes of FIG. 1A, interfaces over a mobile phone communication network 317 with a service spot merchant 202 (which, for example, could be a retail application server 302 on Internet 310 for a movie theater ticket, a gas station, etc., a point of sale 315 at a physical location of the merchant 202) - the retail application 302 implements a virtual store front (for ordering goods or retrieving the payment amount and is accessible through a web server) and implements the UPTF-related functions for effecting mobile phone cashless purchasing; (2) the mobile phone wireless wallet 106 displays a listing of the available merchant 202 offered services (via Channel A between the mobile phone wireless wallet 106 and the retail application 302 in FIGS. 2 and 3); (3) the consumer 200 selects the service (e.g., ordering a meal, or payment at checkout station) with a simple keypad input at the mobile phone wireless wallet 106; (4) once a purchase amount is determined, the consumer 200 presses a designated payment button on the mobile phone wireless wallet 106, which begins the payment stage and results in retrieval of a purchase order (i.e., the agreement) from the merchant 202; following a visual inspection by the consumer 200, the consumer 200 is requested to input the consumer's security PIE (also optionally selecting which financial entity account to use for payment); (5) the consumer 200

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 599 of 1360

receives on the mobile phone wireless wallet 106 a confirmation and a receipt, if the transaction was successful (the service spot merchant 202 also receives a notification of the successful transaction).

[0056] It is important that the payment stage (5) is explicitly initiated by the consumer 200, so that the consumer cannot be spoofed into typing a PIN into an attacker-served page. In a typical implementation of the embodiment described herein, pressing the payment button results in termination of a browsing application (e.g., an execution thread) executed at the mobile phone 106 and the launching of new application (e.g., another execution thread) for user entry (albeit transparent to the user). As long as the user never entered a PIE without first pressing a payment button, hijacking of the PIE can be prevented.

[0057] The retail application 302 implements a virtual store front (for ordering goods or retrieving the payment amount and is accessible through the web server) and the UPTF-related functions for effecting purchasing.

[0058] The mobile phone wireless wallet 106 can deliver a user experience to execute UPTF SAS based cashless monetary transactions in a fast and intuitive manner. The mobile phone wireless wallet software 108 delivers an implicit localization by allowing interfacing at any location (location independent) to merchants 202. The speed and its simple and unified interface are effective and with some practice, performing a transaction could be accomplished in seconds (e.g., 30 seconds, or less than 12 seconds in case of a WLAN mobile phone wireless wallet 106); which can be less than a typical cash or card transaction involving getting change or physical paper receipts. A consumer 200 could purchase (or be offered) a mobile phone wireless wallet 106, for example, on-line via the sign up application computer 102. In other words, the consumer 200 would obtain a PIE as well as obtain (download) a wireless wallet software 108 for a mobile phone to execute mobile phone UPTF SAS based transactions. Merchants 202 would provide UPTF SAS functions in retail and purchasing applications 302, 315.

[0059] FIG. 4 is a diagram of UPTF cashless monetary transaction messages based upon Secure Agreement Submission (SAS) protocol to execute a mobile phone cashless monetary transaction, according to an embodiment of the present invention. In FIG. 4, colors are used to highlight features/concepts described herein. The SAS protocol is used for encrypting and submitting views of desired UPTF based cashless financial transactions. The message structure and encryption mechanism of SAS are designed to provide many of the desired security properties in an insecure pervasive communication environment envisioned for wireless purchasing, such as:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 600 of 1360

[0060] o Authentication: the agreement parties and the verification party are authenticated to each other, as is the integrity of the agreement group;

[0061] o Anonymity: agreement parties may remain anonymous to each other and personal and/or other account related information is not revealed to the other party;

[0062] o Protection of the agreement content: the agreement is kept private, it is tamper-resistant, non-replayable, and strong non-repudiation proper-ties are provided. In particular, a continuously changing, time dependent, device specific key is used to encrypt the views.

[0063] The underlying SAS algorithms are well-suited for a system using low-cost user devices, which have limited computing resources, while minimizing the complexity of use for the user. In addition, some of the information necessary to use the SAS, in particular the PIE, is not permanently stored on the UPTD 106 and not included in any data transmissions, so that if the UPTD 106 is lost or stolen, the UPTD 106 cannot be used. Additional details of the SAS and the encryption mechanism are provided with reference to FIG. 4, as follows.

[0064] The internal structure and the generation process of view messages 402, 404 (i.e., UPTF SAS cashless monetary transaction messages) are shown in FIG. 4. The UPTF SAS based views 402, 404 are implemented in software and/or computing hardware as the electronic wireless wallet software application 108 that is executed in the UPTD 106, such as the mobile phone 106. Since the views 402, 404 from the payer and the payee are symmetrical, the payer's 200 view 402 is only described. The symbols used in FIG. 4 are explained below:

[0065] o DIDc: device ID, a unique identifier for the Payer's UPTD device 106 (the consumer (c) or source transaction party).

[0066] o DIDm: device ID, a unique identifier for the Payee's device (the merchant (m) or destination transaction party).

[0067] o RSN: random sequence number.

[0068] o TS: local current timestamp.

[0069] o TID: transaction ID, a unique identification number assigned to an agreement, which is maintained by the STS 120 to identify corresponding UPTF agreement views 402, 404.

[0070] o MD: message digest

[0071] o PIE: Personal identification entry, a user and STS 120 maintained input secret

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 601 of 1360

entry, such as an alphanumeric string. In a typical embodiment described herein, the PIE is only maintained by the user and the STS 120, is not known to and/or maintained by another party to a transaction and/or the financial institutions 122, 204, and is temporally known as an intermediate parameter to the mobile phone 106 of the payer 200 for encrypting the payer view 402. More particularly, the PIE is not included in transaction messages (e.g., UPTF SAS messages and/or SAS based informational messages) and, thus, the wireless wallet software 108 does not transmit the PIE. The PIE can be non-secure by being a substantially short alphanumeric string, such as a 4 digit number. The user enters the PIE whenever the user attempts a transaction. Preferably the PIE is issued to the user following the registration of the user for the application 108 that the client device 106 is used for. The user can also select the PIE at such time. The PIE is an alphanumeric string. In order to speed up the user entry to make it easier for the user to remember it, the PIE can be a number such as 4-digit or 5-digit PIN. The PIE is, however, a piece of highly secure information in the sense that it is never transmitted during the UPTF protocol execution, it is only known to the user and the STS 120, and its secrecy should be well protected. It is assumed that the PIE can be input by the user on a mobile phone 106 in a secure fashion or it may be deterministically generated using a biometric device such as a fingerprint sensor. For example, a computation applied on the fingerprint data received from a fingerprint sensor can be used to generate a PIE that is initially communicated by the user to the STS 120. Whenever the user attempts a transaction, the user applies her finger to the fingerprint sensor, thus generating the PIE. The PIE is not kept in permanent storage on the mobile phone 106, but is used as an intermediate parameter required for the generation of the encryption key for a transaction and it should not be retained by the device 106 for a period longer than the transaction execution time. If a particular implementation of the present invention uses a form of PIE that is not convenient for a user to input for each agreement transaction and the device needs to store its user's PIN, the storage must be secure and tamper-resistant.

[0072] As shown in the FIG. 4, a view 402 comprises a cipher text part (or encrypted part) 406 and a perceptible (e.g., plaintext) part 408. A plaintext part 408 includes the TID, the DIDc of the payer 200 generating the view 402, and the local current timestamp (TS) of device 106. The TS, among other functions described herein, is also used to prevent transaction replay. The encrypted part 406 includes two critical fields: the agreement data and the DIDm of the payee's 202 device 106 involved in the agreement. The DIDm is the minimum necessary reference field in order to provide the desired verification properties of the UPTF protocol. Therefore, a user can execute a UPTD 106 cashless monetary transaction with a transaction party according to a PIE and a wireless wallet software 108

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 602 of 1360

authentication parameter RSN and transaction messages comprising an identifier of the mobile phone, an identifier of the transaction party and an identifier for a transaction (for example, an identifier and/or other transaction related data such as payment amount, etc.) thereby providing the UPTD wireless wallet based upon a combination of the mobile payment software at the UPTD and STS association of the PIE and the software authentication parameter with financial entities of the user and exchange of the transaction messages between the user, the transaction party and the STS 120.

[0073] First, DIDc and the TS obtained from the UPTD's local clock (and/or as provided as a part of the agreement data), are utilized by the device's 106 pseudorandom number generator to generate a time-dependent RSN. Therefore, the parameters of the generator are particular to each device 106. The encryption key K is then generated from the RSN and user input PIE (shown in FIG. 4 with green coloring), where the PIE is generated by the STS 120 as shown in FIG. 1A. Firstly, the RSN and PIE are combined using a function F and then a hash function H is applied to the result (typically a string) to generate the encryption key:

[0074] K = H (F ((PIE, RSN))

[0075] A message digest function can be applied to the agreement data, the DIDm, and the DIDc to generate a MD of the view. The MD can further strengthen the security by ensuring that no other party has tampered with or modified the contents of the view 402 in any way. The encryption algorithm with the encryption key K is then applied to the MD, the agreement data, the DIDc, and the DIDm to generate the cipher text part of the view 402, as shown in FIG. 4 with yellow coloring. For further protection, the SAS protocol uses random message padding in order to further prevent "known-text" attacks. According to an aspect of the embodiment described herein, the embodiment uses Advanced Encryption Standard (AES) for encryption, a Keyed-Hashing for Message Authentication (HMAC)-based scheme for random number generation, and SHA1 Secure Hash Algorithm for the hash function.

[0076] The STS 120 has sufficient prior knowledge of the functions and specific parameters used by each device 106 in the encryption process, so that when combined with the plaintext portions of a message 402, 404, it is possible to decrypt the message 402, 404 by reversing the above process. For example, from the plaintext part 408 of the view 402, the STS 120 recovers the DIDc and TS, which are used to look-up the customer's 200 PIE and other parameters of the RSN generator that can be stored in the STS database 203. These are used to compute the RSN. The encryption key K can then be computed using the same method with which the customer UPTD 106 generates the encryption key. The cipher text part 406 of the view message 402 is then decoded.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 603 of 1360

[0077] After all applicable fields of the payer 200 view 402 are acquired, the STS 120 locates the payee's 202 view 404 for the same transaction, using the DIDm and TID included in the previously decoded payer 200 view 402. After going through a similar decryption process, the decoded fields of the agreement data of the payee 202 view 404 are compared with the corresponding fields from the payer 200 view 402. If all applicable corresponding fields match (correspond according to application design), the received views 402, 404 are considered verified. Further processing is then carried out and external executions are triggered as necessary.

[0078] Any responses from the STS 120 to the payer 200 or payee 202 are encrypted by the STS 120 using the same encryption methods and using the parameters for the destination devices 106, 302 and the TS of the original transaction. Only the intended recipient can decrypt the response message, insuring privacy protection and authentication of the STS.

[0079] Another example encryption key generation for the UPTF SAS is described herein. In FIG. 4, using the view 402, the key KEYc is a hash of a RSNc and a PIEc; the detailed key generation procedure is as follows:

[0080] The initialization data for the RSNc are created when a new UPTD account is created by the STS (e.g., when the code executable 108 is created by the STS 120 at operation 110 in FIG. 1A). Specifically:

[0081] 1. a random 128-bit seed is generated using a software service function.

[0082] 2. a random 160-bit initialization timestamp is created also at new UPTD account creation time, using software service function. Therefore, in FIG. 1A, at operation 110, the STS 120 generates device 106 specific initialization parameters of a random number and an initialization time stamp, both of which, at operation 114 are transmitted via the wireless wallet application 108 to the UPTD device 106 (e.g., mobile phone 106).

[0083] In FIG. 1A, at operation 110, the PIE is created by the STS 120 when a new account is created at the STS 120, as follows: a 32-byte random value is created using a software service function , convert each byte to a decimal value string, and concatenate them all to produce a long string. Randomly chop 4 digits from this string to create PIE.

[0084] When the key needs to be created in order to encrypt a transaction message, the following steps take place:

[0085] 1. A 160-bit current timestamp is generated, as follows:

[0086] a. Convert current time to string, for example, converting the current time to a 16

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 604 of 1360

characters string, e.g., 5:04pm, Jan 26, 2004 is written in "0000170401262004."

[0087] b. Take the string and a one way function to output another value, for example by hashing the current time string using SHA1 algorithm, which produces a 160-bit output.

[0088] 2. XOR an init timestamp and current timestamp to produce a 160-bit output. This operation is essentially a form of deterministically calculating a difference between two values of time (i.e., a deterministic transformation between two values).

[0089] 3. Use the 128-bit seed software authentication parameter as data, and the XORed value of the two time stamps as the key, compute the HMAC result (a 160-bit value). The result of the HMAC is the RSNc. Use of the HMAC accommodates unpredictability in the RSNc generation.

[0090] 4. Chop the first 128-bit of the HMAC result, combine (e.g., concatenate) with the 32-bit PIE (convert from a 4 digit string) for a 160-bit value.

[0091] 5. Compute the hash (SHA1) value of the 160 bit stream in operation (4), and chop the first 128 bit as the final key.

[0092] In the encrypted part of the message a hash of the transaction part of the message (with the padding) using SHA1 (alternatively a CRC can be used) is used.

[0093] In the above-described embodiment, the values of a number of bits are provided as unlimiting examples, and the present invention is not limited to a specific number of bits values. Therefore, as illustrated with reference to FIGS. 1, 2, 3 and 4, a UPTF SAS based transaction requires a device 106 which provides device-specific parameters that determine a device-specific and time-specific key and an operator for the device who provides a fixed PIE that is only known to the STS 120 and the operator. The combination of the two is required for an encrypted transaction request that can be validated by the STS 120. Intercepting one (or more) transaction message and successfully decrypting it would not be sufficient for purposes of inferring either the PIE, or the device specific parameters employed in the key generation process. Moreover, a single, time-dependant key is not re-usable because of the pair-wise agreement notion of transactions processed by the STS 120.

[0094] Accordingly, a system and method of generating, by the mobile phone, a first view of the mobile phone cashless monetary transaction, and transmitting the first view of the transaction to the STS according to the SAS; generating, independently by a party to the transaction, a second view of the transaction, and transmitting the second view of the transaction to the STS according to the SAS; and verifying, by the STS, the first and second views to authenticate the transaction, and causing, by the STS, execution of the transaction

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 605 of 1360

based upon the verifying. The first and second views are symmetrical and the SAS comprises generating as each independent view of the transaction an unencrypted perceptible part comprising an identification of a first mobile phone for the first view and a current timestamp, and an encrypted part by performing a combination of time and authentic mobile payment software dependent transformations based upon the PIE, on a transaction message comprising data of the transaction, the identification of the first mobile phone and an identification of a second mobile phone for the second view.

[0095] An authentic mobile phone wireless wallet software 108, which generates the UPTF SAS views, comprises therein software authentication parameters of an initialization time stamp and an initialization random seed number, and wherein the first and second views are symmetrical and the SAS comprises generating as each independent view of the transaction, an unencrypted perceptible part comprising an identification of a first mobile phone for the first view and a current timestamp, and an encrypted part by performing a combination of transformations based upon the PIE and the software authentication parameters included in the authentic payment software from the STS, on a transaction message comprising data of the transaction, the identification of the first mobile phone and an identification of a second mobile phone for the second view. The combination of transformations to encrypt comprises generating a transaction random sequence number based upon the software authentication parameters of the authentic payment software; and generating an encryption key based upon the transaction random sequence number and the PIE.

[0096] The generating of the encryption key further comprises generating a current time stamp; converting the current time stamp to a string; using a one way function, such as a hash function, to convert the current time stamp string to a current time stamp value; determining a time difference value between the current time stamp and the initialization time stamp; computing a Keyed-Hashing for Message Authentication (HMAC) result, based upon the initialization random seed number and the time difference value, to generate the transaction random sequence number; selecting a number of bits from the HMAC result as the transaction random sequence number and combining the selected number of bits fwith the PIE; computing a hash value of the combination; and selecting a number of bits of the hash value to generate the encryption key. The number of bits is about 128.

[0097] FIG. 5 is a flow chart of a UPTF based mobile phone cashless monetary transaction with a merchant, according to an embodiment of the present invention. A computer system is described that comprises an Online Payment Service (122, 204), a Secure Transaction Server (STS) 120, and a mobile phone wireless wallet application 108

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 606 of 1360

comprising mobile phone specific electronic financial transaction initialization parameters, that is downloadable to a mobile phone 106 for consumers to execute a mobile phone cashless monetary transaction with a merchant, send money to other consumers using their mobile phone or for consumers to request money from other consumers using their mobile phone. When making payments using a mobile phone, the consumer can select any of the accounts registered with the online payment service 122, 204 to make the payment using that account.

[0098] An Online Payment Service (OPS) 122, 204 is a web accessible service that enables consumers to make payments to other consumers or merchants, or consumers or merchants to request payments from other consumers. In current Online Payment Services 122, 204, a consumer 200 identifies a merchant 202 or another consumer 200 by an e-mail address (or some other user identifier, such as a user name, etc.) that has been verified by the OPS 122, 204. Users 200, 202 of the OPS 122, 204 provide to the online payment service 122, 204 the information of their personal accounts (credit cards, bank accounts, etc.), so that any of those accounts can be used when making a wireless device cashless payment. The Secure Transactions Server (STS) 120 is a Universal Pervasive Transaction Framework (UPTF) based system that verifies transaction requests that observe the UPTF.

[0099] As also described above with reference to FIG. 1B, when the user is logged on, over the web, to the OPS 122, 204, the user might see an option that enables them to make payments or request payments from a mobile phone 106. Upon following the link associated with this option, the user will be asked for the phone number of the mobile phone 106 that she would like to use for such transactions and possibly the mobile carrier for that phone number. Upon submitting this information, the user will be shown a PIE to be used for making payments and requesting money from her mobile phone 106 and she will also receive a SMS (Short Messaging Service) message on the specified mobile phone, with a link that if followed will enable her to download to her mobile phone 106 the mobile phone wireless wallet software 108 that will enable her to make payments and request money using her mobile phone 106. The link points to a unique downloadable executable associated with this user at the STS 120 via the STS 120 maintained software authentication parameters and PIE. If the user has access to the web from the mobile phone 106, she will be able to follow that link and download the software 108 to the mobile phone 106. Upon completing the download of the mobile phone wireless wallet application 108, the user will be asked to save the application on the mobile phone 106. From that point on the application 108 is ready for use. The downloaded application can be referred to as mobile phone electronic wireless wallet 108. A consumer 200 who is also an OPS 122, 204 user and has

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 607 of 1360

downloaded a mobile phone wireless wallet 108 to her mobile phone 106 will be referred to as a mobile OPS user (as opposed to a OPS user). All mobile OPS users are also OPS users, so when using the term OPS users, it refers to both OPS users and mobile OPS users.

[00100] As discussed above with reference to FIG. 1A, the mobile phone wireless wallet software 108 is an executable written in a language that is installable and executable on the mobile phone 106, such as Java 2 Platform, Micro Edition (J2ME), Binary Runtime Environment for Wireless (BREW), any other language that might be installable on the mobile phone 106 so that applications written in that language can be executed on the mobile phone 106, or any combination thereof. The executable 108 is created by the STS 120 entirely, or at least partially as the STS 120 needs to create, store and retrieve data that is used to identify this executable 108 and the user associated with it for each future transaction. The STS 120 also creates and stores the PIE that is used for such transactions. The PIE is not stored on the executable 108 or the mobile phone 106 that this executable 108 will be eventually downloaded to. Only the software authentication parameters (operations 50, 52) are included in the mobile phone wireless wallet software 108.

[00101] Also, an OPS user can make a payment from the web-accessible OPS 122, 204 to a mobile OPS user, by using the mobile phone number of the mobile OPS user to identify the consumer who will receive the payment. Typically, OPS users identify other OPS users with an e-mail address. If an OPS user knows the mobile phone number of a mobile OPS user, she can identify that user by the mobile phone number and makes a payment to that user. Similarly if an OPS user wants to request money from a mobile OPS user, she will have to identify that user by a mobile phone number. In the latter case, the mobile OPS user might receive a SMS notification on her mobile phone notifying her that someone has requested money from her. The requestee can the use her mobile phone 106 to make a payment to that OPS user.

[00102] Also a mobile OPS user can use her mobile phone the make payments to other OPS users. If the payee is also a mobile OPS user, the payer can identify the payee by mobile phone number, although she can also identify that payee by e-mail address if she so chooses. Entering a phone number in a mobile phone is easier and faster than typing an e-mail address. If the payee was identified by phone number, the payee will receive a SMS notification about the payment. The payer also will receive a notification SMS if the payment is successful. The payer can select any of the OPS-registered accounts to make the payment from.

[00103] A mobile OPS user can also use her mobile phone to request a payment by an

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 608 of 1360

OPS user, by similarly specifying the OPS user by either e-mail address or mobile phone number if the user knows it. Requestor and requestee will receive a SMS message notifying them of successful request. Mobile OPS users can also view in their mobile phone a list of transactions that involved their mobile wireless wallet software 108 from a relevant menu of the application 108. This list can include all transactions that involved the mobile phone 106 in order to effect the transaction. Specifically, this includes payments that were made from the mobile phone 106 (including a payment made in response to a request for payment) and requests for payments to other OPS users. OPS users can view in the web-accessible OPS, a list of all transactions that they have performed, regardless of whether they were made from the web-accessible OPS or from their mobile phone 106.

[00104] Payments and request for payments from the mobile phone 106 using the mobile phone wireless wallet software 108 result in UPTF messages (e.g., 402, 404), encrypted according to UPTF, send by the mobile phone's 106 wireless wallet 108 to the STS 120 and/or generated by the STS 120 (i.e., in case of a person-to-person mobile phone payment, the STS may or may not create a second view for the payment transaction depending on system configuration and/or application design and/or transacting party preference). For example, in FIG. 5, in case of a member-to-member, as a person-to-person transaction example, cashless payment transaction involving one payment service 122, 204 in which both members have registered accounts, the merchant 202 transaction system 302 and the payment service 122, 204 could be logically (conceptually) one entity/system 500 for through processing (via a channel D between the OPS 122, 204 and the STS 120) the UPTF views 402, 404 to/from the STS 120. In general, in a person-to-person type transaction scenario, each transacting party creates its own view. In case of a payment by one person to another person using the mobile phone wireless wallet 106, because the other person (payee) may not require (or be required) to approve a payment made to the payee, the payee might not need to create a view to accept the payment. Therefore, in case of a payment transaction, the payee's view can be omitted and the STS 120 may simply only verify a first payment request view 402 from a payer 200, or the STS 120 may create the other person's (payee 202) second view 404 on the payee's behalf. Paired views 402, 404 are used in case of a plurality of online payment services 122, 204 to achieve person-to-person mobile payment transactions. According to an aspect of the embodiment described, the system 500 can also comprise the STS 120. Also, responses to messages from the STS 120 to a mobile phone 106 are UPTF SAS messages, encrypted according to UPTF SAS. The OPS 122, 204 has a secure connection (i.e., channel D) to the STS 120.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 609 of 1360

[00105] According to an aspect of the embodiment described herein, in case of person-to-person payment transaction, a payment action from the web-accessible OPS 122 (i.e., in case of a payment from a desktop to a mobile phone wireless wallet 106), 204 can be carried through the secure connection D to the STS 120 and need not be encrypted according to UPTF SAS. As discussed above, payment from the web-accessible OPS is effective immediately and does not require an action by the payee. Still, the STS 120 will receive that payment action, decrypt the payment action, which according to the UPTF SAS serves to authenticate the originating payment action requester, including the transaction, and will determine if the payee is a valid mobile OPS user, who is still active with the STS 120, and possibly notify the payee 202 mobile phone wireless wallet 106.

[00106] According to another aspect of the embodiment described herein, the STS 120 through the secure connection D between the STS 120 and the OPS 122, 204, can receive a request for payment to a mobile OPS user (i.e., in case of a request for payment from a desktop to a mobile phone wireless wallet 106). Upon receipt of the request the STS 120 will send a notification SMS to the mobile phone 106 of the mobile OPS requestee. When the mobile OPS user, using her mobile phone 106 and the mobile phone wireless wallet software 108 checks for pending requests she will see that request and can decide to make a payment to the requestor. Upon receipt of the payment message by the STS 120, the STS 120 will check against the pending request by the request, will determine according the UPTF methods that the complete transaction is valid and accordingly notify requestor and requestee.

[00107] According to another aspect of the embodiment described herein, a request for payment by a mobile OPS user that uses her mobile phone for that request, is handled similarly. If the requestee was identified as a mobile OPS user, the requestee will receive a notification SMS and will see the request upon checking for pending requests with the wireless wallet software 108 and can decide to complete a payment. The STS 120 will use the UPTF criteria to compare with the requestor's messages to the STS 120 and determine the validity of the complete transaction. Upon such determination the STS 120 will notify the OPS and the requestor and requestee.

[00108] All of the above described transaction examples, only require that the mobile OPS user use her mobile phone 106 and the mobile phone wireless wallet software 108 and entering the designated PIE for those transactions. The STS 120 and OPS 122, 204 may be operated by the same entity and/or execute in the same computer system, or they me be operated by different entities. According to an aspect of the embodiment(s) described herein, a user can be notified at the mobile phone wireless wallet 106 of a status (e.g.,

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 610 of 1360

result, confirmation, state, success/failure, problem/help notification, etc.) of the mobile phone UPTF authenticable cashless monetary transaction using Short/Multimedia Message Service, email, and/or voice message.

[00109] FIG. 6 is a flow chart of a UPTF based mobile phone cashless monetary transaction to purchase a movie ticket, according to an embodiment of the present invention. FIGS. 7A-B are mobile phone display screen user interface images to execute mobile phone cashless monetary transaction to purchase a movie ticket and to obtain, store and retrieve a transaction receipt, according to an embodiment of the present invention. With reference to FIGS. 5, 6, and 7A-7B, an example mobile phone cashless monetary transaction with a merchant is described. In FIG. 5, at operation 502, a mobile phone 106 user/consumer 200 uses an installed (FIGS. 1A, 1B, 1C) mobile phone wireless wallet 108 to request a purchase order from the merchant 302 payee 202. In FIGS. 5 and 6, operation 502 comprises binding the consumer 200 with the merchant 302 transaction information, for example, by browsing a merchant ticket sales application (merchant transaction server (MTS)) 302 (FIGS. 2, 3) for purchasing a movie ticket via a mobile phone (cellular) communication network. The binding of the user with a merchant's virtual shopping cart can also be performed by inputting at the mobile phone wireless wallet software 108 an identifier for the merchant (e.g., a POS 135 transaction paper receipt information) and/or the mobile phone wireless wallet might have pre-stored a merchant identifier (e.g., Internet Universal Resource Locator (URL) address). In FIG. 7A, for example, at operation 502, mobile phone user interface screen images 702a-h are displayed for browsing the merchant ticket sales application 302, which comprise, at 702a, selecting the mobile phone wireless wallet software 108, at 702b, selecting "Go shopping," at 702c, selecting "Movie Theater," at 702d, selecting "Movies Playing Next," at 702e, selecting movie times from displayed movie time information, at 702f, selecting a movie from displayed movies at the selected time, and, at 702g, completing a purchase order form request to be sent to the merchant 302, and, at 702h, transmitting to the merchant 302 the purchase order request , which is a binding of the consumer 200 with the merchant 302 transaction information by identifying what is being paid for (electronic shopping cart) and payment information.

[00110] At operation 504, the mobile phone wireless wallet software 108 receives a purchase order from the merchant ticket sales application 302, which, for example, can result in mobile phone user interface screen image 704 that displays a summary of the electronic shopping cart, including payment information, from the merchant 302, and a "Please press PAY button" selection. According, to an aspect of the invention, at operation 504, information used as a device identifier of the merchant (DIDm) (FIG. 4) can be identified

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 611 of 1360

by the mobile phone wireless wallet 108 based upon the purchase order received from the merchant 302 payee 202.

[00111] At operation 506, selection of the "PAY" button at 704 begins the UPTF SAS functions of the embodiment. In particular, via the mobile phone user interface screen images 706a, 706b, the mobile phone wireless wallet software 108 requests input of the PIE (e.g., a PIN) and generates a UPTF SAS view 402 (as described with reference to FIG. 4), as a consumer 200 REQuest transaction, and transmits the REQuest transaction to the merchant 302. As shown in FIG. 6, the UPTF SAS based messages 402 from the mobile phone wireless wallet software 108 are carried over the mobile carrier's network, either directly to the STS 120 or indirectly through the merchant application 302, as indicated by Channel B. The transport layer between client 108 and MTS 302 and/or STS 120 uses Internet (Internet Protocol) HTTP communication. However, the transport layer can by any known transport layer, such as HTTP, web service calls, socket based communication, etc. According to an aspect of the embodiment(s) described herein, the MTS 302 is implemented with a web interface for sending and receiving messages from and to the mobile phone client 106; specifically the mobile phone wireless wallet software client 108 running on the mobile phone 106 sends its messages to the MTS 302 by submitting them to a pre-specified CGI-like interface, and the MTS 302 forwards/receives the same/responses to/from the STS 120 using web service calls. In other words, a UPTF message is an HTTP parameter. Since HTTP is stateless, the MTS 302 uses a small database to keep track of state(s) during the sending and receiving the messages. Also, because messages are carried over HTTP, a hex encoding of the encrypted UPTF SAS based message is used to avoid problems with special ASCII characters in the encrypted form of the message, as it is transported over HTTP.

[00112] At operation 508, the MTS 302 generates an MTS UPTF SAS view 404, as an MTS REQ, and transmits the MTS REQ and the Consumer REQ (i.e., views 402, 404) to the STS 120. According to an aspect of the embodiment, at operation 506, information used as a device identifier of the consumer (DIDc) is obtained by the MTS 302 from the unencrypted part of the consumer REQuest view 402, based upon which the MTS 302 generates the MTS REQuest view 404.

[00113] At operation 510, the STS 120 gets abstracted account listing for the consumer 200 from the payment service 122, 204. In particular, if at 706b, the consumer 200 inputs a request to use a financial account other than a default account, the consumer REQuest view 402 includes a request for financial account information. At operation 510, the STS 120 uses an account association 123 for the consumer 200, which is provided from the payment

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 612 of 1360

service 122, 204 (i.e., operations 105 in FIG. 1A), to confirm the consumer REQuest with the payment service 122, 204. At operation 512, the STS 120, receives an account reference listing (not actual account numbers) from the payment service 122, 204. At operations 514, 516, the STS 120 forwards via the MTS 302, an STS Response to the consumer REQuest view 402, which includes the account reference listing. At operation, 516, the mobile phone user interface screen image 708 displays a selectable user account reference listing. At operation 518, the consumer 200 authorizes the transaction. At operation 520, the MTS 302 sends an MTS authorization and the consumer authorization to the STS 120.

[00114] At operation 522, in response to the MTS and consumer authorization requests of operation 520, the STS 120 sends an AUTHorization transaction to payment service 122, 204 and, at operation 524, receives a payment service response. At operation 526, the STS 120, forwards to the MTS 302 the payment service response to the AUTHorization transaction, which, at operation 528, the MTS 302 forwards the STS response to AUTHorization transaction to the consumer 200. In particular, at operation 528, the mobile phone user interface screen image 710 displays a transaction success confirmation message. Accordingly, at operations 508 and 520, the STS 120 receives and verifies the UPTF SAS based merchant and consumer views 402, 404 (e.g., decrypting and cross-referencing the UPTF SAS based MTS REQ and consumer REQ messages and the MTS AUTH and consumer AUTH messages).

[00115] According to an aspect of the described embodiment herein, the wireless wallet application 108 running on the mobile phone 106 receives receipt related information, as shown in the display screen image 712, which according to an aspect of the embodiment is in the form of a barcode image on a computer display screen, as shown in a barcode image 714 displayed on the mobile phone display screen 106, after every successful purchase and stores these receipts on the mobile phone 106 for further reference and reuse (e.g., to be displayed on a display screen of the mobile phone wireless wallet 106 and read from the computer displayed barcode image by a barcode reader 315 to gain physical access to the paid service at a physical merchant service spot, such as a cinema point of sale (POS) 315). The transaction receipt related information could be remotely stored and retrievable. Therefore, the wireless wallet application 108 provides transaction receipt management and in FIG. 7B, an example of mobile phone display screen user interface images 716a-d is illustrated for retrieving transaction receipt related information. According to another aspect of the embodiment(s) described herein, provided is a system and method of notifying the user at the mobile phone of a status of the mobile phone UPTF authenticable cashless monetary transaction using Short/Multimedia Message Service, email, and/or voice

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 613 of 1360

message, including transaction receipt information, wherein the receipts can be forwarded to another (e.g., in case of a movie ticket purchase, a barcode image movie ticket receipt delivered to the mobile phone wireless wallet 106 can be forwarded to another person for theater entry). Therefore, the wireless wallet software 108 includes a general receipt management mechanism based upon a computer display screen image of a barcode 714. In FIG. 6, the VPN is a Virtual Private Network.

[00116] The wireless wallet application 108 running on the mobile phone 106 combines both a browser and a payment application. The browser (lightweight web client) is used for purchasing and the payment application component is used for executing a UPTF SAS transaction.

[00117] FIG. 8 is a flow chart based upon mobile phone display screen user interface images and message flow between a requestor device, a secure transaction server (STS) and a requestee to execute a person-to-person mobile phone cashless payment transaction, according to an embodiment of the present invention. FIG. 9 is a flow chart based upon mobile phone display screen user interface images and message flow between a requestor device, a secure transaction server (STS) and a requestee to execute a person-to-person mobile phone cashless payment request transaction, according to an embodiment of the present invention. FIG. 10 is overall mobile phone display screen user interface images and possible workflows available to an operator of a wireless wallet on a mobile phone to execute person-to-person cashless monetary transactions, according to an embodiment of the present invention. FIGS. 11-12 are diagrams of mobile phone person-to-person cashless monetary transaction message formats to execute various mobile phone cashless monetary transactions, according to an embodiment of the present invention. An example of a person-to-person payment and a person-to-person payment request will be described with reference to FIGS. 8, 9, 10 and 11. FIG. 8 is a flow chart of a person-to-person payment when a mobile phone payer 200 makes payment via a payment request or via responding to a received request for payment from a payee 202. In FIG. 8, at operation 802, a mobile OPS payer 200 starts the mobile phone wireless wallet 108 and chooses option "P2P Payment," corresponding to the mobile phone user interface display screen image 1002 (Form 0). At operation 804, the user selects option "Make Payment," corresponding to the mobile phone user interface display screen image 1004 (Form 1). Also, at operation 806, the user can select option "Pending Requests," corresponding to the mobile phone user interface display screen image 1004 (Form 1). If, at operation 804, the user selects "Make Payment," at operation 810, the user is prompted, via the mobile phone user interface display screen image 1006 (Form 2), to enter a phone number/email address. After

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 614 of 1360

operation 804 and operation 806 (as the case may be), the user is prompted, via the mobile phone user interface display screen images 1010 (Form 4) or 1018 (Form 7), to enter a PIE, such as a PIN. At operation 812, when the user enters the PIN, the mobile phone wireless wallet software 108 uses the input PIN to create encrypted payee id request/pending list request (as the case may be) according to UPTF SAS message view 402 and sends the message view 402 to the STS 120. At operation 814, the STS 120 receives the message views 402 and authenticates the user payer 200, and identifies payee 202/returns a pending request list (as the case may be).

[00118] At operation 814, the STS 120 creates and transmits response requests to a "payment request" or a "pending payment request list," according to UPTF SAS message views 402. At operation 816, in case of a "payment" transaction, the mobile phone wireless wallet software 108 receives from the STS 120 a payee id (e.g., udid, id, fullname), and the user is prompted, via the mobile phone user interface display screen images 1012, 1014 (Forms 5, 6), respectively, to enter amount the user payer 200 wants to pay and confirm. At operation 818, in case of a "pending payment requests" transaction, the mobile phone wireless wallet software 108 receives from the STS 120 a pending payment request list, and the user is prompted, via the mobile phone user interface display screen images 1016, 1018 (Forms 8, 6), respectively, to select from a pending payee payment request list and confirm. At operation 814, for a make payment transaction, if a payee 202 confirmation message view 404 is not required, the STS 120 only authenticates payer 200 message view 402 and identifies payee 202. At operation 814, for a make payment transaction in response to a payment request from another person, the STS 120 verifies both message views 402, 404 of the payer 200 and the payee 202, respectively, according to the UPTF SAS.

[00119] At operations 816 and 818, the mobile phone wireless wallet software 108 sends a payment message view 402 that comprises payer, payee and amount information, and, at operation 820, the STS 120 receives and processes the payment message view 402 (display screen image 1020), and returns a final result to payer 200. If the payment transaction is successful, the payee 202 can be notified as well. In particular, at operation 822, the mobile phone wireless wallet software 108 receives a payment result message view 402 and informs the user payer 200, via the mobile phone user interface display screen image 1022b (Form 10), of the payment result and ask if the user wants to bookmark payee. At operation 820, a notification to payee 202, via SMS or email, can be sent.

[00120] FIG. 9 is a flow chart of a person-to-person payment when a mobile phone payee 202 requests payment from a payer 200. In FIG. 9, at operation 902, a mobile OPS payee 202 starts the mobile phone wireless wallet 108 and chooses option "P2P Payment,"

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 615 of 1360

corresponding to the mobile phone user interface display screen image 1002 (Form 0). At operation 904, the user selects option "Request Payment," corresponding to the mobile phone user interface display screen image 1004 (Form 1). At operation 906, the user is prompted, via the mobile phone user interface display screen image 1006 (Form 2), to enter a phone number/email address for the payer 200. Also, at operation 908, the user can be prompted, via the mobile phone user interface display screen images 1006 and 1008 (Forms 2 and 3), respectively, to select a payer 200 from a favorite list. After operation 906 and operation 908 (as the case may be), the user is prompted, via the mobile phone user interface display screen image 1010 (Form 4), to enter a PIE, such as a PIN. At operation 910, when the user enters the PIN, the mobile phone wireless wallet software 108 uses the input PIN to create encrypted payer identification request according to UPTF SAS message view 402 and sends the message view 402 to the STS 120. At operation 912, the STS 120 receives the payer identification request message view 402 and authenticates the user payee 202, identifies payer 200 and resolves payer 200 information and returns payer 200 information to the mobile phone wireless wallet software 108.

[00121] At operation 912, the STS 120 creates and transmits response requests according to UPTF SAS message view 402. In particular, at operation 912, the STS 120 creates a payer 200 information (e.g., udid, id, full name) response message view 402. At operation 914, the mobile phone wireless wallet software 108 receives from the STS 120 the payer 200 information (e.g., udid, id, fullname), and the user is prompted, via the mobile phone user interface display screen images 1012, 1014 (Forms 5, 6), respectively, to enter amount the user payee 202 asks to be paid from the payer 200 and confirm.

[00122] At operations 914, the mobile phone wireless wallet software 108 sends a payment request from payer 200 message view 402 that comprises payer, payee and amount information, and, at operation 916, the STS 120 receives and processes the payment request from payer 200 message view 402 (display screen image 1020). At operation 916, the STS 120 processes (i.e., decrypting according to SAS and logging) the received payment request from the mobile phone wireless wallet software 108 by creating a new payment request entry for the payer 200, which can be requested by the payer via operation 806. In particular, at operation 916, the STS logs a transaction identifier of the message view 402, and with reference to FIG. 8, at operation 806, the payer 200 can select "Pending Payment Requests" to receive the created payment request, including the transaction identifier, of operation 916. In FIG. 8, via operations 812, 814 and 816, the payer 200 creates a corresponding agreement view 404, including the transaction identifier of the payment request, which corresponds to the created payment request of operation 916 and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 616 of 1360

can be processed by the STS 120 according to UPTF SAS by decrypting and verifying both views 402, 404 of the payer 200 and payee 202, respectively. At operation 916, if payer 200 is a mobile phone wireless wallet software 108 user, SMS can be sent to the payer 200 or otherwise an email notification can be sent to the payer 200. At operation 916, the STS 120 returns a request result to payee 202. In particular, at operation 918, the mobile phone wireless wallet software 108 receives a payment request result message view 402 and informs the user payee 202, via the mobile phone user interface display screen image 1022a (Form 10), of the payment request result and ask if the user wants to bookmark payer.

[00123] More particularly, FIG. 11 is a format diagram of six example mobile phone person-to-person cashless monetary transaction message views 402, 404, including unencrypted part 408 and encrypted part 406, for executing mobile phone person-to-person payment transactions. In FIG. 11, according to an aspect of the embodiments described herein, messages A and C are informational message views that are essentially SAS messages (encrypted according to SAS, which authenticates a sender of a message and the content). Responses from the STS 120 to the mobile phone wireless wallet 106 (messages B, D, and G) are also SAS messages (encrypted according to SAS, which authenticates a sender of a message and the content) (i.e., the messages are encrypted with a generated key (FIG. 4) corresponding to the device 106, even though the messages are sent by the STS 120, thus from the device 106 perspective, authenticating the sender (the STS 120 in this case) and the content, because only the corresponding device 106 with the installed authentic wireless wallet software 108 (via software authentication parameter(s) and the STS 120 can possibly successfully reconstruct the key used for encrypting a message at a particular time (timestamp). Messages E/F are essentially agreement message views (a transaction message, including a transaction identifier, for an agreement that involves or relates to two or more parties) that comply with UPTF and are also secured according to SAS encryption, hence UPTF SAS. Therefore, in the embodiments described herein, mobile phone transactions are executed according to SAS as well as UPTF SAS. For example, message A is a pending payment request list message view 402 created at operation 806, which is provided after operation 812 to the STS 120. Message B is a pending payment request list reply message view 402 created at operation 814 by the STS 120. Message C is a person (e.g., peer) identification request message view 402 created at operation 810 by the mobile phone wireless wallet 108, which is provided after operation 812 to the STS 120. Message D is a person (e.g., peer) identification reply message view 402 created by the STS 120 at operation 814, which is transmitted to the mobile phone wireless wallet software 108 at operation 816. Messages E/F are make payment request/request payment request message views 402 created by the mobile phone wireless wallet software 108 at operations

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 617 of 1360

816 and 818, respectively, and transmitted to the STS 120 for processing at operation 820. Message G is a transaction result message view 402 created by the STS 120 at operation 820, which is transmitted to the mobile phone wireless wallet software at operation 822.

[00124] FIG. 10 illustrates and describes three possible flows for mobile phone user interface display screen images. In FIG. 10, flow I is mobile phone user interface display screen images 1002, 1004, 1006, 1008, 1010, 1012, and 1014. In FIG. 10, flow II is mobile phone user interface display screen images 1002, 1004, 1006, 1010, 1012 and 1014. In FIG. 10, flow III is mobile phone user interface display screen images 1002, 1004, 1018, 1016 and 1014. FIG. 12 is a diagram of an example envelope of a mobile phone cashless monetary transaction message view 402 for a pending payment request list reply (Message B in FIG. 11). In FIG. 12, the message B view 402 is according to the SAS. The "message" portion contains an actual content of a message, as encrypted according to SAS. FIG. 12 shows example of message B (FIG. 11) for a Pending Payment Request List Reply. The message format 1202 is an example format of the "message" portion for a Pending Payment Request List Reply message B sent by the STS 120 in reply to message A. The message format 1202 comprises a list of pending payment requests and a list of abstracted account identifiers to select from for payment. Padding 1 and padding 2 can be random numbers to hide location of the "message" portion. Ptr1 and ptr2 are pointers indicating where the "message" portion begins.

[00125] A true mobile (service spot independent) electronically anonymously authenticable wireless wallet 106 is provided in which the user does not carry any financial account information, the mobile device does not temporally and/or permanently store any actual user financial account information, the mobile device does not require/need to be swiped over and/or even interface with a point of sale (POS) reader (i.e., a user is not bound to a payee location) to execute mobile authenticable cashless monetary transactions, and no bank card swiping is performed by the user at the mobile device and/or via the mobile device. A mobile phone, comprises a computer readable medium storing a mobile payment software initialized at a secured transaction server (STS) with a software authentication parameter, as an authentic mobile payment software; and a programmed computer processor executing the authentic mobile payment software controlling the mobile phone according to a process comprising prompting a user to input a personal identification entry (PIE) that is correlated by the STS with a phone number of the mobile phone and the authentic mobile payment software, and generating according to the PIE and the software authentication parameter a transformed authenticable mobile phone cashless monetary transaction, as a mobile phone wireless wallet of the user of the mobile phone, thereby

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 618 of 1360

accommodating mobile phone UPTF SAS based transactions.

[00126] Although the above-described embodiments are directed to mobile phone user electronically authenticable cashless monetary transaction, the embodiments are not limited to cashless monetary transactions, any type of user electronically authenticable transaction can be accommodated. The user mobile phone wireless wallet 106 provides an always-on, always-available, always-accessible "footprint" for accessing, delivering and paying (for) services with selectable accounts. The "footprint" is an authentic mobile phone wireless wallet application 108 according to a mobile phone application platform, such as J2ME, and running on a consumer's mobile phone 106. The authentic mobile phone wireless wallet application 108 can be distributed and managed directly by the "business" without the collaboration, participation and consent of a mobile phone communication carrier. The services that include "sensitive" data, such as payment, are securely accessible by the user, with a simple user maintained (i.e., not permanently stored on the mobile phone 106) identifier, such as a 4 digit PIN. Further, a provider-controlled "footprint" for additional services beyond payment can be accommodated.

[00127] For example, in case of a movie ticket purchase service using the user mobile phone wireless wallet 106, a main service would be payment for movie ticket at any location (mobile) and redemption at a service spot in the movie theater to gain entry admission. Some example additional services can be browsing movie schedules prior to purchasing, rating of movies for a reward (discount) to be applied towards future purchases, loyalty programs with immediate awards, download previews, and provide notifications of movie times based on customer profile. Also, ability to send notifications (SMS) for promotions/advertisements that are accessible once starting the mobile phone wireless wallet application 108 and/or redeemed with the wireless wallet application 108 (e.g., in combination with payment towards something that is paid for and the promotion is applied towards).

[00128] Other example mobile phone wireless wallet application 108 services comprise financial related transactions for person-to-person and customer-online merchant. Additional services can be online auction related services, such as initial informational services for an online auction service customer, checking watched auctions, etc., and payment to another transaction party for a successful bid. Also, ringtone, game, digital/media content, software, advertisements, coupons, etc. rewards mechanism (or credits for ringtone, game, digital content/media, software, etc. purchasing) can be provided in connection for mobile to mobile payments using the mobile phone wireless wallet application 108. More particularly, according to an aspect of the embodiment(s) described herein, a system and method is

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 619 of 1360

provided that ties transactions with a wireless wallet 106 (e.g., wireless wallet software 108 payment transactions/purchases) to a reward system for receiving/purchasing mobile phone related items, such as ringtone, game, digital/media content, software, etc. According to another aspect of the embodiment described herein, a mobile phone reward system and method is provided in which a reward is immediately deliverable to a mobile phone, for example, after completion of a wireless wallet 106 payment, an automatic ringtone download, via a mobile phone communication network, to the mobile phone 106. The mobile phone wireless wallet application 108 makes the process of earning and redeeming credits much easier. Customers can be online payment services, banks, credit card companies, online merchants, and/or physical merchants using a mobile phone wireless wallet 106 as a point of sale (POS).

[00129] Other example mobile phone wireless wallet application 108 services comprise ordering and payment for medical prescriptions and refills prior to pickup at an authorized merchant. Additional services of notification (SMS) of refill due, when ready for pickup, rewards, transfer prescriptions by providing doctor's identifier and prescription number from mobile phone and incorporating validation of doctor and prescription.

[00130] Other example mobile phone wireless wallet application 108 services comprise payment, in-store, using the store loyalty card with the mobile phone wireless wallet 106, along with additional services of augmenting a royalty program, delivering and accessing rewards, coupons, etc. and redeeming.

[00131] Other example mobile phone wireless wallet application 108 services comprise various types of financial transactions, such as browsing accounts, funds, stocks, selling, buying, transferring stocks/funds/bonds using funds, broker accounts, banks, debit/credit cards. Additional services of notification onto the mobile phone wireless wallet 106 if stock meets price range, delivering and accessing recommendations, reports, analysis, trends, tracking, and voice activation.

[00132] The above-described processes of the present invention are implemented in software and/or computing hardware. The embodiment(s) described herein can be thought of as a server-side wallet to which access can be controlled through a four digit PIN, with the UPTF notions of multi-party agreements and time-of-transaction dependent key generation combining to provide expected security properties. The combined solution does not require any storage of critical data on the mobile device, it does not impose special hardware requirements and "reduces" security to a 4-digit PIN which is a major convenience for the user. The mobile phone wireless wallet described herein is computationally fast; on mobile phones the key generation and encryption (or decryption) (i.e., SAS portion) can take

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 620 of 1360

approximately 100 ms on a fast available mobile phone (approximately 500 ms on a slow mobile phone) using J2ME for 160-bit AES encryption for each message. Thus, the security-related computational time is non-noticeable with respect to the transaction time (time it takes for messages to travel over a communication link).

[00133] In view of the above described examples of preferred embodiments, a computing device 106 suitable for use in implementing the present invention can be any electronic computing device (a programmable electronic device that can store, retrieve, and process data) allowing mobile (wireless) telecommunication with other computing devices and having one or more communicably connected components of computer/computing processors, such as Central Processing Units (CPUs); input unit(s)/device(s) (e.g., microphone for voice command/control, etc., keyboard/keypad, pointing device (e.g., mouse, pointer, stylus), touch screen, etc.); output unit(s)/device(s) (e.g., computer display screen (including user interface thereof, such as graphical user interface), speaker(s), printer(s), etc.); computer network interface(s), including known communication protocols thereof, (e.g., mobile telephone (voice/data (Internet)) (cellular radio networks, satellite, etc.) network, radio frequency technology, local area network, etc.); and computer readable recording media to store electronic information, such as software (e.g., operating system, wireless wallet software 108) and/or electronic data (any known computer readable media, such as volatile and/or non-volatile memory (Random Access Memory), hard disk, flash memory, magnetic/optical disks, etc.) for execution by computer/computing processors and/or electronic circuitry.

[00134] The many features and advantages of the invention are apparent from the detailed specification and, thus, it is intended by the appended claims to cover all such features and advantages of the invention that fall within the true spirit and scope of the invention. Further, since numerous modifications and changes will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation illustrated and described, and accordingly all suitable modifications and equivalents may be resorted to, falling within the scope of the invention.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 621 of 1360

CLAIMS

What is claimed is:

1. A method, comprising:

initializing, at a secure transaction server (STS), a mobile payment software with a software authentication parameter, as an authentic mobile payment software;

providing an STS correlation between a personal identification entry (PIE) and the authentic mobile payment software;

installing, in a mobile phone, the authentic mobile payment software; and

inputting, by a user, the PIE to the installed authentic mobile payment software to generate according to the PIE and the software authentication parameter a transformed secure authenticable mobile phone cashless monetary transaction over a mobile phone network, as a mobile phone wireless wallet of the user of the mobile phone.

2. The method of claim 1, further comprising implementing the authentic mobile payment software according to an application platform of the mobile phone.

3. The method of claim 1, further comprising implementing the authentic mobile payment software according to Java 2 Platform Micro Edition (J2ME) and/or Binary Runtime Environment for Wireless (BREW).

4. The method of claim 1, further comprising:

providing to the mobile phone a download link to the authentic mobile payment software; and

downloading to the mobile phone the authentic mobile payment software via the download link, thereby performing the installing of the authentic mobile payment software.

5. The method of claim 4, wherein the authentic mobile payment software downloaded link is transmitted to the mobile phone using short/multimedia message service.

6. The method of claim 1, wherein the mobile phone authenticable cashless monetary transaction is performed according to Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol.

7. The method of claim 1,

wherein the authenticable mobile phone cashless monetary transaction is performed

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 622 of 1360

according to Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol,

wherein the initializing of the authentic mobile payment software comprises:

providing to the user a mobile phone cashless monetary transaction activation link at a computing device;

registering a phone number of the mobile phone of the user via the activation link;

transmitting the registered phone number of the mobile phone to the STS;

generating, by the STS, an executable mobile payment software including the initialization parameter, as the authentic mobile payment software; and

generating, by the STS, the PIE correlated in the STS with the authentic mobile payment software, and

wherein the installing of the authentic mobile payment software download link comprises:

transmitting, by the STS, via short/multimedia message service using the registered mobile phone number, a download link to the authentic mobile payment software to the mobile phone of the user;

downloading to the mobile phone the authentic mobile payment software via the download link, thereby performing the installing of the authentic mobile payment software; and

providing, by the STS, the PIE to the user.

8. The method of claim 6, further comprising:

correlating, at the STS, abstracted registered financial entities information of the user with the authentic mobile payment software;

binding the authentic mobile payment software with transaction information of a transaction party;

presenting, by the STS at the mobile phone, a selectable list of abstracted identifiers corresponding to the registered financial entities of the user correlated with the authentic mobile payment software; and

executing the mobile phone cashless monetary transaction with the transaction party using the PIE and the software authentication parameter and according to UPTF transaction messages that comprise an identifier of the mobile phone, an identifier of the transaction party, and an identifier of the transaction, thereby providing the mobile phone wireless wallet based upon a combination of the authentic mobile payment software at the mobile phone and the STS correlations of the authentic mobile payment software with the PIE, the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 623 of 1360

software authentication parameter, and the financial entities of the user, and exchange of the UPTF transaction messages between the user, the transaction party and the STS.

9. The method of claim 6, wherein the UPTF SAS comprises

generating, by the mobile phone, a first view of the mobile phone cashless monetary transaction, and transmitting the first view of the transaction to the STS according to the SAS;

generating, independently by a party to the transaction, a second view of the transaction, and transmitting the second view of the transaction to the STS according to the SAS; and

verifying, by the STS, the first and second views to authenticate the transaction, and

causing, by the STS, execution of the transaction based upon the verifying.

10. The method of claim 9, wherein the first and second views are symmetrical and the SAS comprises generating as each independent view of the transaction an unencrypted perceptible part comprising an identification of a first mobile phone for the first view and a current timestamp, and an encrypted part by performing a combination of time and authentic mobile payment software dependent transformations based upon the PIE, on a transaction message that comprises data of the transaction, the identification of the first mobile phone and an identification of a second device for the second view.

11. The method of claim 9,

wherein the software authentication parameter comprises a plurality of parameters of an initialization time stamp and an initialization random seed number, and

wherein the first and second views are symmetrical and the SAS comprises:

generating as each independent view of the transaction, an unencrypted perceptible part comprising an identification of a first mobile phone for the first view and a current timestamp, and an encrypted part by performing a combination of transformations based upon the PIE and the software authentication parameters included in the authentic payment software by the STS in the initializing, on a transaction message that comprises data of the transaction, the identification of the first mobile phone and an identification of a second device for the second view.

12. The method of claim 11, wherein the combination of transformations to encrypt comprises:

generating a transaction random sequence number based upon the software

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 624 of 1360

authentication parameters of the authentic payment software; and

generating an encryption key based upon the transaction random sequence number and the PIE.

13. The method of claim 12, wherein the generating of the encryption key further comprises:

generating a current time stamp;

converting the current time stamp to a string;

using a one way function to convert the current time stamp string to a current time stamp value;

determining a time difference value between the current time stamp and the initialization time stamp;

computing a Keyed-Hashing for Message Authentication (HMAC) result, based upon the initialization random seed number and the time difference value, to generate the transaction random sequence number;

selecting a number of bits from the HMAC result as the transaction random sequence number and combining the selected number of bits with the PIE;

computing a hash value of the combination; and

selecting a number of bits of the hash value to generate the encryption key.

14. The method of claim 13, wherein the number of bits is about 128.

15. The method of claim 4, wherein an online payment system provides the mobile phone cashless monetary transaction activation link to a member of the online payment system as the user, thereby providing person-to-person mobile phone authenticable cashless monetary transactions using the user's mobile phone wireless wallet.

16. The method of claim 15, further comprising:

displaying on the mobile phone of the user a graphical user interface presenting selectable menu items comprising person-to-person payment, person-to-person transaction, a pending payment request by another person, setup, or any combination thereof;

upon selection of the person-to-person payment or the pending payment request menu items, displaying a graphical user interface accepting inputs comprising a mobile phone number, an email address or any combination thereof, of a transaction party; and

upon input of a mobile phone number and/or an email address of the transaction party, and the PIE, executing the mobile phone cashless monetary transaction with the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 625 of 1360

transaction party using the mobile phone wireless wallet of the mobile phone user.

17. The method of claim 16, wherein the accepting inputs further comprises accepting abstracted previously registered financial account reference identifiers of the mobile phone user to execute the transaction.

18. The method of claim 1,

wherein the mobile phone authenticable cashless monetary transaction is performed according to Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol, and the method further comprises:

correlating, at the STS, abstracted financial entity information of the user with the authentic mobile payment software; and

providing person-to-person mobile phone UPTF authenticable cashless monetary transactions using the user mobile phone wireless wallet.

19. The method of claim 1, wherein the PIE is an alphanumeric string having less than or equal to 5 characters.

20. The method of claim 6, further comprising transmitting the mobile phone authenticable cashless transaction messages over a mobile phone communications network according to Hypertext Transfer Protocol (HTTP), socket based communication, and/or web service calls.

21. The method of claim 8, wherein the executing of the mobile phone cashless monetary transaction further comprises:

receiving a mobile phone display screen displayable barcode image as a receipt of the executed mobile phone cashless monetary transaction and/or other transaction, receipt related information;

displaying the barcode image on a display screen of the mobile phone; and

reading, at a physical point of service of the transaction party, the displayed barcode image for transaction management by the transaction party.

22. The method of claim 18, wherein the person-to-person mobile phone UPTF authenticable cashless monetary transactions comprise sending a payment to a person, requesting a payment from another person, checking a pending request for payment from another, storing and retrieving records of transactions, or any combination thereof.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 626 of 1360

23. The method of claim 1, wherein the installing of the authentic mobile payment software in the mobile phone comprises downloading the authentic mobile payment software to the mobile phone, storing the authentic mobile payment software on a mobile phone installable computer readable medium, storing the authentic mobile payment software in a mobile phone embedded computer readable medium, or any combination thereof.

24. The method of claim 7, wherein the providing of the PIE to the user comprises delivering the PIE to the user as an image through a third party.

25. The method of claim 21, further comprising storing in the mobile phone the barcode image transaction receipt.

26. The method of claim 1, further comprising rewarding a mobile phone wireless wallet transaction with an automatic download of a mobile phone content comprising a ringtone, a game, a digital/media content, software, or any combination thereof, and/or a credit towards any thereof.

27. The method of claim 22, further comprising notifying the user at the mobile phone of a status of the mobile phone UPTF authenticable cashless monetary transaction using Short/Multimedia Message Service, email, and/or voice message.

28. The method of claim 21, further comprising notifying the user at the mobile phone of a status of the mobile phone UPTF authenticable cashless monetary transaction using Short/Multimedia Message Service, email, and/or voice message, including transaction receipt information.

29. The method of claim 18, wherein the PIE is an alphanumeric string having less than or equal to 5 characters.

30. A mobile phone, comprising:

a computer readable medium storing a mobile payment software initialized at a secured transaction server (STS) with a software authentication parameter and correlated with a personal identification entry (PIE), as an authentic mobile payment software; and

a programmed computer processor executing the authentic mobile payment software controlling the mobile phone according to a process comprising:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 627 of 1360

prompting a user to input the PIE, and

generating according to the PIE and the software authentication parameter a transformed secure authenticable mobile phone cashless monetary transaction over a mobile phone network, as a mobile phone wireless wallet of the user of the mobile phone.

31. A computer system, comprising:

a computer server comprising a programmed computer controlling the server according to a process comprising:

initializing a mobile payment software with a software authentication parameter, as an authentic mobile payment software,

generating a secured personal identification entry (PIE);

providing a secured correlation between the PIE and the authentic mobile payment software, and

providing an online purchasing interface; and

a mobile phone in mobile phone network communication with the server and comprising:

a computer readable medium storing the authentic mobile payment software, and

a computer processor executing the authentic mobile payment software controlling the mobile phone according to a process comprising:

interfacing with the online purchasing interface to generate a virtual shopping cart,

prompting a user to input the PIE,

generating according to the PIE and the software authentication parameter a transformed secure authenticable mobile phone cashless monetary transaction based upon the virtual shopping cart, and

transmitting over the mobile phone network the transformed secure authenticable mobile phone cashless monetary transaction to the computer server to execute the transaction.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 628 of 1360

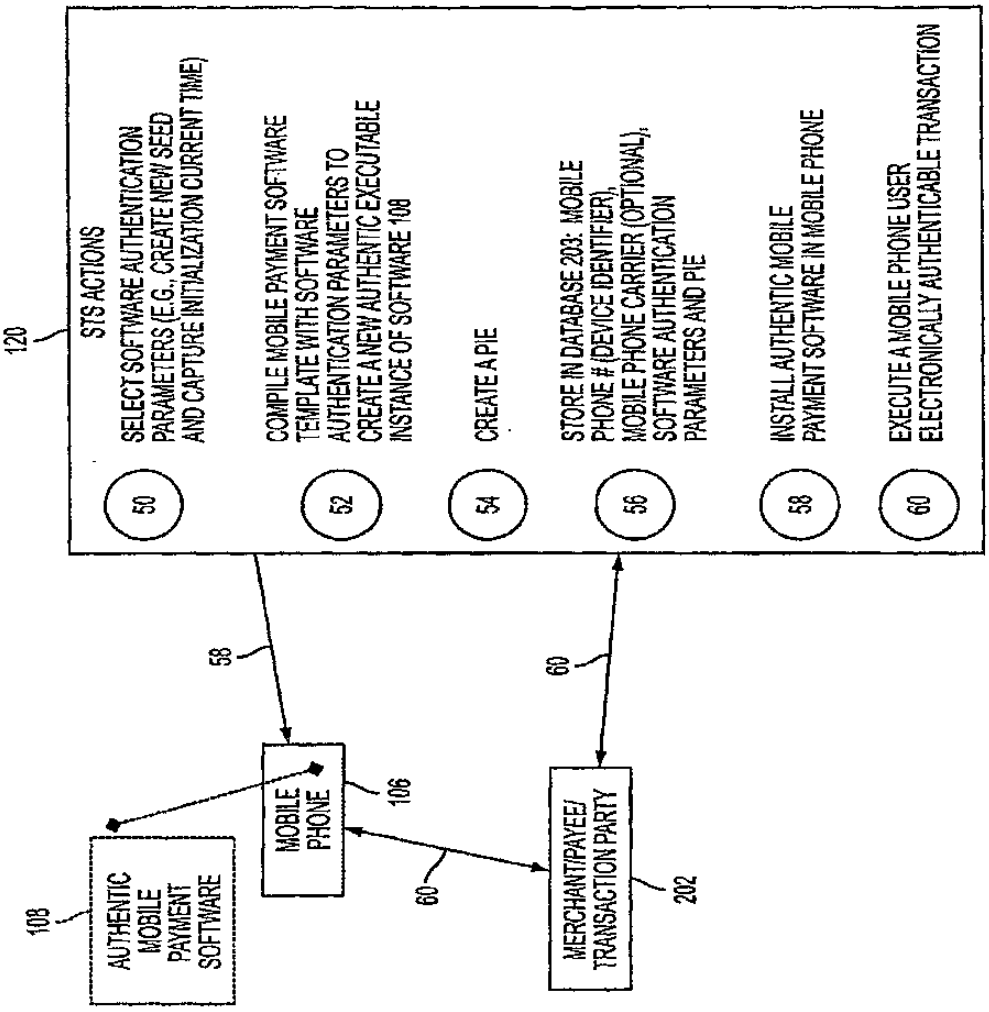


FIG. 1A

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 629 of 1360

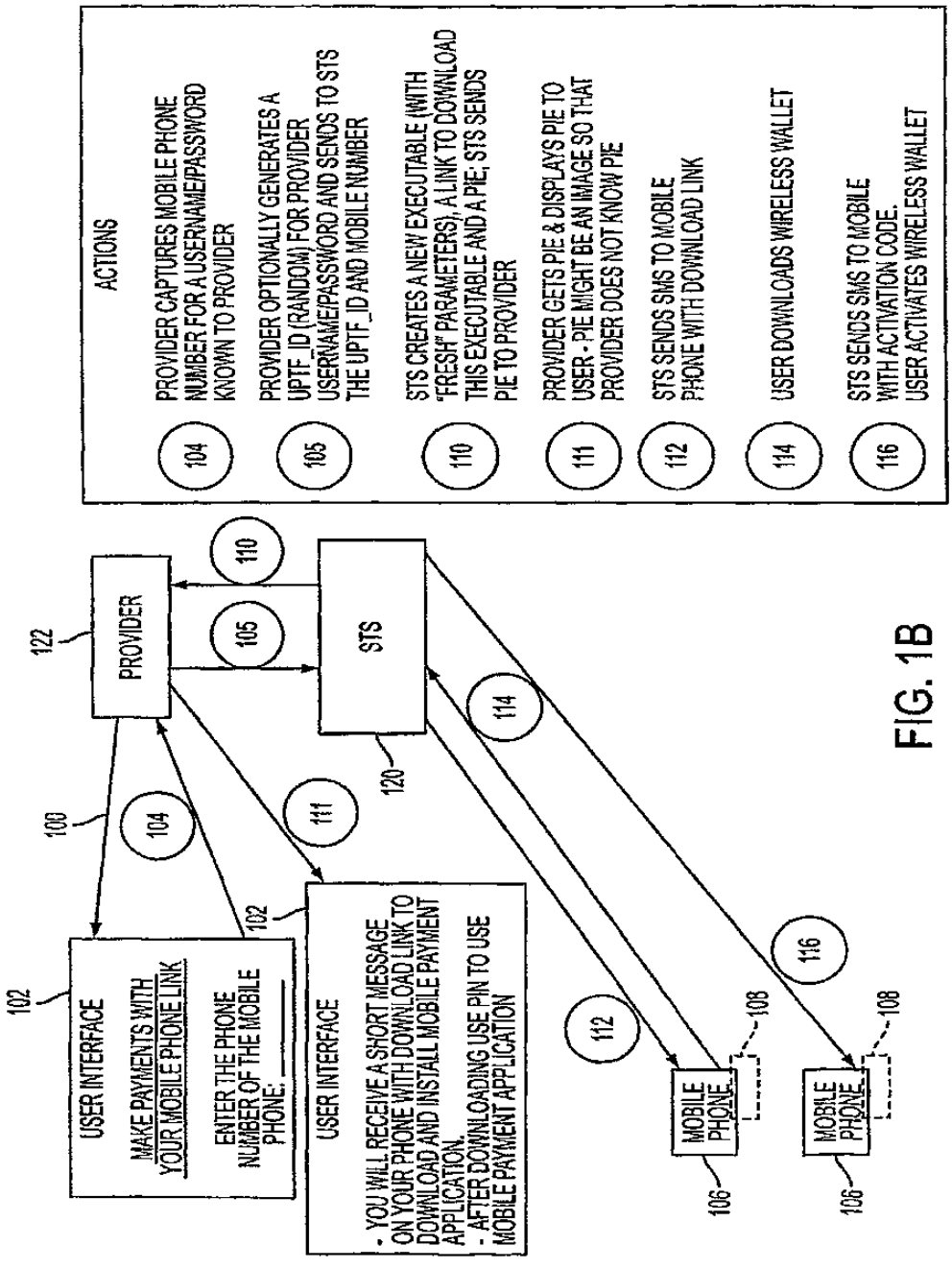


FIG. 1B

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 630 of 1360

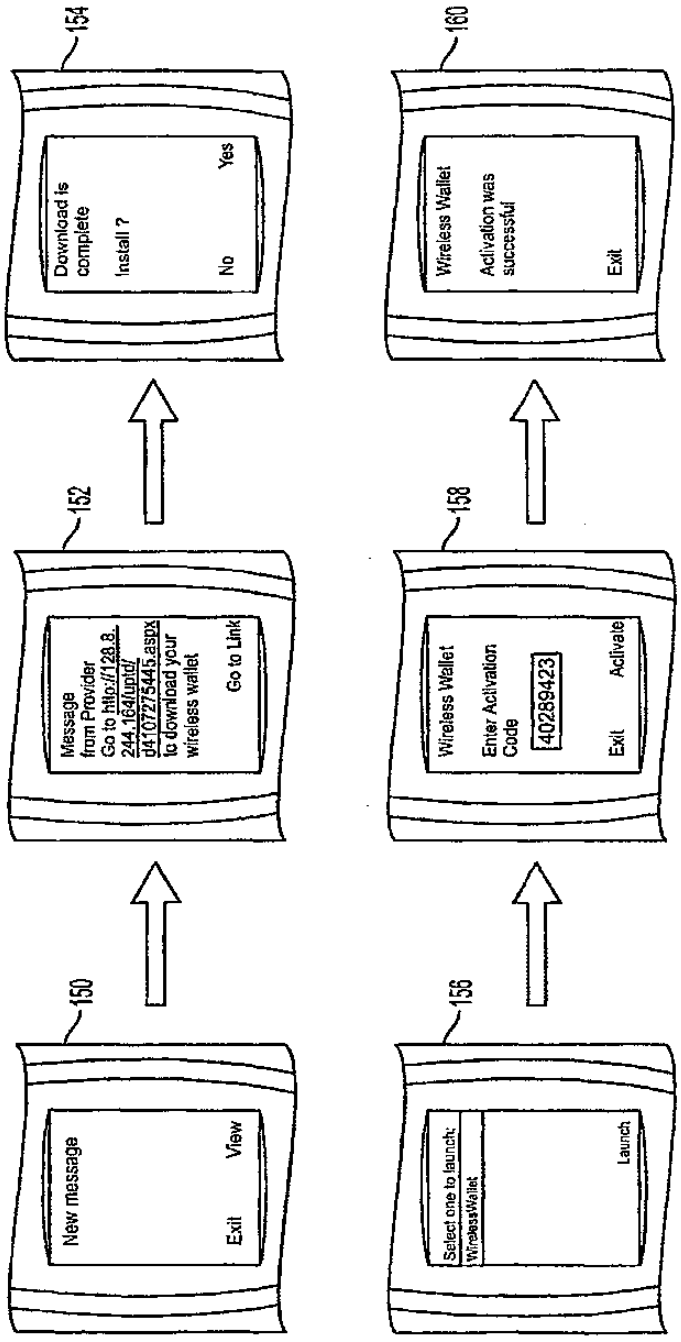


FIG. 1C

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 631 of 1360

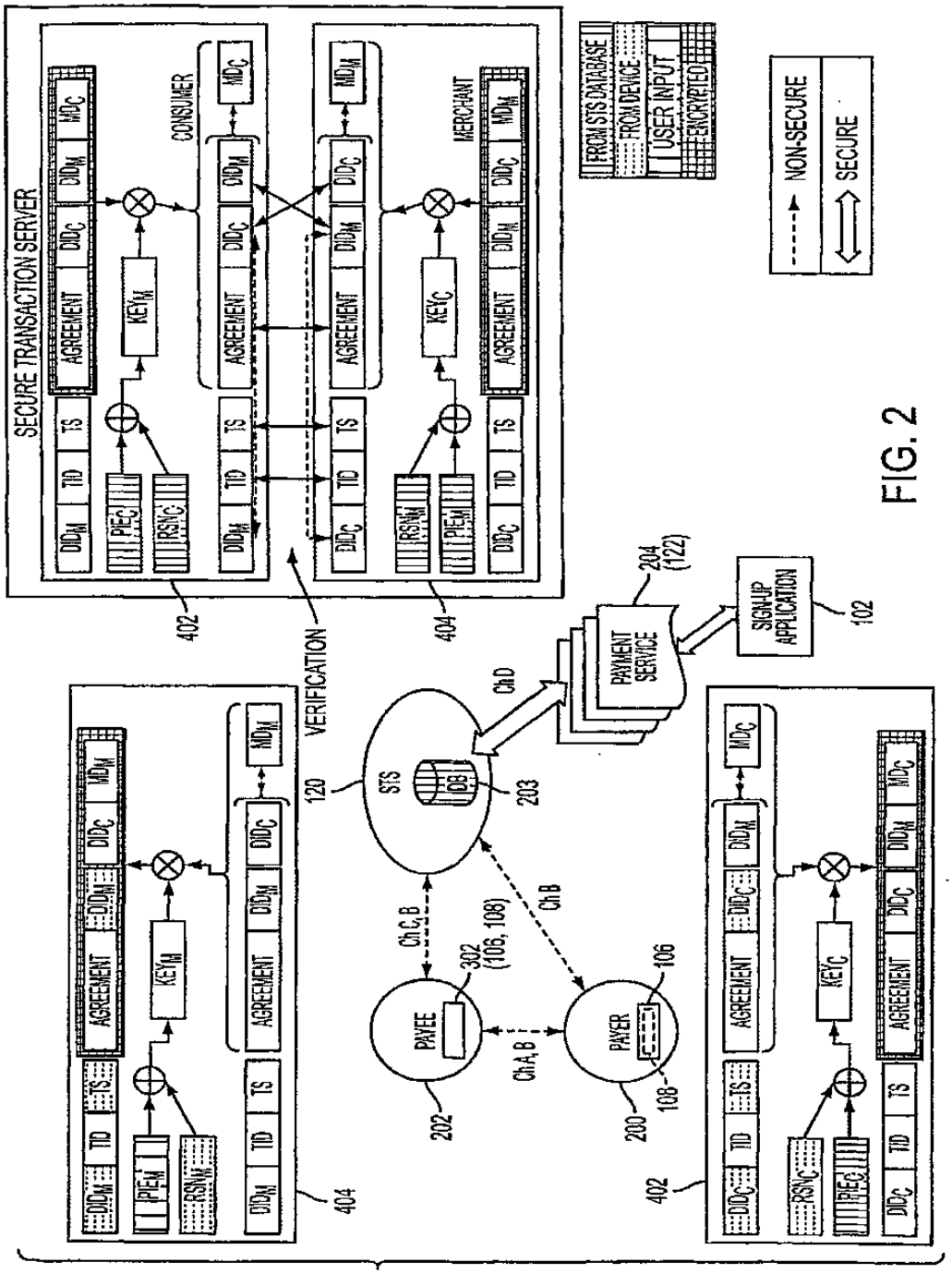


FIG. 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 632 of 1360

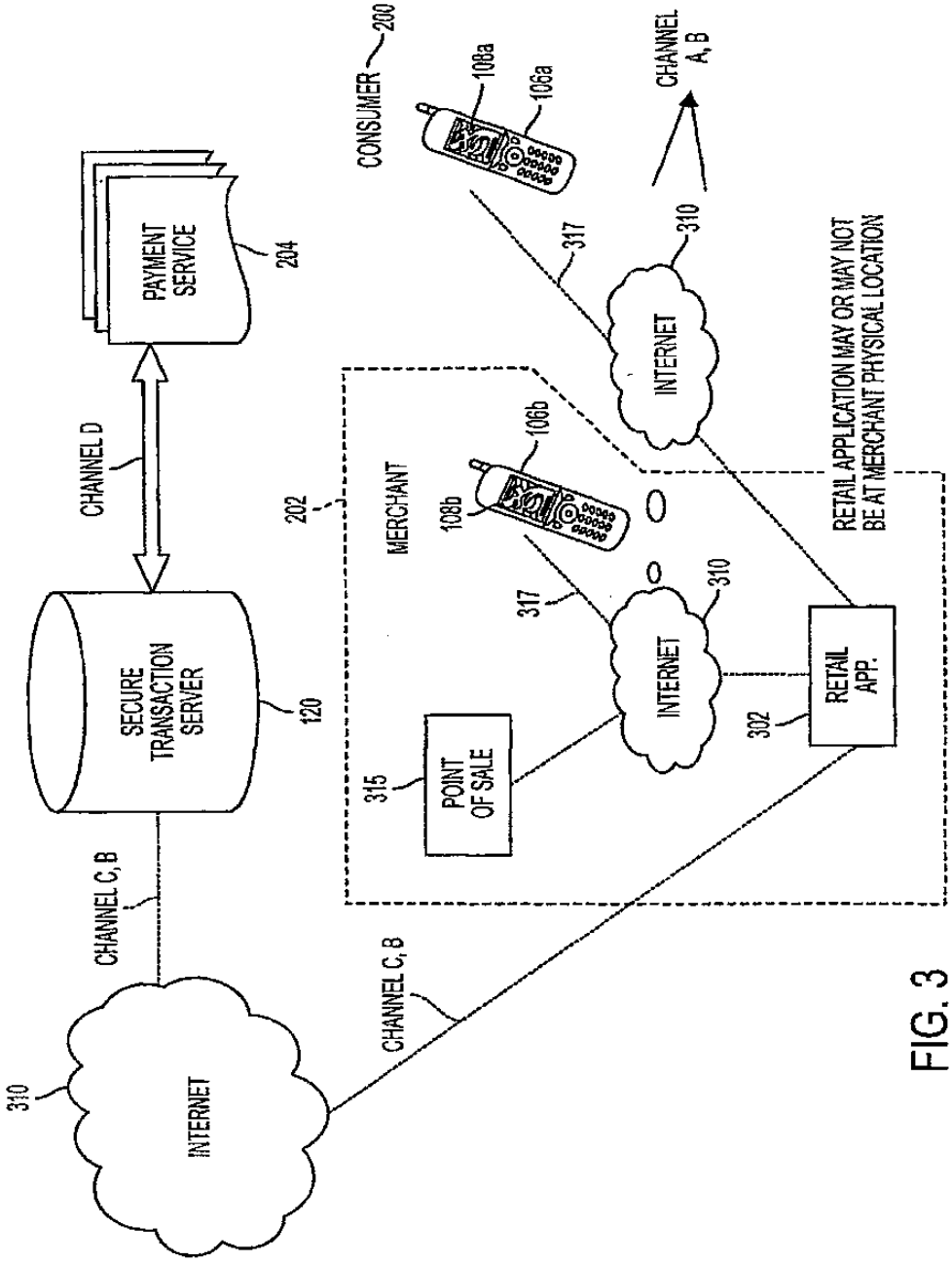
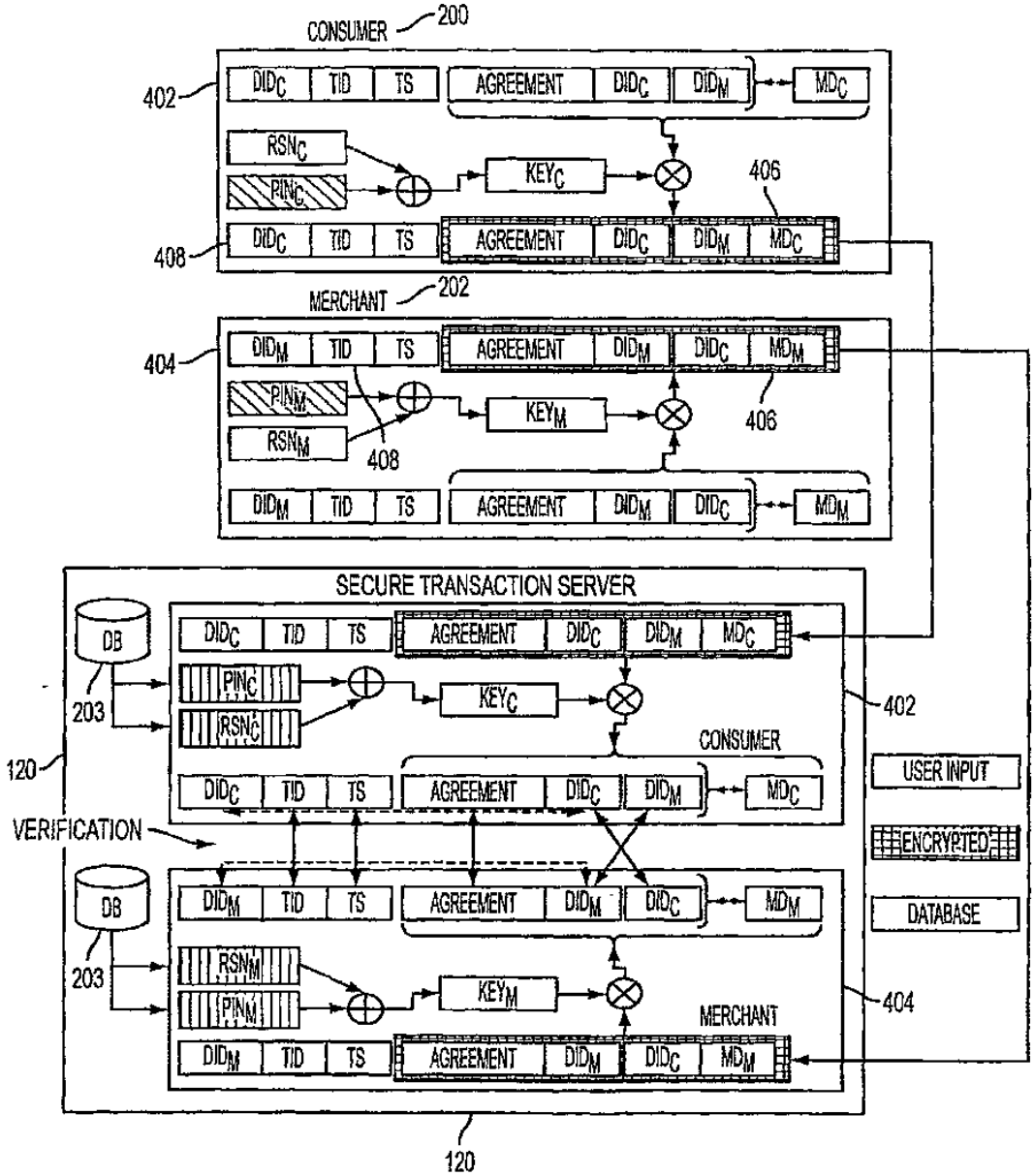


FIG. 3

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 633 of 1360



CONSUMER AND MERCHANT MESSAGE ENCRYPTION AND SECURE TRANSACTION SERVER PROCESSING

FIG. 4

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 634 of 1360

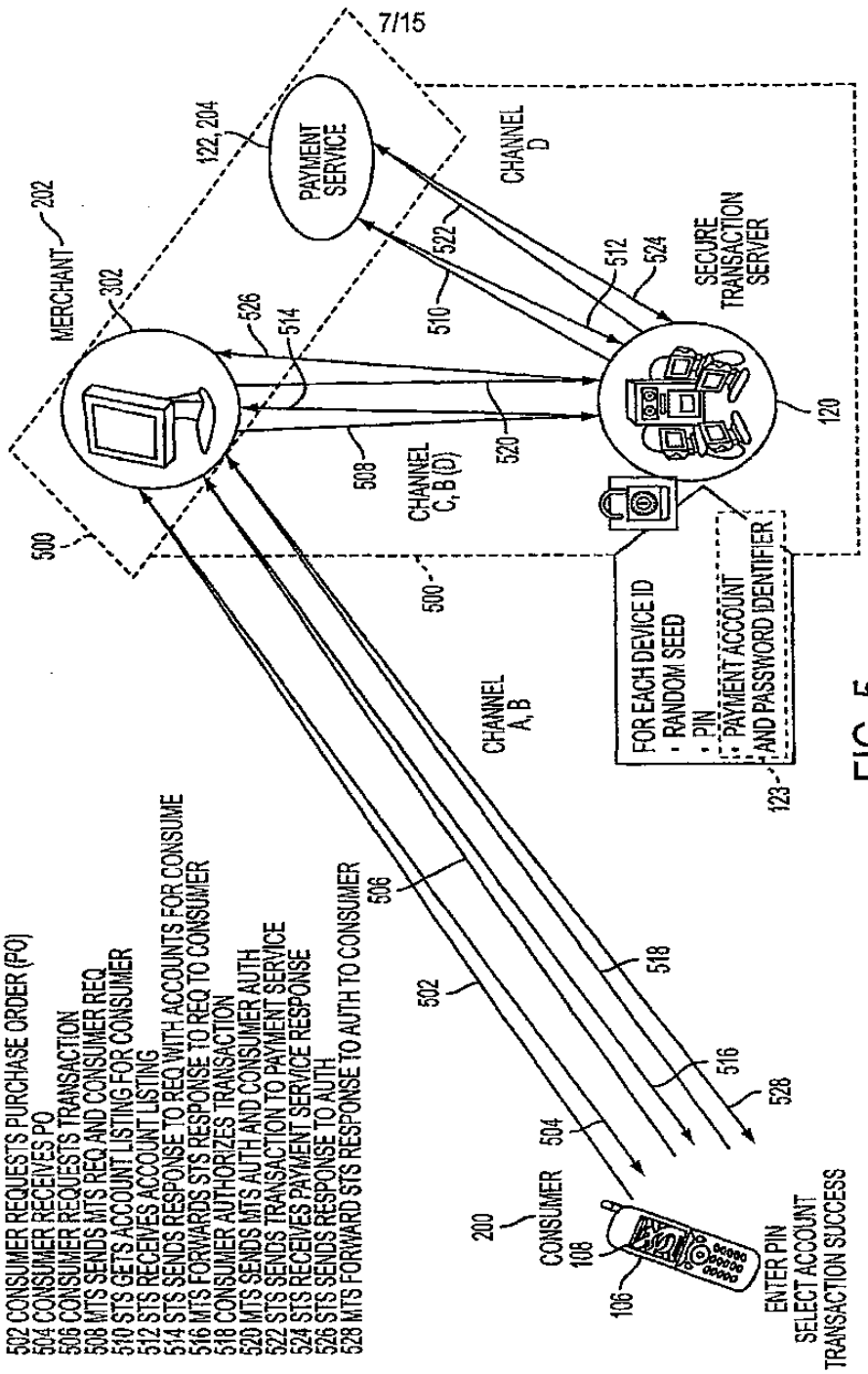


FIG. 5

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 635 of 1360

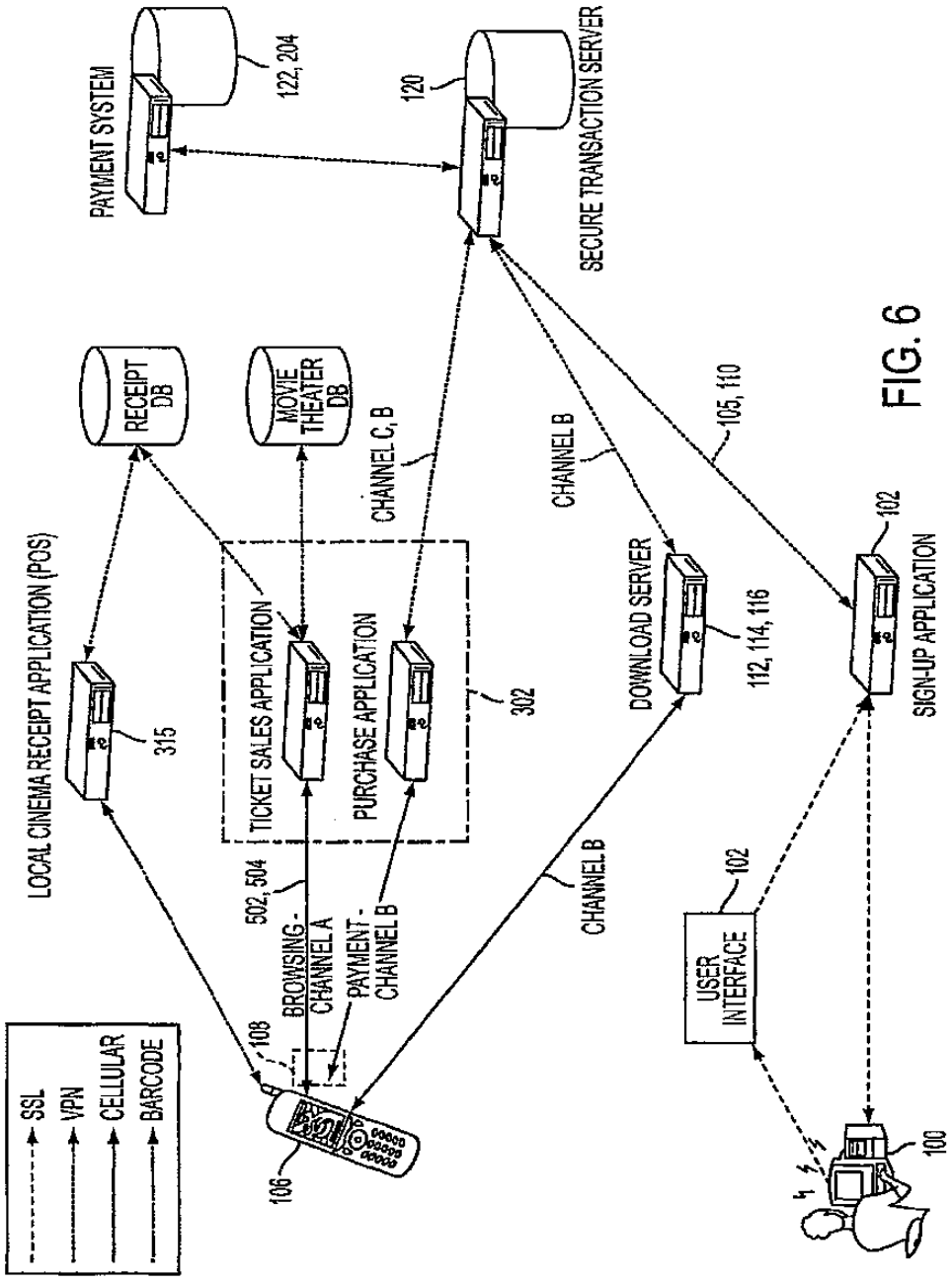


FIG. 6

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 636 of 1360

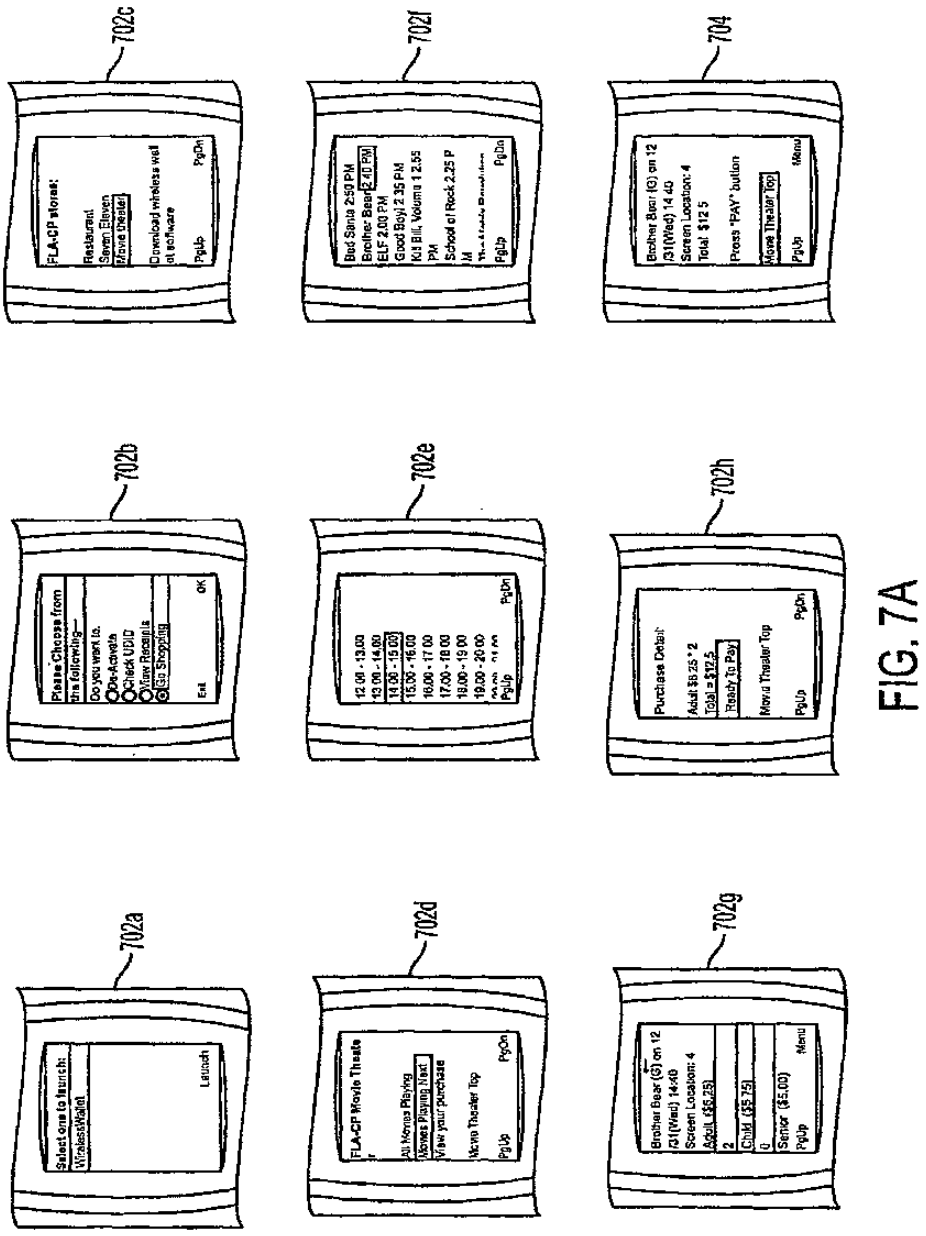


FIG. 7A

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 637 of 1360

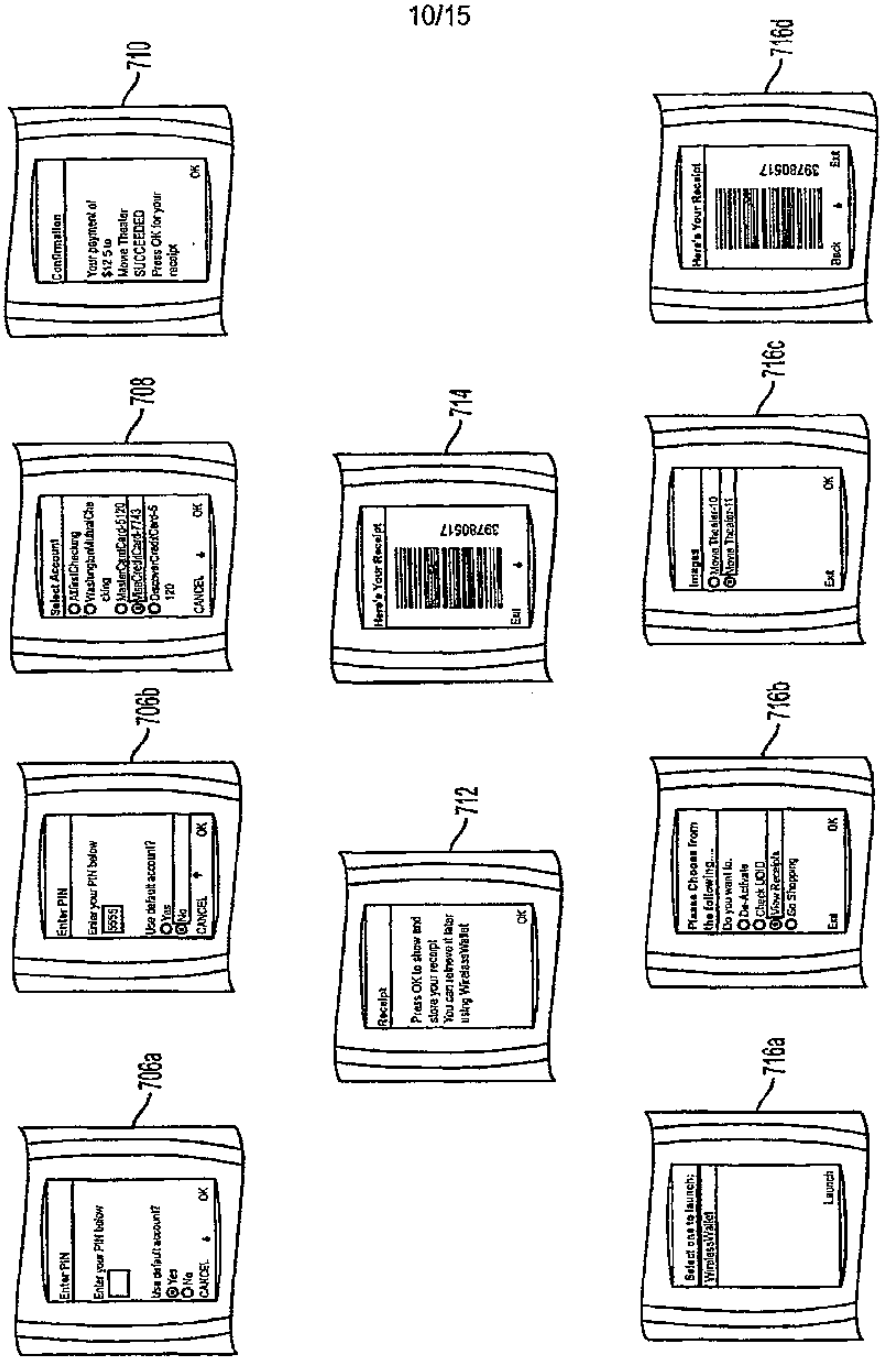


FIG. 7B

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 638 of 1360

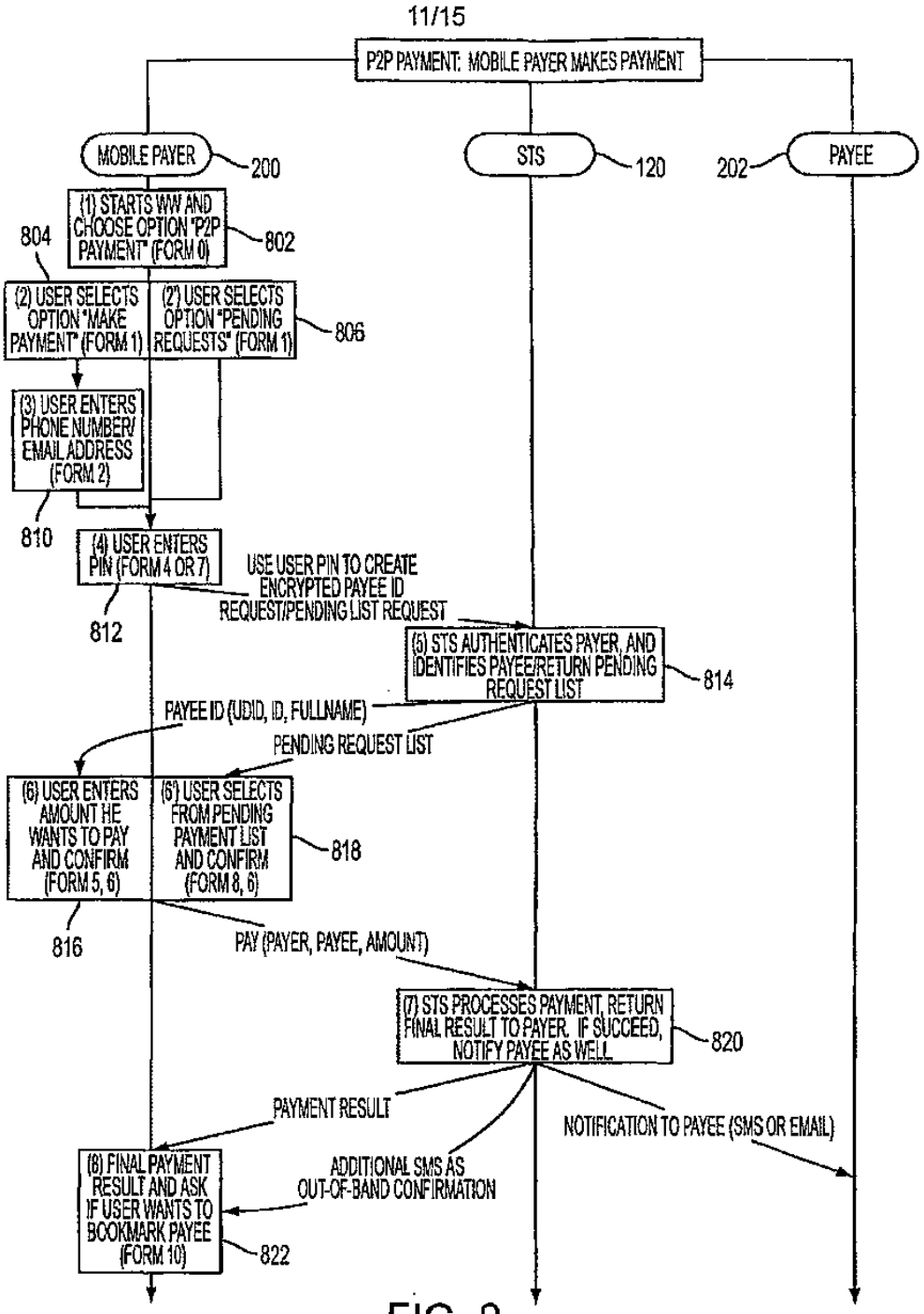


FIG. 8

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 639 of 1360

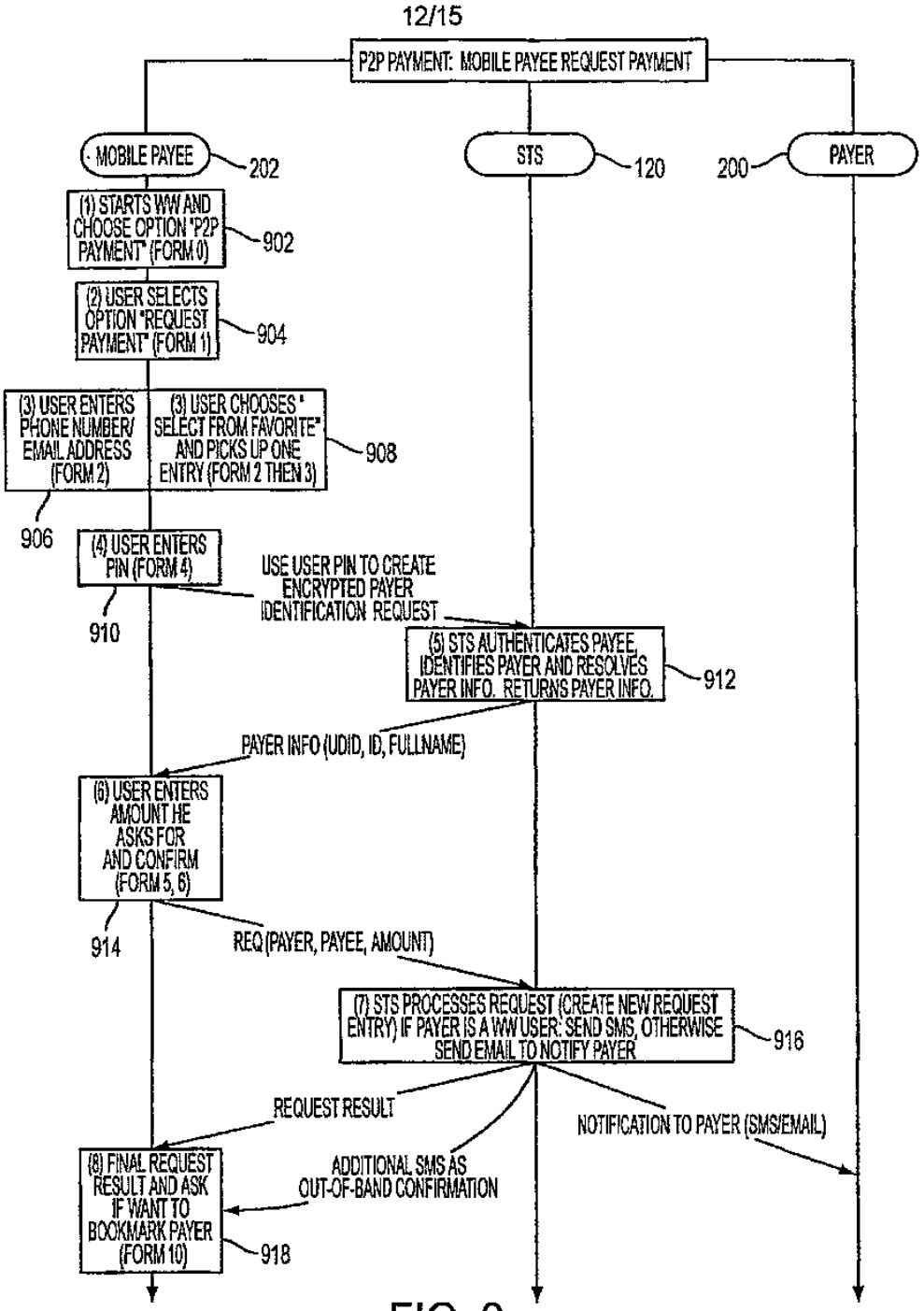


FIG. 9

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 640 of 1360

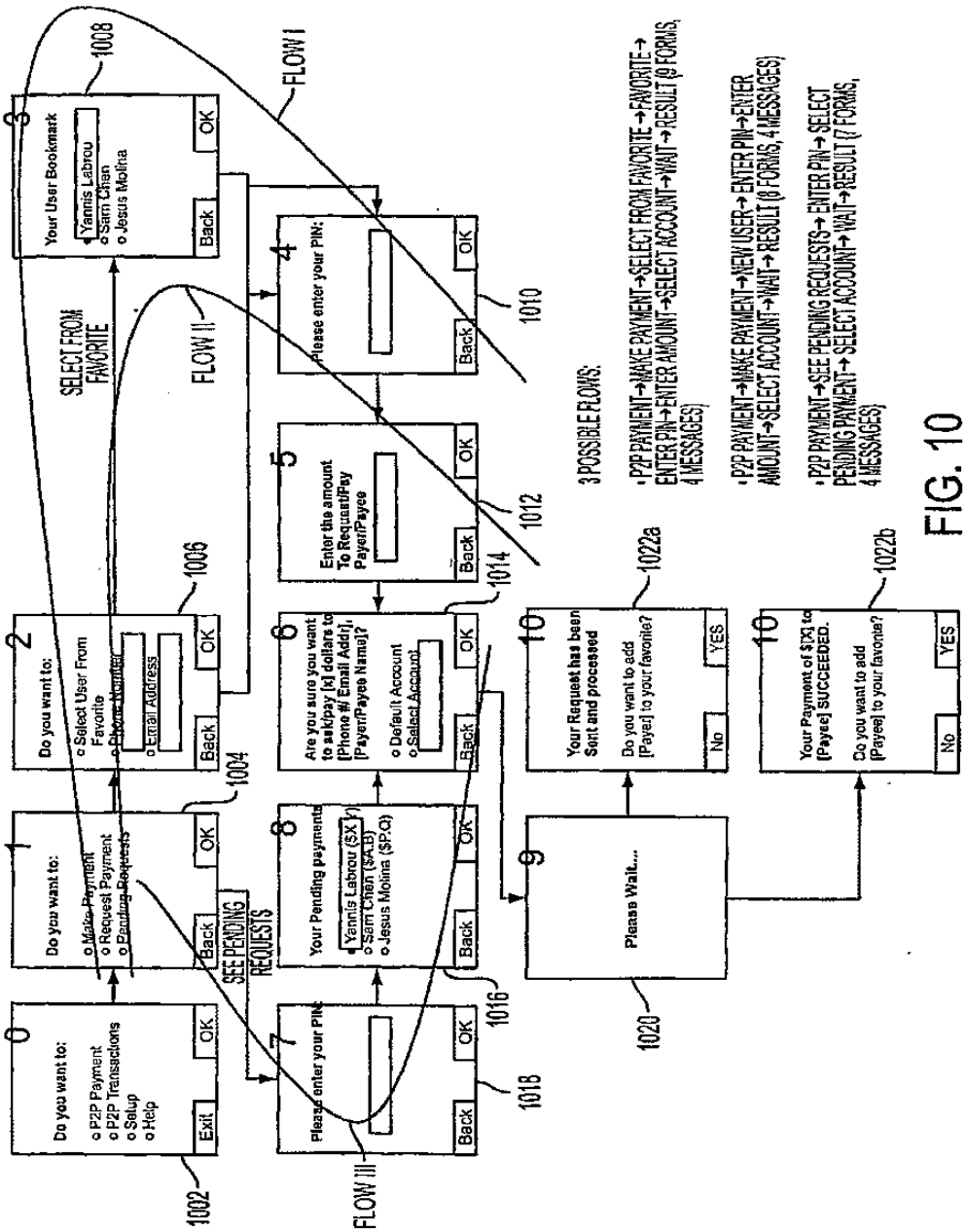


FIG. 10

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 641 of 1360

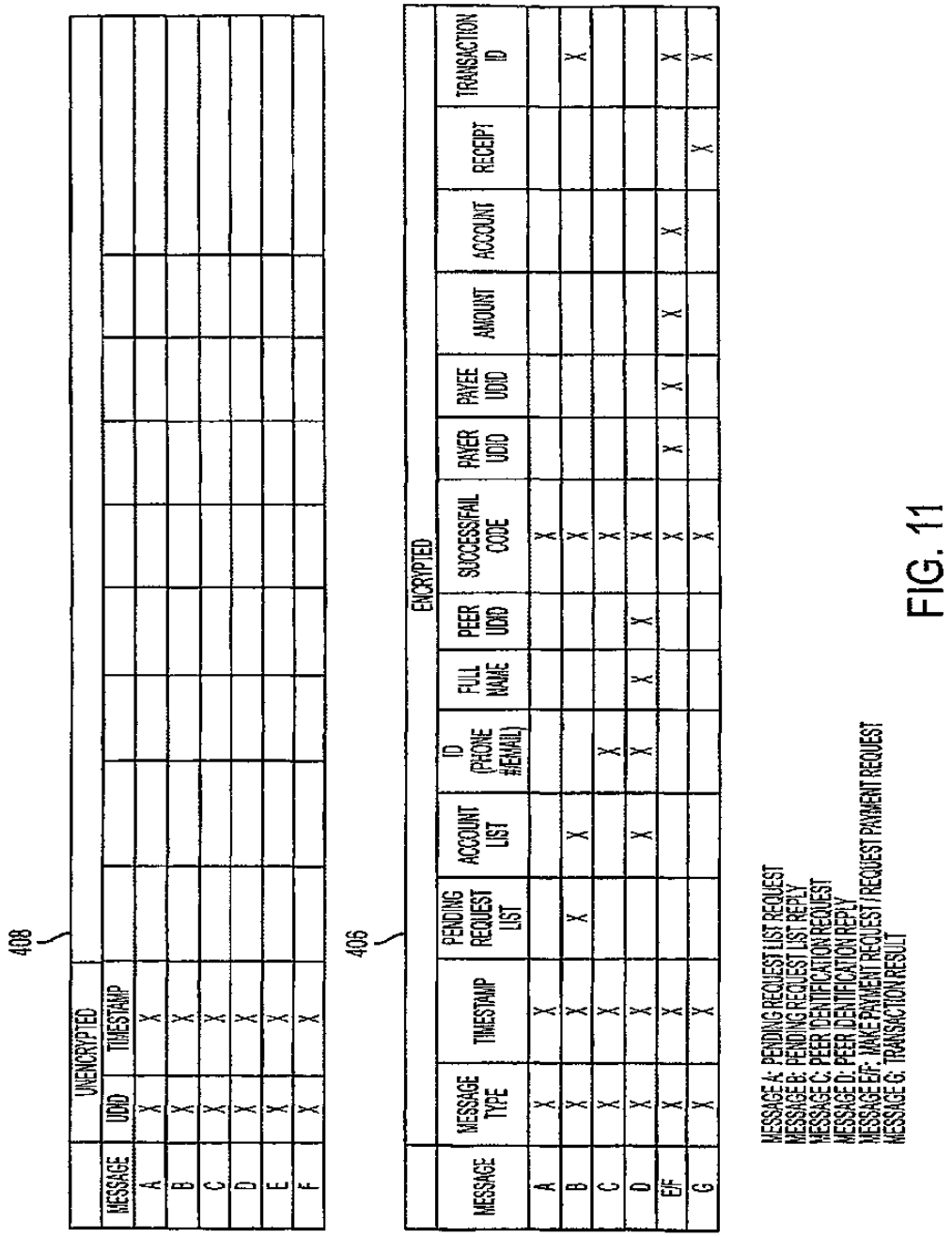


FIG. 11

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 642 of 1360

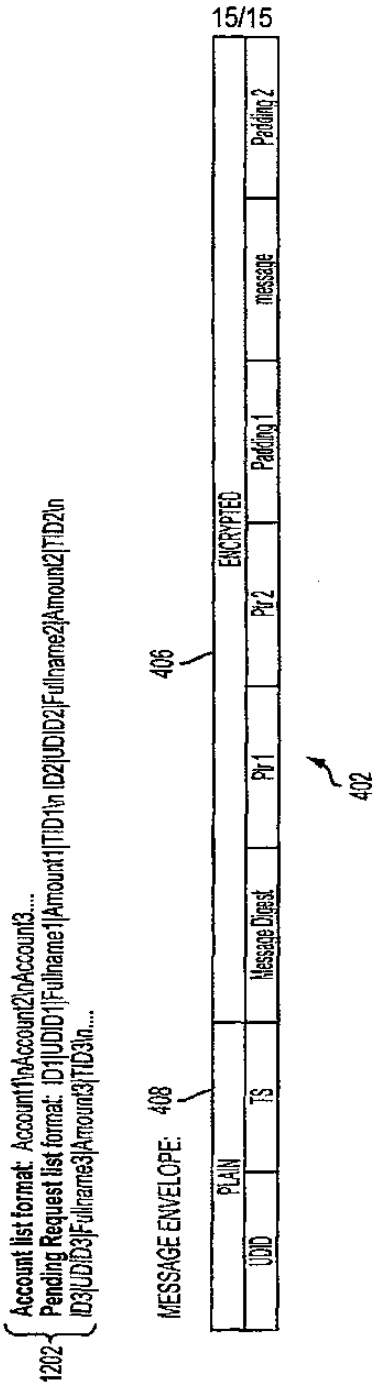


FIG. 12

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 643 of 1360

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/086593 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/IN2005/000038

(22) International Filing Date: 4 February 2005 (04.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
165/DEL/2004 5 February 2004 (05.02.2004) IN

(71) Applicant *(for all designated States except US)*: **A LITTLE WORLD PRIVATE LIMITED** [IN/IN]; 403, Alpha, Hiranandani Business Park, Powai, Mumbai 400 0076 (IN).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GUPTA, Anurag** [IN/IN]; 403, Alpha, Hiranandani Business Park, Powai, Mumbai 400 0076 (IN). **PANDA, Lokanath** [IN/IN]; Flat No. : 103, Srinivasa Residency, 7th Cross, N. R. Colony, Bangalore 560 017 (IN).

(74) Agent: **VAIDYANATHAN, Alamelu**; 451, 2nd Cross, 3rd Block, 3rd Stage, Basaveshwaranagar, Bangalore 560 079 (IN).

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

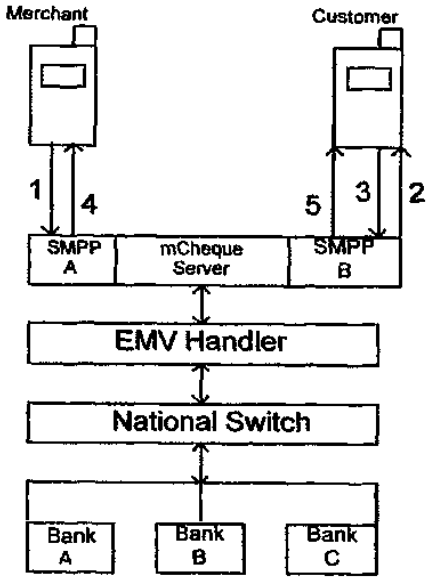
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,*

[Continued on next page]

(54) **Title:** INTER OPERABLE, MULTI OPERATOR, MULTI BANK, MULTI MERCHANT MOBILE PAYMENT METHOD AND A SYSTEM THEREFOR



(57) **Abstract:** This invention relates to an inter-operable Multi-operator, Multi-bank, Multi-merchant Mobile Payment System. This invention makes the mobile phone a debit/credit instrument for payment as well as an instrument to carry out payment terminal functions. The debit/credit card(s) on the mobile phone could be used to carry out payment transactions with another mobile phone, a regular Point-of-Sale terminal, an ATM, a Vending Machine or Internet.

WO 2005/086593 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 644 of 1360

LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

AN INTER-OPERABLE MULTI-OPERATOR, MULTI-BANK, MULTI-MERCHANT MOBILE PAYMENT METHOD AND A SYSTEM THEREFOR.

This invention relates to an Inter-operable Multi-operator, Multi-bank, Multi-merchant Mobile Payment System. This invention makes the mobile phone, a debit/credit instrument for payment as well as an instrument to carry out payment terminal functions. The debit/credit card(s) on the mobile phone could be used to carry out payment transactions with another mobile phone, a regular Point-of-Sale terminal, an ATM, a Vending Machine or Internet.

Introduction:

The existing financial transaction systems involve use of physical currency, debit and credit cards based on Magnetic Stripe technology. The Magnetic Stripe debit/credit card based transactions are inherently prone to security violations given to the fact that Magnetic Stripes can be easily read and duplicated. Also, there are disadvantages in terms of physical damage to the Magnetic Stripe after some swipes on a physical merchant terminal. The existing smartcard based transaction systems are secure, but mandate use of an expensive Point-of-Sale Terminal to carry out a financial transaction, be it a stored value transaction or an online/offline debit/credit transaction.

The secure and more reliable alternative lies in use of a mobile phone, which offers computational capabilities and guarantees security with cryptographic support in the phone/SIM operating system.

Europay Mastercard Visa (EMV) and Common Electronic Purse Scheme (CEPS) standards provide means for development of interoperabe payment scheme. In this context A.Little.World is implementing a new interoperable payment brand in India and abroad known as mCheque. mCheque platform provides a secure all-purpose debit/credit payment system on mobile phones.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 646 of 1360

The proposed solution enables the consumer (hereby referred to as 'payer' or 'customer') to carry out financial transactions from his/her Mobile Phone with debit/credit cards configured on the Mobile Phone and helps the merchant (hereby referred to as 'payee' or 'merchant') to use a hosted Virtual Terminal service, while the mobile phone of the merchant is used as the payment terminal. However the payer can use the debit/credit card(s) configured on the Mobile Phone to engage in a payment transaction with the payee application on the regular Point-of-Sale Terminal, Vending Machine, Internet or ATM.

Large-scale use of mobile-to-mobile payment between customers and merchants - using any mobile phone as an EMV debit/credit payment instrument issued by a Bank, to pay any merchant who has another mobile phone. No additional terminal infrastructure apart from mobile phone is required by Bank or by merchants. No compromises made on transaction security.

Funds flow will be handled entirely through the banks, using proven EMV security with the added layer of mobile network security for secure communications. The EMV handler will provide an effective intermediary solution to the Bank without need for the Bank having to upgrade its back-end infrastructure to EMV.

Public Key Infrastructure (PKI) will be used for non-repudiation in specific application areas. Mobile Phones will have the capability of a universally usable digital ID (to be issued as an X.509 certificate by a Certification Authority) for digitally signing transactions for non-repudiation. RSA is the preferred standard for security implementation for PKI applications of mCheque.

The application download and personalization of the mobile phone can be done both over-the-counter (OTC) and over-the-air (OTA). The complete application functionality for the customer's payment card will be provided on the phone. The application functionality for the merchant's terminal will be provided at the back-end as a Virtual Terminal, with the phone used for confirmation of the transaction (transaction receipt).

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 647 of 1360

The ready availability of communications network; the display screen; and the large memory on the phone to store and view transaction records helps enhance the Bank's product value for the customer and makes this the most user friendly and versatile payment instrument the customer will ever use. The mobile phone can be used both as a credit and debit cards at the same time multiple debit/credit accounts from different banks can be configured on the same mobile phone without any security compromise. A single PIN for all accounts will simplify banking and payment for the customer.

PRIOR ART:

There are known instances of various forms of payment mechanisms using mobile devices, such as Singapore Patent Publication No. 86428 using a payment center backend without use of real debit/credit card and involving a bank in the transaction.

US Patent No. 6,612,488 describes a method of payment using credit cards using a portable communication terminal such as a cellular phone. However, this method does not avoid the use of the credit card or debit card. The portable communication terminal is used to only identify the purchaser to avoid fraudulent use of the cards.

US Patent No. 6, 678, 664 issued to CheckFree Corporation suggests cashless transactions, e.g. purchases of goods and services without making cash payments at the time of purchase, by transmitting, preferably from a point of purchase, information identifying the purchaser of a product without identifying a payment account for the purchaser, the point of purchase being, for example, a register within a retail store or a server at an internet site.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 648 of 1360

Though the aforesaid US patent suggests the use of personal identification information such as purchaser's name, address and drivers license or passport number or any other identification code, this process of identification is little cumbersome and yet requires some document to be carried by the purchaser. Further, the transaction cannot be completed by using a wireless communication device and also it does not offer a virtual terminal to the seller. In other words, the seller is required to have a terminal, a scanner or other similar means to transmit the personal identification details to the bank or to the payment operator.

Objects of The Invention:

- The primary object of the present invention is to provide an inter-operable, multi-operator, multi-bank, multi-merchant, mobile payment method and system.

- In the proposed payment method/system, a regular mobile phone is used as a bank-account linked debit/credit payment instrument to pay any merchant with a regular mobile phone, without customisation of phone hardware. The merchant does not need a regular payment terminal. However, the merchant terminal can be a regular Point-of-Sale terminal, vending machine, Internet or ATM.

- Genuine 'card present' transactions using debit/credit cards configured on the mobile phone.

- EMV Handler solution enabling banks to participate in the secure debit/credit card based transactions without having to migrate to EMV.

The following is the scope of the mCheque payment method/system:

Use a regular mobile phone as an EMV-based payment instrument linked to a debit or credit account in a Bank, to pay any merchant who has a mobile phone or an on-line EMV capable terminal. The merchant does not need a regular payment terminal. EMV security is fully implemented for this product.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 649 of 1360

The ready availability of a communications network; the display screen on the mobile; and the large memory on the phone to store and view transaction records helps enhance the product value for the customer and makes this the most user friendly and versatile payment instrument the customer will ever use. The mobile phone can be used both as a credit and debit cards at the same time. Multiple debit/credit accounts from different banks can be configured on the same mobile phone without any security compromise. A single PIN for all accounts will simplify banking and payment for the customer.

In case of availability of a Subscriber Identification Chip module on the phone (SIM for GSM and R-UIM for CDMA), the application is developed without need to customize either the phone hardware or software. The only change is made to the SIM/R-UIM software through the use of the SIM Application Toolkit or a script using existing SIM/R-UIM browsing environment. In case of phones without having a Subscriber Identification Chip module, the application is developed on the phone. As a result, nearly the entire base of mobile phones can be used as cards and terminals without extra investment required in cards or terminals. The payment application for debit/credit card on payer's mobile phone and the merchant terminal on payee's mobile phone use security mechanisms prescribed by EMV.

The application download and personalization of the mobile phone will be done both over-the-counter (OTC) and over-the-air (OTA). The complete application functionality for the customer's payment card will be provided on the phone. The application functionality for the merchant's terminal will be provided at the back-end, with the phone or a connected PoS terminal being used for confirmation of the transaction (transaction receipt).

The EMV handler solution will be used to provide an effective intermediary solution to banks that have not yet upgraded their back-end infrastructure to EMV. This applies both to the debit/credit card issuance, transaction authorization and merchant acquiring systems of the bank.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 650 of 1360

The transactions will be cleared and settled domestically through the inter-bank switch for domestic transactions or an international settlement agency for cross-border transactions. Security Key management will be provided by the scheme operator or the domestic banking regulator for both Symmetric Keys based on 3-DES or AES and Asymmetric Keys based on RSA.

Multiple mobile operators and multiple issuer and acquiring banks can be part of the system. Funds flow is handled entirely through the banking system, using proven EMV security with the added layer of GSM/CDMA security for secure communications.

The mCheque Platform in its true sense of 'Interoperability' is intended to support existing systems and technologies used by mobile operators, mobile phones, transaction systems and banks.

The following are the unique features of the present invention:

a. Use of mobile phone as a debit/credit card.
b. Use of mobile phone as a merchant terminal.
c. Use of mobile phone to have multiple debit/credit cards
d. Use of mobile phone to store Track-2 data of a debit/credit card.
e. Responsibility of Authentication of mobile debit/credit card transaction lies with the bank and not with mobile operator.
f. Provisioning of debit/credit card on mobile phone without a contact interface using OTA interface.
g. Provisioning of digital certificate on mobile phone without a contact interface using OTA interface.
h. EMV Handler: Authorization of transaction security on behalf of banks. Ability to handle EMV Transactions in a multibank interoperable environment without enforcing the banks to change their existing infrastructure.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 651 of 1360

i. Providing printed payment receipt using a mobile phone, wherever possible without making any change on the mobile phone hardware using an external receipt printer.

j. Payment over Internet using debit/credit card on mobile phone.

k. ATM cash-withdrawal using bank card on mobile phone.

l. Person-to-person transfer of payment or funds transfer using mobile phone both domestic and international.

m. Use of Public Key Infrastructure on mobile phones for transactions requiring non-repudiation.

n. Maintaining and managing loyalty pools and coupons on mobile phone.

This invention thus provides a multi-bank interoperable payment system using mobile phone as debit/credit card which comprises the steps of:

(i) establishing connectivity with multiple mobile operators, issuing banks and acquiring banks participating in the "interoperable mCheque system" and inter-bank clearing & settlement systems, both domestic and international, via the mCheque back-end system/issuance system;

(ii) establishing a link with mutual authentication and trust using standard security mechanism between mCheque issuance system, participating bank and the mobile operator. A third party Certification Authority can provide certificates to establish mutual authentication and trust between different systems.

(iii) providing transaction security which is dependent on the bank's security domain defined on the mobile phone. The mobile network is used as a transport and the system does not necessarily depend on the security provided by the mobile network to guarantee transaction security. However, the security provided by the mobile network is treated as a complementary measure.

(iv) Application Provisioning Step-1: loading of payment application containing the basic menus, transaction logic, application security keys

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 652 of 1360

and application configuration data; on the target mobile phone of payer/payee using the over-the-air system of the mobile operator;

(v) Application Provisioning Step-2: loading of a conventional Track-2 data provided by the participating bank with EMV security keys and risk management parameters on the target mobile phone of payer using the over-the-air system of the mobile operator; and

(vi) Application Provisioning Step-3 (optional): loading of a digital certificate on the target mobile phone of payer/payee using the over-the-air system of the mobile operator requiring non-repudiation; and

(vii) establishing a link between the PIN number allotted to the customer and a common mCheque PIN.

The system takes care of post-issuance activities including blocking/unblocking of debit/credit card, creation/deletion of debit/credit cards, update loyalty pool, loyalty redemption, offering of loyalty coupons, blocking/unblocking/resetting of PIN, key version control, application version control, restoration of debit/credit accounts and loyalty details for a lost/stolen mobile phone.

This invention will now be described with reference to the accompanying drawings, wherein:

Fig. 1 illustrates the mCheque transaction flow;

Fig. 2 illustrates the mCheque transaction system;

Fig. 3 illustrates the mCheque Card Issuance/Merchant Configuration System; and

Fig. 4 illustrates the mCheque Digital Certificate System.

The use of mobile phone as a debit or credit card involves the following five steps, which is illustrated in Fig. 1.

1. Payee Mobile sends a message through mobile network to mCheque back-end with Payer Mobile Number, Transaction Amount and a Random Number.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 653 of 1360

2. mCheque back-end sends a message through mobile network to Payer Mobile with Random Number, Request for Payment and Merchant Details.
3. Payer Mobile sends a message to mCheque back-end through mobile network with EMV Cryptogram.
4. mCheque back-end through mobile network sends a message to Payee Mobile with Transaction Receipt .
5. mCheque back-end through mobile network sends a message to Payer Mobile with Transaction Receipt .

Message-1: Payment Request Message Originating from Merchant

1. Merchant enters the Amount of Transaction, Customer's ID (generally customer's mobile number or a proxy number similar to the mobile number assigned by mCheque) and Merchant PIN using mCheque menus.
2. mCheque Application on Merchant device generates a Random Number (to be used as the seed for the Application Request Cryptogram to be generated on Customer's Mobile Phone for EMV transaction) and signs the transaction data.
3. The Merchant Mobile Phone initiates a session with the mCheque Server and sends the signed data.

Message-2: Confirmation Request Message Terminating on Customer Mobile

1. The signed message from Merchant reaches mCheque Virtual Terminal Application Server (VTAS), which verifies the signature and adds EMV specific terminal risk management parameters and Merchant's Name to the original transaction attributes provided by the merchant.
2. mCheque VTAS initiates a session with Customer Mobile Phone.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 654 of 1360

Message-3: Confirmation Response Message Originating from Customer Mobile

1. Customer Mobile Phone receives the message-2 and displays a confirmation message consisting of Merchant Name, Transaction Amount and Merchant Id. Up on confirmation by the customer, a PIN entry is requested.
2. Up on successful PIN entry, the Customer Mobile Phone generates an Application Request Cryptogram (ARQC) as per EMV specifications using the Card Risk Management Parameters, Random Number, Card Master Key (of the key index assigned for the application in the card security domain).
3. Customer Mobile Phone sends the transaction data with the ARQC to mCheque VTAS.

Message-4: Transaction Receipt Message Terminating on Merchant

1. mCheque VTAS sends the transaction online for authorization of funds
2. After receiving transaction authorization from the Issuing Bank of the Debit/Credit Card on Customer's Mobile Phone, mCheque VTAS sends a Payment Receipt to the Merchant.
3. After confirmation of Receipt delivery, mCheque VTAS issues a Transaction Certificate to the online authorization system of Issuing Bank (denoting completion of transaction).

Message-5: Transaction Receipt Message Terminating on Customer Mobile Phone

1. After receiving transaction authorization from the Issuing Bank of the Debit/Credit Card on Customer's Mobile Phone, mCheque VTAS sends a Payment Receipt to the Customer Mobile Phone.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 655 of 1360

To achieve the above, the present invention provides a transaction system (refer Fig. 2 and 3) which comprises of an unique mCheque virtual terminal capable of handling communications from mobile phones of the payer and payee and also ensure security of the transaction, said server having means for customer database and merchant data base, means for providing hardware security, means for storing the digital certificates and application software for life cycle management of payer/payee application.

The process of obtaining a Digital certificate is illustrated in Fig. 4. The mobile phone of the user or purchaser through the personalization system of mCheque issuance system will send in the necessary request to the certification authority and after processing the request, the certification authority will forward the required certificate through to the personalization system of mCheque issuance system back to the mobile phone of the payer/payee.

The following middleware and application systems constitute the mCheque technology platform:

Backend and Middleware Modules:

- **Virtual Terminal Application Server (VTAS):**

VTAS is a secure cluster of virtual EMV terminals, security systems, loyalty systems, bank/operator interfaces running on a High-Availability platform. All mCheque messages originating from the merchant as well as the customer mobile are routed to the VTAS Server. VTAS spawns one instance of Virtual Terminal Application per Merchant Terminal registered in the mCheque system.

- **USAT Interpreter:**

Application Gateway to interpret and perform application codec (encoding/decoding) functions for data flow between VTAS and Mobile phone.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 656 of 1360

- **EMV Handler:**

The mCheque EMV Handler performs secure authorization of EMV Application Request Cryptogram (ARQC) generated by the chip card EMV application (debit/credit card) on the customer's mobile phone and generates an EMV Application Response Cryptogram (ARPC). The EMV Handler filters EMV specific data from the financial transaction message and the transaction is sent to the Issuing Bank for funds authorization as if it were a regular magnetic stripe transaction authorization request. The EMV Handler therefore provides an effective intermediary Issuing and Acquiring solution for Banks to work with chip cards based on EMV security without having to upgrade their back-end systems to EMV. In case an Issuing Bank is capable of handing EMV transactions directly, the transactions will be directly passed through for authorization by the Bank's EMV Switch. The EMV handler system uses a Hardware Security Module compliant to FIPS-140-2 and PKCS#11 standards to carry out all security operations.

- **Remote Personalization System:**

The mCheque Remote Personalization System provides secure personalization of EMV based secure Debit/Credit cards, Loyalty Pools, Coupons on Mobile phone of mobile phones Over-the-Air (OTA). The Remote Personalization System also uses the OTA bridge for personalization as well as application updates (such as update of EMV risk parameters). Multiple accounts can be handled on a single Mobile phone by this system. The remote personalization system uses a Hardware Security Module to carry out security operations.

- **OTA Bridge:**

Application system providing a secure transport of personalization and transaction data between the mCheque Application Backend (VTAS) and the Network Gateway of mobile operators (USSD Center/SMS Center) for all Over-the-Air application operations on payer/payee mobile phones. The OTA Bridge also takes care of security requirements of the mobile operator.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 657 of 1360

- **USSD-IP Gateway:**

Network gateway providing exchange of Unstructured Supplementary Service Data (USSD) messages between the Mobile Station and the IP-based backend of mCheque Payment Platform. The mCheque USSD-IP Gateway is co-located with the Master Switching Centre (MSC) of the Mobile Operator through an SS7 (Signaling System 7) link.

- **Transaction Switch:**

Host system to switch financial transactions between Switches of participating banks in ISO 8583/XML formats. This system is also used to log the clearing data provided as input to the central Clearing and Settlement Host.

- **Clearing and Settlements Host:**

This system is used process the data that passes through the Transaction Switch to create logs for daily reconciliation to be performed either through a Clearing and Settlements Bank or an automated system. The Clearing and Settlement Institution will be given summaries for net settlements between participating Banks and each participating bank will be given detailed logs of all transactions performed by its customers.

- **MIS and Reporting Tools:**

Management Information System of mCheque Payment Platform includes reporting, logging and audit trail of transactional and operational data for all participating entities in the system, including merchants, customers, issuing banks, acquiring banks, mobile operators and personalization system.

- **ATM Module:**

An application specification will be provided for enhancement of the ATM customer screen to be able to accept ATM cash withdrawal transactions using mCheque. This requires collaboration with ATM vendors and the respective Banks.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 658 of 1360

Applications

- Over-the-counter debit/credit payment for small, large and very large amounts. PIN based debit/credit using secure EMV based technology on any mobile phone.
- More versatile than debit/credit cards.
- Display screen, PIN pad and storage add tremendously to usability, convenience and control.
- Multiple cards/accounts can be issued by multiple banks on one mobile.
- Only one PIN to remember - common PIN for all cards/accounts.
- Transaction amount limits and daily limits can be managed on mobile phone.
- Common rewards points pool across all cards/accounts.
- Small value transactions feasible in both credit and debit mode.
- Transaction details stored on mobile phone.
- Balance enquiry.
- Full audit and traceability.
- Unique new method to receive payments: eliminates need of cheque-book.
- PKI based non-repudiable digital-ID and signatures on mobile phone. Ideal for all kind of Government payments and transactions.
- Secure and convenient payment for Internet purchases (unique new method with highest level of security and convenience).
- Instant, anywhere, anytime payment of utility bills; insurance premiums; mobile phone bills; pre-paid top-ups.
- Payment to vending machines (snacks, beverages, etc.).
- Cash withdrawal at ATM machines with subscription based access to large number of ATMs in arrangement with banks.
- Loyalty points-pool-on-mobile phone for accumulating rewards from different merchants. Instant over-the-counter redemption.

The applications are developed without need to customize either the mobile phone hardware. As a result, the entire base of mobile phones available can be used as debit/credit cards and payment terminals without any significant extra investment.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 659 of 1360

CLAIMS:

1. An inter-operable, multi-operator, multi-bank, multi-merchant mobile payment method using mobile phone as debit/credit card comprising the steps of:
   a. establishing connectivity with each mobile operator, issuing bank and acquiring bank participating in the "interoperable mCheque system" and in any inter-bank clearing & settlement systems, via the mCheque back-end system/issuance system;
   b. establishing a link with mutual authentication and trust using standard security mechanism between mCheque issuance system, participating bank and the mobile operator;
   c. providing transaction security which is dependent on the bank's security domain defined on the mobile phone;
   d. loading of payment application containing the basic menus, transaction logic, application security elements and application configuration data;
   e. loading of at least one conventional Track-2 data provided by the participating bank of the payer, EMV security elements and risk management parameters on the target mobile phone using the over-the-air system of the mobile operator; and
   f. optional loading of digital certificate on the target mobile phone using the over-the-air system of the mobile operator to support applications requiring non-repudiation; and
   g. establishing a link between the PIN number allotted to the customer and the common mCheque PIN.

2. An inter-operable mobile payment method as claimed in claim 1, wherein the loading of payment application is carried out using application provisioning step- 1.

3. An inter-operable mobile payment method as claimed in claim 1, wherein the loading of Track-2 data provided by the participating bank is carried out using application provisioning step-2.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 660 of 1360

4. An inter-operable mobile payment method as claimed in claim 1, wherein the optional loading of the digital certificate on the target mobile phone using the over-the-air system of the mobile operator to support applications requiring non-repudiation is carried out using application provisioning step-3.

5. An inter-operable mobile payment method as claimed in claim 1, wherein multiple debit/credit card Track-2 data are loaded on the mobile phone.

6. An inter-operable mobile payment method as claimed in claim 1, including an EMV handler for handling EMV Transactions in a multi-bank interoperable environment.

7. An inter-operable mobile payment method as claimed in claim 1, including software for maintaining and managing loyalty pools and coupons on mobile phone.

8. An inter-operable, multi-operator, multi-bank, multi-merchant mobile payment system using mobile phone as debit/credit card comprising of;
   a. mCheque back-end system/issuance system comprising means for establishing connectivity with each mobile operator and issuing bank participating in the "interoperable mCheque system" and in any inter-bank clearing and settlement systems;
   b. Means for establishing a link with mutual authentication and trust using standard security mechanism between mCheque issuance system, participating bank and the mobile operator;
   c. Means for providing transaction security which is dependent on the bank's security domain defined on the mobile phone;
   d. Application provisioning software I to enable loading of payment application containing the basic menus, transaction logic and application configuration data;
   e. Application provisioning software II to enable loading of at least one conventional Track-2 data provided by the participating bank on the target mobile phone using the over-the-air system of the mobile operator;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 661 of 1360

f. Application provisioning software III for optional loading of digital certificate on the target mobile phone using the over-the-air system of the mobile operator to support applications requiring non-repudiation; and

g. Means for establishing a link between the PIN number allotted to the payer and the common mCheque PIN.

9. An inter-operable mobile payment system as claimed in claim 7, wherein multiple debit/credit Card Track-2 data are loaded in the mobile phone.

10. An inter-operable mobile payment system as claimed in claim 7, including an EMV handler for handling EMV Transactions in a multi-bank interoperable environment.

11. An inter-operable mobile payment system as claimed in claim 7, including software for maintaining and managing loyalty pools and coupons on mobile phone.

12. An inter-operable mobile payment system as claimed in claim 7, wherein the mobile phone of user is used as debit/credit card.

13. An inter-operable mobile payment system as claimed in claim 7, wherein the mobile phone of the merchant is used as merchant terminal.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 662 of 1360

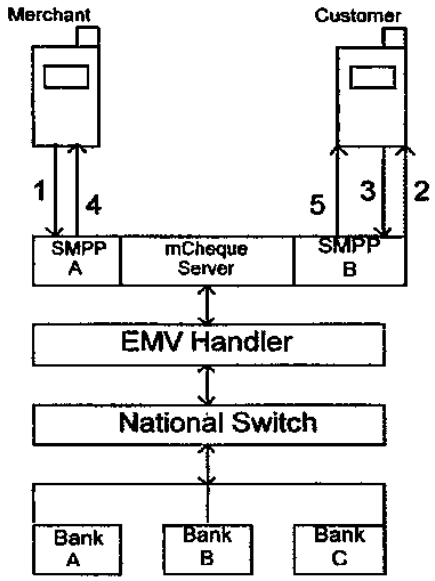

Merchant
Customer
1
4
5
3
2
SMPP A
mCheque Server
SMPP B
EMV Handler
National Switch
Bank A
Bank B
Bank C

Fig. 1.

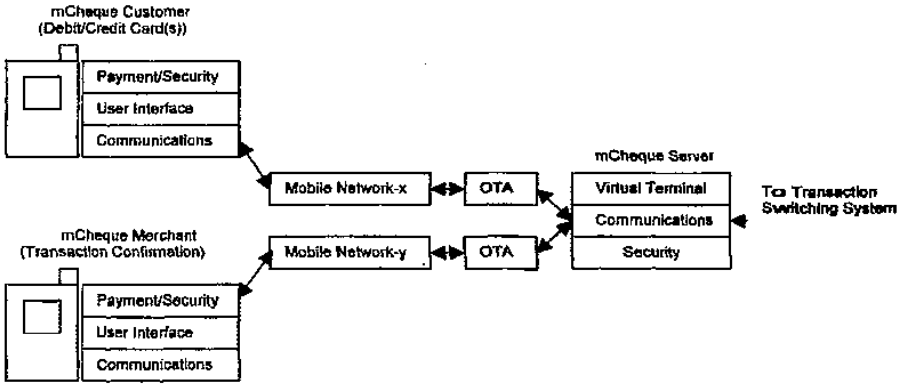

mCheque Customer
(Debit/Credit Card(s))
Payment/Security
User Interface
Communications
Mobile Network-x
OTA
mCheque Server
Virtual Terminal
Communications
Security
To Transaction
Switching System
mCheque Merchant
(Transaction Confirmation)
Mobile Network-y
OTA
Payment/Security
User Interface
Communications

Fig. 2

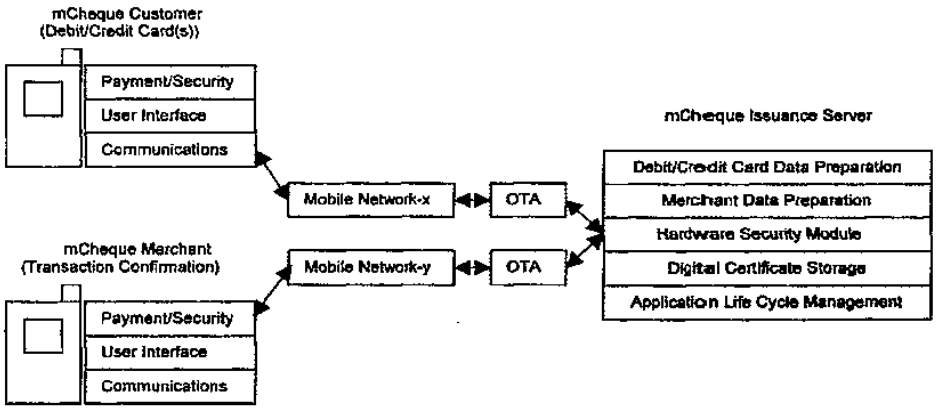


Fig. 3

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 665 of 1360

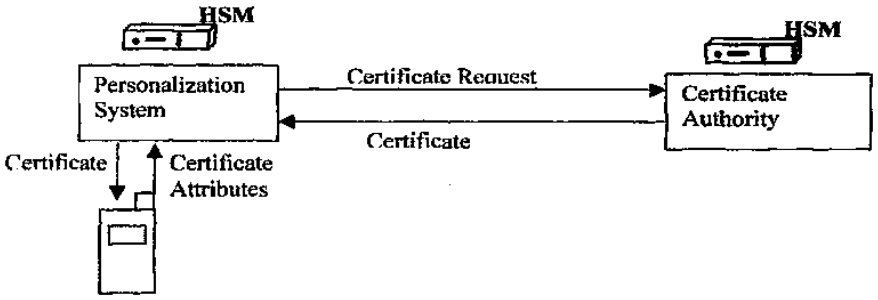

HSM
HSM
Personalization System
Certificate Request
Certificate
Certificate Authority
Certificate
Certificate Attributes

Fig. 4.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2007 (21.12.2007)

PCT

(10) International Publication Number
WO 2007/145500 A1

(51) International Patent Classification:
G07F 19/00 (2006.01) *G06Q 10/00* (2006.01)
G06Q 20/00 (2006.01) *H04M 15/00* (2006.01)
H04M 17/00 (2006.01)

(21) International Application Number:
PCT/MY2007/000038

(22) International Filing Date: 11 June 2007 (11.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 20062712 12 June 2006 (12.06.2006) MY

(71) Applicant *(for all designated States except US)*: **MOBILE MONEY INTERNATIONAL SDN BHD** [MY/MY]; Lot 23-24, 2nd Floor, I.O.I. Business Park, 47100 Puchong, Selangor (MY).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LOH, Jin, Feei, Jeffrey** [MY/MY]; 55 Jalan BU 10/7, Bandar Utama, 47800 Petaling Jaya, Selangor Darul Ehsan (MY). **LEE, Eng, Sia** [MY/MY]; 18 Halaman York, Georgetown, 10450 Penang (MY).

(74) Agent: **CHEW, Kherk, Ying**; Wong & Partners, Level 41 - Suite A, Menara Maxis, Kuala Lumpur City Centre, 50088 Kuala Lumpur (MY).

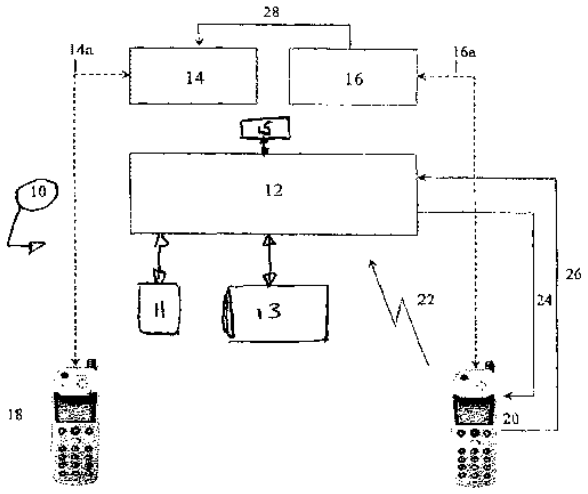
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

[Continued on next page]

(54) Title: TRANSACTION SERVER



(57) Abstract: A transaction server is disclosed that has a receiver module configured to receive an instruction message from a first mobile communications device for a transaction from a first account to a second account. The transaction server also has a transmission modul configured to send a response message to the first mobile communications device a request for a validation instruction for the transaction, the response message being in response to the receipt of the instruction message. The server is configured to record receipt of the validation instruction. The server is also configured to record receipt of the validation instruction. In response to the validation instruction, the server validates and effects the transaction. A corresponding method is also disclosed.

WO 2007/145500 A1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 667 of 1360

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TRANSACTION SERVER

Technical Field

The invention relates to a transaction server for effecting transactions from a user account. More particularly, the invention relates to validating transactions from the user account.

Background

Systems for implementing mobile phone based payments where, essentially, a mobile telephone acts as an electronic wallet (e-wallet) are known. In such systems, a monetary value is held in an e-wallet for each user, and the details of each e-wallet are stored centrally in a server database.

With a mobile telephone, transactions may be conveniently and commonly effected using a messaging service such as SMS. For example, to send $20 from a first e-wallet identified or associated with a first mobile phone +60122070239 to a second e-wallet identified with a second mobile phone +60164452228, the following SMS is sent:

```
PAY 0164452228 20 753535
```

As can be seen, the text string of the message comprises several fields: "0164452228" is the recipient mobile telephone's number; "20" is the transfer amount (e.g. $20); and 753535 is a six-digit PIN associated with the user and/or the e-wallet +60122070239. The server receives this SMS through a telecommunication link to an SMS centre or portal.

Such a system is attractive because it facilitates money movement. It means practically anyone, anytime, anywhere can be paid. For example, to pay a friend several miles away all a user need do is to use their mobile telephone to send a simple SMS to the SMS portal to effect payment from the e-wallet or account.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 669 of 1360

Unfortunately, such a system has several drawbacks which, if not properly addressed, can adversely affect its implementation and security.

Messaging services such as SMS as a means of communication are never 100% reliable. A sender of an SMS never knows for certain if the message will be delivered or when. Sometimes an SMS is delivered to the same recipient multiple times. These failings of SMS are particularly problematic for e-wallet transactions. For example, a user may be at a shop and use their mobile telephone to send an SMS to the server's SMS portal requesting payment for goods to the shop owner's account. However, it is possible that the mobile telephone may not receive acknowledgement from the server that the payment request has been either received, or that payment has been initiated. Such situations can arise during a period of peak use of the SMS system or, simply, the SMS is "dropped" by the messaging service. In such situations, the user is presented with a quandary. What should the user do? Should the user just leave? Should the user send another payment request? The server might receive the user's first SMS and effect the transaction the moment after a second instruction SMS is sent, or the user gives up and leaves the shop. Alternatively, the server might receive several copies of the single SMS and the server effects multiple payments to the shop owner for a single transaction. The user is unlikely to be able to receive any real help from the help centre for the server as the call centre may advise the user that the SMS has not arrived yet and that no transaction has been effected so far. Conceivably, the SMS could arrive at the server the very moment the user terminates the telephone call with the call centre.

Another problem is human error. Inevitably, users will key in a wrong recipient's mobile number or incorrect transaction amount in the SMS. The user may call the call centre to request a reversal. In cases like these, security for the recipient could be compromised – e.g. the recipient is a shop owner who has provided goods or services in good faith to an e-wallet user. Should the call centre do the reversal? The user may have just bought something from the shop owner and requested a reversal the moment after the goods were collected or the user has left the shop.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 670 of 1360

Security is another problem. It is a well-known fact that SMS can be spoofed quite easily. If a fraudster somehow manages to obtain a person's PIN, the fraudster can spoof an SMS message to the server to instruct a transaction quite easily.

Summary

The invention is defined in the independent claims. Some optional features of the invention are defined in the dependent claims.

If the transaction instruction (e.g. SMS from the user to the server) is delayed or not delivered, the user knows very well no transaction has been effected from his account (e-wallet) as the user is neither requested to provide the validation instruction and, therefore, it is not possible for the user to provide the validation instruction. If the user receives a request for the validation instruction from the server at a later time seeking validation for the transaction, the user then has the option to proceed with the validation instruction for the transaction or to decline to send the validation instruction. In the event the server receives multiple copies of the transaction instruction (e.g. SMS), the server may be configured also to send multiple requests for validation in the form of SMS messages to the user seeking confirmation and the user can choose how many of these requests for a validation instruction he/she can reply to, if any. In embodiments of the invention, each request for validation provides different instructions for effecting the validation instruction (e.g. different telephone numbers are provided for the user to call to validate the transaction). The user may then selectively choose whether and how many times the recipient in the transaction is to be paid. Optionally, additional information such as the account (e-wallet) balance and details of previous transactions are included in the request for the validation instruction.

Further, the likelihood of user error is now significantly reduced. In embodiments of the server, the server is configured to look up the recipient's name from a server database, and to transmit the requested recipient's details to the user with the request for the validation instruction to the user. Optionally, the transaction amount is also shown.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 671 of 1360

Yet further, the server provides enhanced security and fraudsters may find it more difficult to spoof the server. The server may selectively choose the means by which the user is to request validation of the transaction; e.g. in embodiments of the invention, a telephone number for the user to call or message to is randomly picked from hundreds of numbers; the user may be requested to enter a URL on the user's internet browser to request validation, or any of many other possible ways in which a communication can be effected. Thus, the fraudster will not know the number to call to confirm a transaction, or the URL to visit. This means the fraudster must intercept the request for validation of the transaction sent by the server and at the same time spoof a user ID.

Brief Description of the Drawings

Exemplary embodiments will now be described, by way of example only, and with reference to the accompanying drawings. In the drawings:

Fig. 1 is a block diagram illustrating implementation of an exemplary;

Fig. 2 is a flow diagram illustrating the process of the implementation of an exemplary embodiment;

Fig. 3 illustrates the process of an exemplary embodiment; and

Fig. 4 illustrates a schematic view of the basic structure of an e-wallet system.

Detailed Description of the Exemplary Embodiments

Implementation of a transaction with a transaction server is illustrated in Figure 1. The system 10 comprises a transaction server 12, a first e-wallet 14 representing/being associated with a first account, and a second e-wallet 16 representing/being associated with a second account. The first e-wallet 14 is associated with the mobile communication device 18 and in particular with the owner of mobile communications device 18. Association with the device 18 is represented by the dashed line 14A. Association of second e-wallet 16 with the second mobile communication device 20 is represented by the dashed line 16A. Mobile communications devices 18, 20 may be a mobile telephone, portable telephone, cellular telephone, PDA, a device such as a "Blackberry", or telecommunications-enabled portable computer such as a laptop computer, notebook computer, tablet computer, and so forth.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 672 of 1360

To effect a transaction, the second communication device 20 is used to send a message 22 via a messaging service – e.g. SMS, MMS or email – to a receiving module such as, for example, the SMS portal 13 of server 12. The intended transaction is for the transfer of a sum of money to the e-wallet 14 of the first user being the user of communication device 18. The message 22 takes the form of:

```
PAY 0164452228 20 753535
```

As discussed above, the first field is the instruction "PAY", second field in the transaction instruction is an identifier for the recipient account preferably being the telephone number of first communication device 18; third field "20" is the value of the transaction; and the fourth field 753535 is an authentication code for the transaction, for example, a PIN of the second communication device 20 or a specific authentication code for the transaction. This provides a first level of security for the transaction. Responsive to receiving the instruction 22 from the device 20, the server 12 first matches the authentication code of the fourth field with the stored authentication code (extracted from the server 12 by, for example, recognition of the telephone number of the communication device 20 and using a look-up table to find the authentication code) and a transmission module 11 of the server sends to the device 20 a request 24 for the transmission of a validation instruction for the transaction. In embodiments of the server 12, this request may also be sent via a messaging service. Should the second user at device 20 wish for the transaction to be processed, the device 20 is then used to send a validation instruction 26 to the receiving module 13 of server 12. The server 12 records receipt of the validation instruction 26 and, responsive to this, the server 12 validates the transaction. Embodiments of the server then effect the transaction 28 of (in this example) $20 from second e-wallet 16 to first e-wallet 14.

Embodiments of the server 12 allow for the communication device 20 to be used to make a telephone call to a communications module 15 of the server 12 (or another communications portal) to provide the validation instruction. The request for the transmission of a validation instruction may, in embodiments of the server 12, provide details of the telephone number at server 12 to be called.

Embodiments of the server 12 are configured only to allow receipt of reliable means of communication for the request for validation: e.g. a telephone call, a message sent through GPRS (General Packet Radio Services) or through a secure (e.g. encrypted) internet communication.

It will be appreciated that one or more of the communications portals 11, 13, 15 may be distinct from server 12, may be used to send and receive communications from the devices 18, 20. In such embodiments of the server 12, the server 12 is configured to initiate and control sending and receipt of these instructions, so that a transaction may be effected from an account/e-wallet 16.

It will be further appreciated that embodiments of the server 12 allow for the e-wallets 14, 16 to be integral with the server 12.

In embodiments of the server 12, the server 12 is configured to validate the transaction if receipt of the validation instruction is recorded by the server 12 within a pre-determined period from sending, to the communication device 20, the request 24 for the transmission by device 20 of a validation instruction. If the receipt of the validation instruction 26 is not recorded by the server 12 within that pre-determined time period, the transaction may be voided.

After the server 12 receives a transaction request 22 (say at 5:15pm 24th May) from the device 20, the server 12 forwards to the device 20 the following SMS message, seeking confirmation:

```
Please confirm $20 transfer to 0164452228 (Lee Eng
Sia) by calling 0320540301. This message expires
5:25pm 24/05.
```

Thus, the request for the validation instruction confirms the identifier for the recipient account for the transaction. By doing so, the risk of human error in instructing a transaction to a wrong account may be reduced.

In exemplary embodiments of the server 12, the server 12 invites a telephone call to be made from communications device 20 to a telephone number (0320540301 above) to provide the validation instruction 26. In exemplary embodiments, the server 12 employs a pool of several hundreds (or even thousands) of telephone numbers, and 0320540301 is selected from this pool. Exemplary embodiments of the server 12 are configured to select a different telephone number for different transactions. The selection may be random, or organised.

Exemplary embodiments of the server 12 allow for the telephone number to be called by device 20. It is not necessary for the telephone call to be connected; the server need only capture the caller identifier from the telephone call. Either the call may be disengaged the call after, say, two or three rings, or the server is configured to disengage the call once an ID of device 20 has been extracted from the call. From this, the ID may be determined, providing further enhanced security for the transaction. Thus, there is no requirement for incurring unnecessary cost in actually connecting the telephone call to provide the validation instruction.

Thus, in exemplary embodiments of the server 12, the transaction will only be effected by the server 12 if the call 26 from the second mobile communications device 20 is received before 5:25pm on 24th May. This gives a window of 10 minutes to instruct validation of the transaction and, thereby, to confirm payment.

If the sender makes a (missed) call to 0320540301 before the expiry time, the transaction proceeds and both the devices 18, 20 of the sender and the recipient are notified accordingly. Exemplary embodiments of the server 12 allow for this to made via a messaging service – e.g. SMS, MMS or equivalent – and, in the event of messaging service notification failure, a call can be made into a helpline IVR (Interactive Voice Response, not shown) where confirmation of the validation of the transaction is made by providing the last transaction from the e-wallet. Optionally, a call centre can easily handle such enquiries either by receiving a call from or placing a call to one or both of the communication devices 18, 20.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 675 of 1360

Thus, exemplary embodiments of the server may alleviate the problems associated with prior art e-wallet payment systems.

It will be appreciated that variations on this implementation for a transaction may be effected. For instance, the communications device 18 may be requested to transmit a validation instruction and/or receive confirmation of the payment. Communication with one or other of the devices 18, 20 may be over the Internet or, via GPRS, either of which are relatively reliable forms of communication. When the device 18 must send the validation instruction, further layers of security might be implemented to avoid situations where a device that erroneously receives the request for validation (i.e. the sender keys in a wrong number) can validate the transaction and receive payment. For example, the device 18 may be required to obtain a further authorisation code or the like from the device 20. The validation instruction may be required to include, for example, a PIN. Further security can be implemented in many ways.

Figure 2 illustrates the process flow for a transaction validated by the transaction server 12 of Figure 1.

The process starts at 50. At 52, a transaction instruction 22 is sent to the receiving module 13 of server 12 by SMS. At 54, this instruction 22 is received at the server 12 and, responsive to this, the transmission module 11 of server 12 sends a request 24 for a validation instruction 56. At 58, the server 12 waits for the validation instruction 26. If this is not received, the process may end simply at 66 or the process loops around waiting for the validation instruction 26 as indicated by dashed line 60. When/if it is determined at 58 that the validation instruction 26 is received at receiving module 13, the transaction is validated at 62 and, optionally, the server may effect the transaction at 64. The process ends at 66. As a further option, one or both of the communication devices 18, 20 are sent a confirmation message to confirm that the transaction has been validated and/or effected. Alternatively, the server can call either or both the devices 18, 20 to announce the transaction validation. To save unnecessary costs, the server 12 is optionally configured to disengage (hang up) the call even before the call is answered –

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 676 of 1360

a missed call in reverse. But it serves a simple purpose of letting the sender know the transaction has been validated and/or effected successfully.

In all SMS messages from the server to the devices 18, 20, additional information such as the e-wallet balance, and/or details of previous transactions, may be included.

The owner of the device with the telephone number 0164452228 may not have an authorised account. That is, the user of device 18 is not an existing e-wallet user. Thus, a new account needs to be created for the telephone number 0164452228. Indeed, this mobile number may not be valid because of human input error. In cases like this, the server 12 is configured to request that the (missed) call is made by the communication device 18, instead of the communication device 20. This ensures the mobile number 0164452228 is not keyed in wrongly by the sender for the message sent by SMS. The request for a validation instruction – e.g. an SMS seeking confirmation from the payer – would thus take the form:

```
Please confirm $20 transfer to 0164452228 (NEW USER)
by asking 0164452228 to missed call 0320540322. This
message expires 5:25pm 24/05.
```

The transaction is validated once the server receives a call from 0164452228 to 0325040322. Alternatively, the server 12 is configured for either the sender (payer) or the recipient (payee) to call the telephone number to validate the transaction – irrespective of whether the recipient is a new user or not.

This is an advantageous design feature and may be provided independently as will be discussed below.

Some mobile telephones have their caller ID barred or disabled. Thus, the server 12 is unable to capture the caller ID when such users place a call to provide the validation instruction. To overcome this, and for the creation of each new e-wallet, the number to call for the validation instruction (0320540322 in the above example) is allocated from

a special pool of pre-determined telephone numbers and the server is configured to activate only one number at any one time for one transaction. So when a call without caller ID is received by the server at 0320540322, the server is configured to recognise that this is a validation instruction for a particular transaction, and the fact that the new user (caller) has caller ID feature disabled in his phone is immaterial. Therefore, if the caller mobile has no caller-ID, then the transaction server can still validate one particular transaction based solely on the telephone number called. Generally, if caller-ID is available for caller identification, a single telephone number for validation can be used for validation of simultaneous/multiple transactions.

Further, embodiments of the server 12 are configured to effect all future transactions for this user in the same or similar way. Effectively, the server is configured to identify a category for this transaction in this way. That is, the server identifies that the category of the transaction is such that it is for payment to a particular recipient who does not have an authorised account.

This feature may also be particularly effective for, say, catalogue shopping. For a payer to make a payment to purchase an item from a catalogue, the payer is invited to call a particular number to purchase the item. By the very action of calling that number, the server identifies the category of the transaction (e.g. it is a purchase of a particular goods) and processes the transaction accordingly.

The server may also be configured to validate transactions for catalogue sales where each item in the catalogue is tagged with a product code. When a customer wants to purchase a product, they can enter a message into their mobile device for the device to send an SMS. The message contains the relevant product code. Once the server has received the SMS, a call must be made to confirm the purchase. Similarly, the same principle can be used for soft goods or services such as discounted call airtime, mobile phone airtime top-ups, and so forth.

The method described in the first embodiment above is particularly useful for paying merchants where the sender must know with certainty whether a transaction has been

effected. In certain less formal situations, a quicker payment method is often desirable; for example, when a user wishes to transfer money to, say, the user's sister. However, even in these situations, it is important that a method is in place to ensure the money transfer is not done wrongly.

In a second embodiment, a missed call mechanism is used to build a so-called "buddy list" for each user of e-wallet.

As before an SMS message is sent to the server requesting money transfer:

```
SEND 0164452228 20 753535
```

To initiate such transactions, a different instruction or keyword "SEND" is used to differentiate this from the example in the first embodiment although it will be appreciated that the first field of the transaction request may take a number of different forms.

To prevent the sender incorrectly entering the recipient's number (0164452228), the server checks to determine if 0164452228 is an authorised account. In embodiments of the server, a list of authorised accounts is maintained as a "buddy list". If indeed 0164452228 exists in this list, the $20 is transferred to the e-wallet of 0164452228. No further validation may be required. Thus, upon receipt of a transaction instruction for a transaction to an account for a recipient, responsive to determining that the account for the recipient is an authorised account, the server 12 automatically validates the transaction.

In situations where the recipient account is not an authorised account, once a validation instruction 26 for the transaction to the unauthorised account is received, the server is configured to flag the recipient account as an authorised account.

However if this is not the case, the server 12 sends a message to the payer:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 679 of 1360

```
0164452228 is not in your buddy list. To add
0164452228 to your buddy list, please ask 0164452228
to call 0320540202.
```

Once 0164452228 makes a (missed) call to 0320540202, the server 12 is configured to flag 0164452228 as being an authorised account for that payer; that is the recipient is added to the payer's "buddy list". The server also effects the transfer from e-wallet 16 to e-wallet 14 once the missed call is received.

Alternatively, the sender can also request 0164452228 to make a (missed) call to 0320540202 even before the sender sends his SMS, assuming 0320540202 has been advertised to him for this purpose. In such a case, the server 12 need not send the above SMS to the sender. Straightaway, 0164452228 shall be added to the sender's buddy list and the transfer can be made.

Embodiments of the server are configured to receive an instruction from a user to add a recipient account as an authorised account. This is particularly helpful in situations where the recipient 0164452228 has caller ID barred, the payer can still add 0164452228 to his buddy list by sending the following SMS to the server:

```
BUDDY 0164452228
```

When a recipient account is an authorised account for one user, embodiments of the server are configured to flag an account associated with the user as an authorised account for a recipient with whom the recipient account is associated. That is, the buddy list can be mutual; if user A is in user B's buddy list, then the server is configured to add user B to user A's buddy list automatically.

The process of the second embodiment is described with reference to Figure 3. The process starts at 100. At 102 communications device 20 sends a request for a transaction to a recipient (user at device 18) account. The server 12 determines whether the recipient account is an authorised account at 104 and upon determination the recipient

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 680 of 1360

account is authorised, the transaction is validated and, optionally, effected at 112. If determined at 104 that the recipient account is not an authorised account, the server 12 sends a request for a validation request. When this validation request has been received 108, the transaction is validated at step 112, subject to the transaction request meeting any requirements for validation. The process may loop around 108 with loop 110 while waiting for the validation transaction.

Optionally, when the transaction to the new (previously unauthorised) recipient account has been validated, the new account is flagged as an authorised account.

Embodiments of the server are configured to de-authorise an authorised account within a pre-determined time period from authorisation of the authorised account. That is, an expiry date is attached to each entry in the buddy list. This means that if a payer does not send money to a recipient before the expiry date, the recipient is removed from the payer's buddy list. The expiry date is renewed every time money is transferred to the recipient.

A further embodiment of the server seeks to address the problem that users are worried their mobile communication devices might be misused when their mobile phones double as a payment instrument.

Thus, embodiments of the server are configured to record receipt of an activation telephone call from a user and, upon recording receipt of the activation telephone call, to activate or deactivate an account for the user. Thus, it is possible for a user to LOCK/UNLOCK his/her account/e-wallet by allocating one or more telephone numbers for the user to call for this purpose.

Embodiments of the server are configured to select between activation and deactivation of the account in dependence of a status of the account. For example, when a user wants to lock his mobile account, the user places a (missed) call to 0320540000. Upon receipt of another call to this number, the server 12 checks the status of the account and, in dependence of this check, toggles the account status: if currently activated, the account

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 681 of 1360

is de-activated and *vice versa*. Alternatively, the user is provided with two telephone numbers: one to lock the account and one to unlock it.

In some embodiments of the server, the server calls the user back through an IVR to prompt him to enter a PIN or UNLOCK code.

If embodiments of the server detect a call to a wrong number 0320540002, the server is configured to disable the mobile payment account associated with that mobile phone. This is to prevent fraud. For example, the server is configured to select from a pool of hundreds or thousands of telephone numbers. For each user the server allocates a different number for LOCKING and UNLOCKING of the account. So, an unauthorized user obtaining an authorised users mobile communications device 18 would not know which number to call to UNLOCK the e-wallet account. Guessing a wrong number from the designated pool will be an indication for the server to lock the e-wallet account.

Figure 4 illustrates a schematic view of the basic structure of an e-wallet system 100 as disclosed in, for example, International Patent Publication No. WO 2006/049582 filed by the present Applicant(s) and hereby incorporated by reference as if disclosed herein in its entirety. The e-wallet system 100 has two sides: a bank sub-system 102 including a bank database 104 and an e-wallet sub-system 202 including an e-wallet database 204.

The bank database 104 has typical banking facilities, including a number of user savings and current accounts, exemplified in Figure 4 by way of a user 1 current account 106, a user 2 current account 108 and a user N-1 current account 110. The bank database 102 also includes a number of user credit accounts, exemplified in Figure 4 by way of a user 1 credit account 112, a user 2 credit account 114, a user N-1 credit account 116 and a user N credit account 118. The user credit accounts contain what may be described as electronic money, but which is generally referred to herein as funds. The user credit accounts may be associated with the respective user current and/or savings accounts, but need not necessarily be. In Figure 4, the user N credit account 118 is not associated with any other bank account.

Additionally, the bank database 104 includes a consolidated e-wallet bank account 120. There is also an e-wallet sub-system credit account 122 and associated e-wallet sub-system current account 124, for the company running the e-wallet system to add money to and withdraw money from the consolidated e-wallet bank account 120. These are operable in similar ways to the user credit and current accounts.

The e-wallet database 204 has a number of user e-wallets 212, 214, 216, 218, one for each user credit account 112, 114, 116, 118 in the bank database 104. Thus, there is a user 1 e-wallet 212, a user 2 e-wallet 214, a user N-1 e-wallet 216 and a user N e-wallet 218. Additionally, the e-wallet database 204 contains an escrow e-wallet 226 and a transaction charges e-wallet 228. Within the e-wallet database 204, the user N e-wallet 118 is treated no differently from the other e-wallets, even though, in the bank sub-system 102, the user N has no bank account other than the user N credit account 118.

Alternatively, in one e-wallet implementation, there is no necessity for an e-wallet account to be associated with any bank account. In this way, large sections of the population of a country who either do not have or seldom use bank accounts – low income workers, foreign workers, inhabitants of rural areas having no banking facilities etc. – may utilise the transaction system. Bank links are there to provide a convenient mechanism to top up their e-wallets. The banks can also act as intermediaries to top up e-wallets for other individuals.

The system of the present server is further enhanced where the user can easily transfer money received in the user's e-wallet to any of the user's bank accounts. Furthermore, by working with selected banks, the user can transfer money automatically from the user's existing bank accounts into the user's e-wallet. All it takes is a simple initial registration of the user's mobile phone number at ATMs of participating banks.

It will be appreciated the invention has been described by way of example only and that various departures in detailed design may be made without departing from the scope of the invention. It will be further appreciated that features presented in association with

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 683 of 1360

one embodiment of the invention may be provided in combination with another embodiment of the invention.

5

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 684 of 1360

THE CLAIMS

1. A transaction server comprising:

a receiver module configured to receive an instruction message from a first mobile communications device for a transaction from a first account to a second account;

a transmission module configured to send a response message to the first mobile communications device a request for a validation instruction for the transaction, the response message being in response to the receipt of the instruction message;

the server being configured to record receipt of the validation instruction; and

the server being configured to record receipt of the validation instruction and, in response thereto, validate and effect the transaction.

2. The transaction server of claim 1, wherein the server is configured to validate and effect the transaction if receipt of the validation instruction is recorded by the server within a pre-determined period from sending the response message.

3. The transaction server of claim 1 or claim 2, wherein the server is configured to send a confirmation message to the first mobile communications device to confirm the transaction has been validated and effected.

4. The transaction server of any preceding claim, wherein the instruction message comprises at least one selected from the group consisting of: an identifier of the second account, a value for the transaction, and an authentication code for the transaction.

5. The transaction server of claim 4, wherein the response message comprises a request for a confirmation of at least one of: the identifier of the second account, and the value for the transaction.

6. The transaction server of any preceding claim, wherein the server is configured to capture an identifier of the first mobile communications device from the validation instruction.

7. The transaction server of any preceding claim, wherein the server is configured to select a telephone number from a pool of pre-determined telephone numbers; the response message comprising the telephone number.

8. The transaction server of any preceding claim, wherein the validation instruction is by a confirmation call between the first mobile communications device and a communications module of the server; the confirmation call being initiated by one of: the communications module of the server, and the first mobile communications device.

9. The transaction server as claimed in claim 8 when dependent on claim 7, wherein the confirmation call is by the first mobile communications device to the communications module using the telephone number.

10. The transaction server of claim 9, wherein the communications module is configured to disengage the confirmation call.

11. The transaction server of claim 10, wherein the communications module is configured to disengage the confirmation call after identifying the first mobile communications device.

12. The transaction server of any preceding claim, wherein the server is configured to identify a category for the transaction from the validation instruction.

13. The transaction server of any preceding claim, wherein the server is configured to determine whether the second account is an authorised account, and to send the response message responsive to a determination the second account is not an authorised account.

14. A transaction server comprising:

a receiver module configured to receive an instruction message from a first mobile communications device for a transaction from a first account to a second account;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 686 of 1360

the server being configured to determine whether the second account is an authorised account; and

responsive to a determination that the recipient account is an authorised account, validate the transaction.

15. The transaction server of claim 13 or claim 14, wherein the transmission module is configured to send the response message to a second mobile communications device associated with the second account.

16. The transaction server of claim 15, wherein the server is configured to, upon receipt of the validation instruction from the second mobile communications device, flag the second account as an authorised account.

17. The transaction server of any preceding claim, wherein the server is configured to receive an instruction from the first mobile communications device to add the second account as an authorised account.

18. The transaction server of any preceding claim, wherein the server is configured to de-authorise an authorised account a pre-determined time after authorisation of the authorised account.

19. The transaction server of any preceding claim, wherein the server is configured to record receipt of an activation telephone call from a user to the server and, upon recording receipt of the activation telephone call, to activate or deactivate the user account.

20. A transaction server for effecting a transaction from a user account, the server being configured to record receipt of an activation telephone call from a user to the server and, upon recording receipt of the activation telephone call, to activate or deactivate the user account

21. The transaction server of claim 19 or claim 20, wherein the server is configured to select between activation and deactivation of the account in dependence of a status of the account.

22. The transaction server of any of claims 19 to 21, the server being configured to place a telephone call to the user to prompt the user to validate activation or deactivation of the account.

23. A method of validating a transaction comprising:

a server receiving from a first mobile communications device an instruction message for a transaction from a first account to a second account;

responsive to receipt of the instruction message, the server sending a response message to the first mobile communications device, the response message comprising a request for a validation instruction;

the server receiving and recording receipt of the validation instruction; and

responsive to recording receipt of the validation instruction, the server validating and effecting the transaction.

24. The method of claim 23, further comprising validating the transaction if receipt of the validation instruction is recorded within a pre-determined period from sending the response message.

25. The method of claim 23 or claim 24, further comprising sending a confirmation message to the first mobile communications device to confirm the transaction has been validated and effected.

26. The method of any one of claims 23 to 25, wherein the instruction message comprises at least one selected from the group consisting of: an identifier of the second account, a value for the transaction, and an authentication code for the transaction.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 688 of 1360

27. The method of claim 26, wherein the response message comprises a request for a confirmation of at least one of: the identifier of the second account, and the value for the transaction.

28. The method of any one of claims 23 to 27, wherein the server captures an identifier of the first mobile communications device from the validation instruction.

29. The method of any one of claims 23 to 28, wherein the server selects a telephone number from a pool of pre-determined telephone numbers; the response message comprising the telephone number.

30. The method of any one of claims 23 to 29, wherein the validation instruction is by a confirmation call between the first mobile communications device and a communications module of the server; the confirmation call being initiated by one of: the communications module of the server, and the first mobile communications device.

31. The method as claimed in claim 30 when dependent on claim 29, wherein the confirmation call is by the first mobile communications device to the communications module using the telephone number.

32. The method of claim 30 or claim 31, wherein the communications module disengages the confirmation call.

33. The method of claim 32, wherein the communications module disengages the confirmation call after identifying the first mobile communications device.

34. The method of any one of claims 23 to 33, wherein the server identifies a category for the transaction from the validation instruction.

35. The method of any one of claims 23 to 34, wherein the server determines whether the second account is an authorised account, and sends the response message responsive to a determination the second account is not an authorised account.

36. A method comprising:

a receiver module of a server receiving an instruction message from a first mobile communications device for a transaction from a first account to a second account;

the server determining whether the second account is an authorised account; and

responsive to a determination that the recipient account is an authorised account, validating the transaction.

37. The method of claim 36, wherein a transmission module of the server sends a response message in response to the receipt of the instruction message.

38. The method of claim 35 or claim 37, wherein the response message is sent to a second mobile communications device associated with the second account.

39. The method of claim 38, wherein upon receipt of the validation instruction from the second mobile communications device, the server flags the second account as an authorised account.

40. The method of any one of claims 23 to 39, wherein the server receive an instruction from the first mobile communications device to add the second account as an authorised account.

41. The method of any one of claims 23 to 40, wherein the server de-authorises an authorised account a pre-determined time after authorisation of the authorised account.

42. The method of any one of claims 23 to 41, wherein the server records receipt of an activation telephone call from a user to the server and, upon recording receipt of the activation telephone call, activates or deactivates the user account.

43. A method for activating or deactivating a user account, the method comprising a server receiving and record receipt of an activation telephone call from the user directly

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 690 of 1360

to the server and, upon recording receipt of the activation telephone call, activating or deactivating the user account

44. The method of claim 42 or claim 43, wherein the server selects between activation and deactivation of the account in dependence of a status of the account.

45. The method of any one of claims 42 to 44, wherein the server makes a telephone call to the user to prompt the user to validate activation or deactivation of the account. for the transaction from the validation instruction.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 691 of 1360

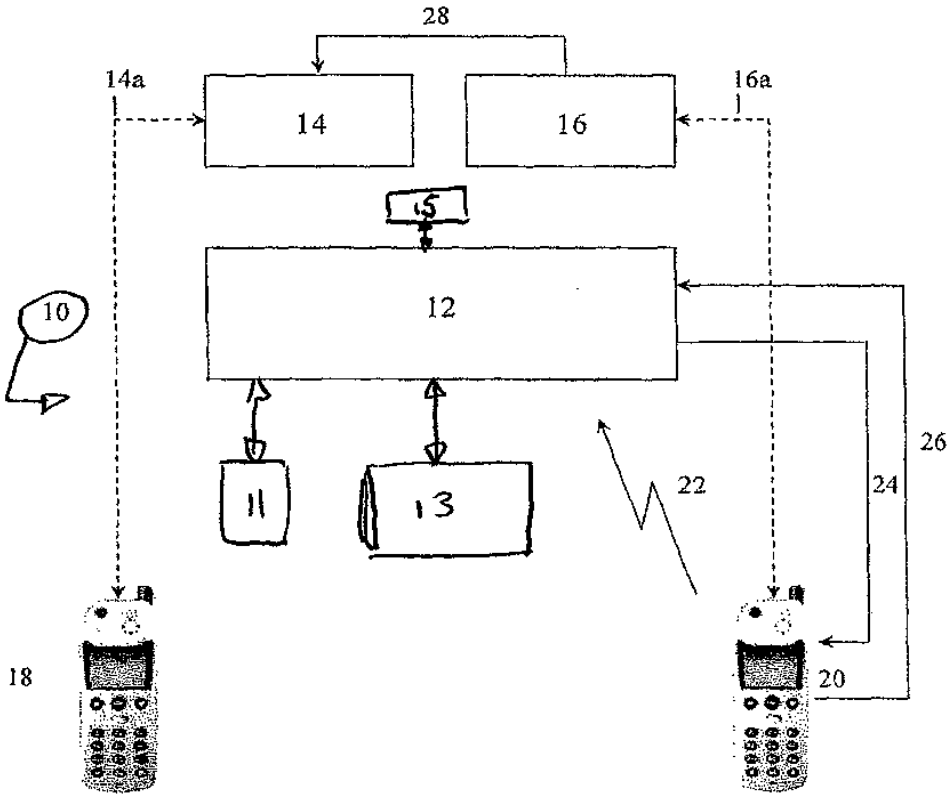


FIG. 1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 692 of 1360

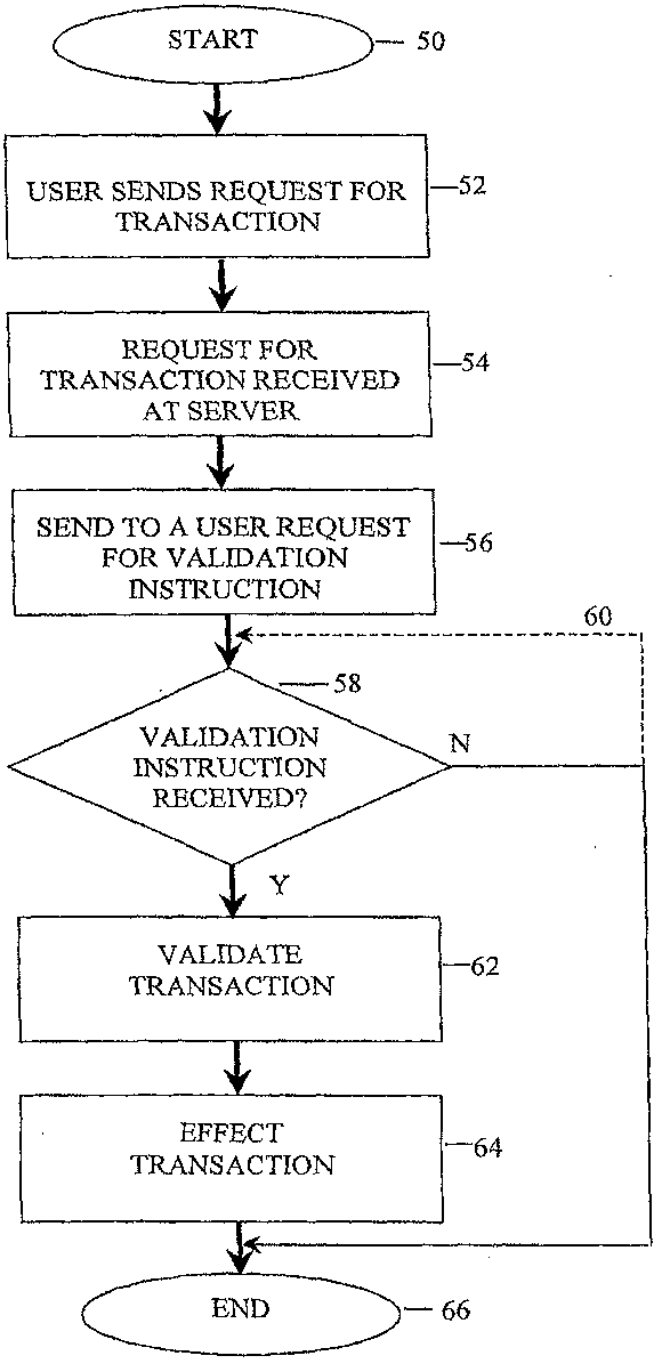

START
50
USER SENDS REQUEST FOR TRANSACTION
52
REQUEST FOR TRANSACTION RECEIVED AT SERVER
54
SEND TO A USER REQUEST FOR VALIDATION INSTRUCTION
56
60
58
VALIDATION INSTRUCTION RECEIVED?
N
Y
VALIDATE TRANSACTION
62
EFFECT TRANSACTION
64
END
66

FIG. 2

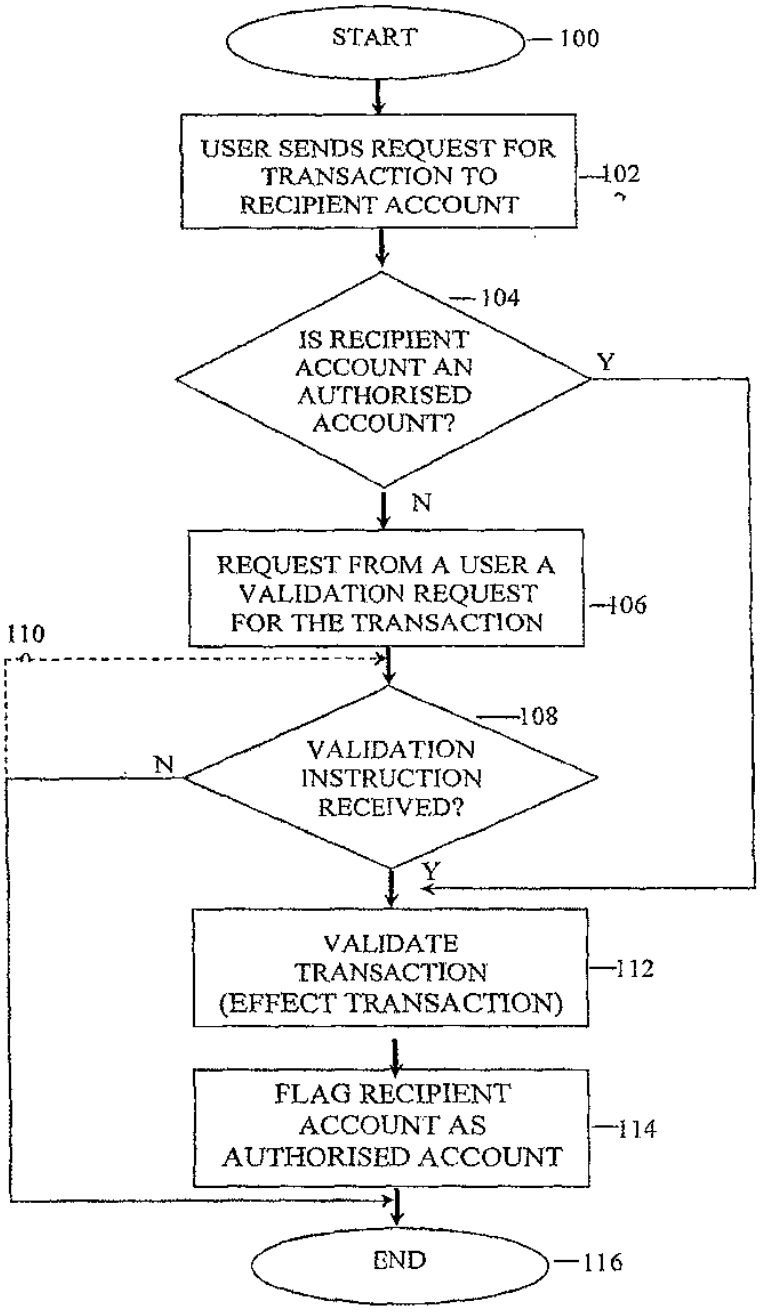


FIG. 3

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 694 of 1360

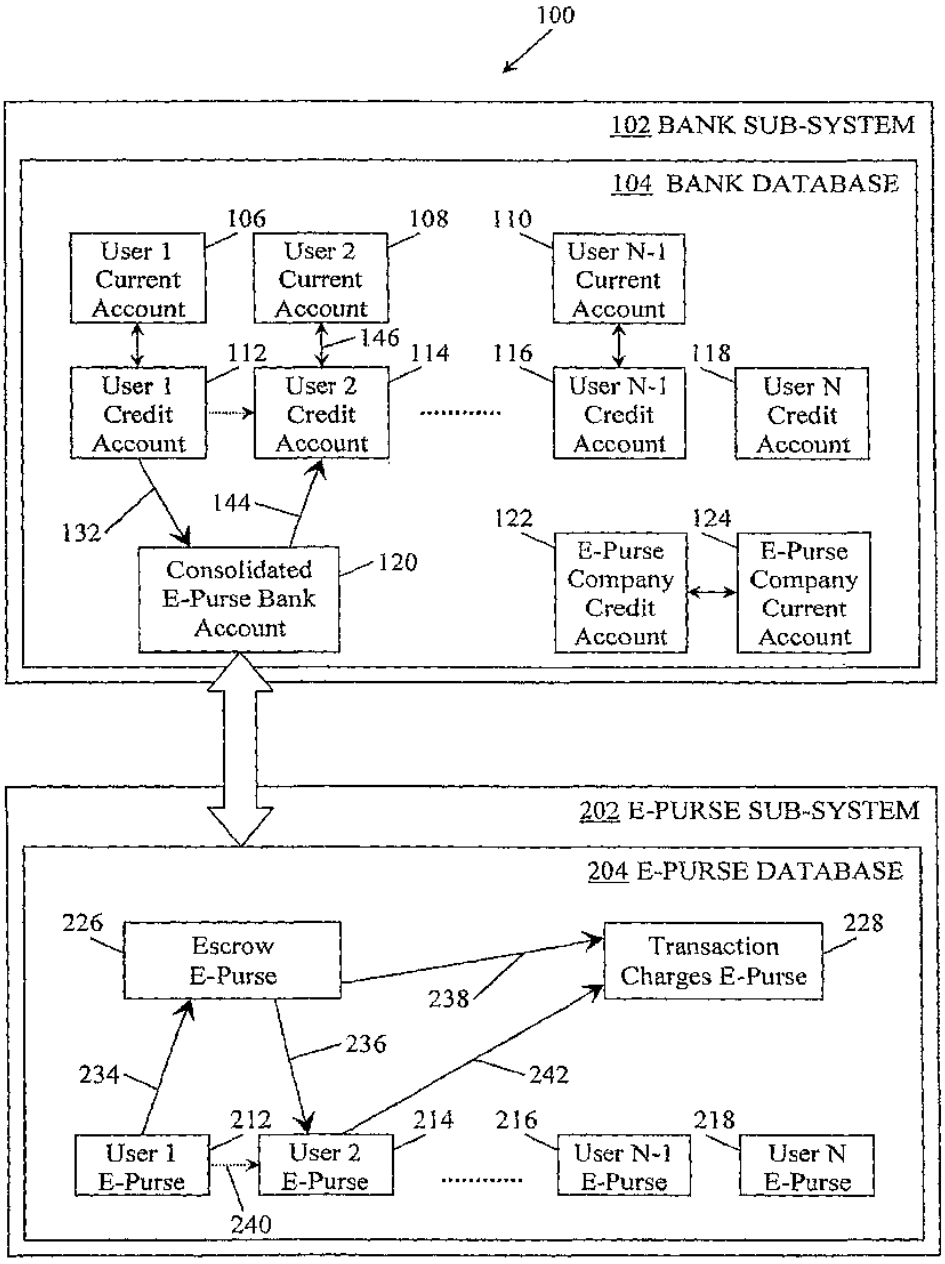

100
102 BANK SUB-SYSTEM
104 BANK DATABASE
106
108
110
User 1 Current Account
User 2 Current Account
User N-1 Current Account
146
112
114
116
118
User 1 Credit Account
User 2 Credit Account
User N-1 Credit Account
User N Credit Account
144
132
122
124
Consolidated E-Purse Bank Account
120
E-Purse Company Credit Account
E-Purse Company Current Account
202 E-PURSE SUB-SYSTEM
204 E-PURSE DATABASE
226
228
Escrow E-Purse
Transaction Charges E-Purse
238
236
234
242
212
214
216
218
User 1 E-Purse
User 2 E-Purse
User N-1 E-Purse
User N E-Purse
240

Figure 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2007/000038

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. ***G07F 19/00*** (2006.01) ***G06Q 20/00*** (2006.01) ***H04M 17/00*** (2006.01)
G06Q 10/00 (2006.01) ***H04M 15/00*** (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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)
WPI + keywords (call, mobile, activate, account, transaction, validate and similar terms)
USPTO + keywords (transaction, mobile, validate and similar terms)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6868391 B1 (HULTGREN) 15 March 2005 Abstract, column 1 line 55 to column 2 line 13, column 3 line 38 to column 9 line 47, figures 1 to 3c.	1 to 45
A	US 2002/0181710 A1 (ADAM et al) 5 December 2002 Whole document	
A	US 2003/0200184 A1 (DOMINGUEZ et al) 23 October 2003 Whole document	
A	WO 2004/079676 A1 (FORTUNATUS HOLDINGS LIMITED) 16 September 2004 Whole document	

☐ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier 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
10 September 2007	20 SEP 2007
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **DEREK BARNES** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : (02) 6283 2198

Form PCT/ISA/210 (second sheet) (April 2007)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/MY2007/000038

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	6868391	AU	70943/98	BR	9808534	CA	2286778
		CN	1260895	EP	0976116	NO	995031
		WO	1998/047116				
US	2002/0181710	AU	32189/01	EP	1221081	IL	134741
		WO	2001/063375				
US	2003/0200184	AU	2003228574	CA	2482558	EP	1497947
		WO	2003/090027				
WO	2004/079676	EP	1604339	GB	2399209		

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 697 of 1360

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **H04M 17/00, H04Q 7/32** | **A1**

(11) International Publication Number: **WO 99/13636**

(43) International Publication Date: 18 March 1999 (18.03.99)

(21) International Application Number: PCT/GB98/02729

(22) International Filing Date: 10 September 1998 (10.09.98)

(30) Priority Data:
9719100.1 10 September 1997 (10.09.97) GB

(71) Applicant *(for all designated States except US)*: TEKTON COMMUNICATIONS LIMITED [GB/GB]; Marsh House, 500 Montagu Road, London N9 0UR (GB).

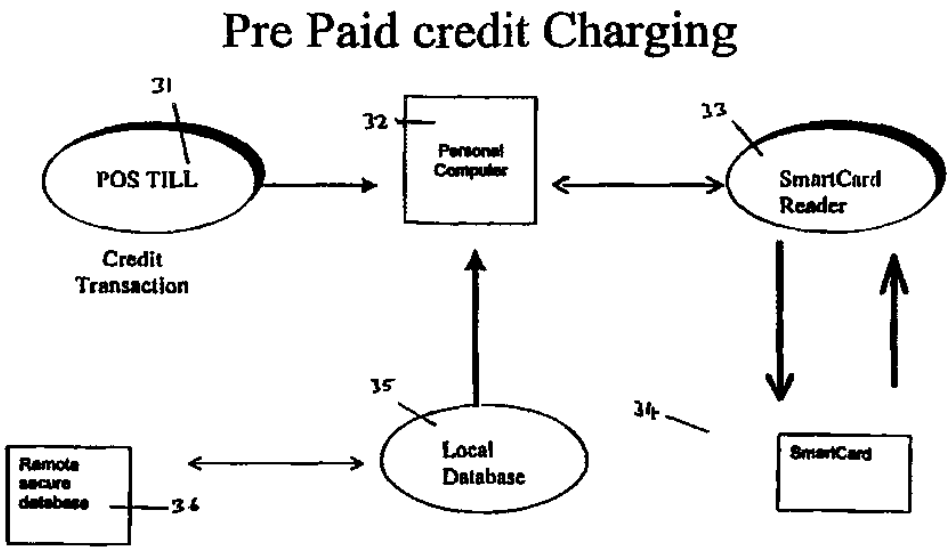
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BISWELL, Anthony, James [GB/FR]; Villa Mas Souleou, Boulevard Plan des Abeilles, F–06230 Saint Jean Cap Ferrat (FR). CASTLE, Derek, Keith [GB/GB]; 4 Tavern Road, Wooley Bridge, Glossop, Derbyshire SK13 2RB (GB).

(74) Agent: COATES, Ian, Harold; Sommerville & Rushton, 45 Grosvenor Road, St. Albans, Herts AL1 3AW (GB).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) **Title:** A PRE–PAYABLE COMMUNICATION DEVICE



(57) **Abstract**

A portable radio communications apparatus comprising: (i) a portable handset; (ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit; (iii) a recess in the handset adapted to accept the removable module; (iv) a reading device in the handset adapted to determine a content of the electronic purse; (v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse; and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 698 of 1360

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A Pre-payable Communication Device

Field of Invention

The present invention relates to pre-payable communication devices and more particularly to pre-payable communication devices which are suitable for use in radio communication networks.

Background to the invention

One problem with radio communication devices such as mobile telephones is that they are relatively expensive both to purchase and to run. This represents a problem both for the subscriber and for the service provider. For example, the service provider needs to rely on the creditworthiness of the mobile phone subscriber and both the service provider and the subscriber are at risk from fraudulent use of the subscriber's terminal. Many people who would otherwise benefit from the occasional use of a mobile phone are prevented from having this benefit because either the cost is too high and/or the service provider is unable to rely on their creditworthiness. For occasional users the monthly line rental charge is often prohibitively expensive.

There are many situations in which the use of conventional mobile telephones is problematic. For example, an employee may be given a mobile telephone by his employer to use only in essential circumstances. The employer would like to ensure that the employee does not run up additional costs by using the phone for personal use. However, this is difficult to do until after the event when the employer is able to check the telephone bill.

Another problem relates to the fact that in different geographic locations, different communication protocol systems are in operation. An example of a protocol system is Global system for Mobile Communications (GSM) which is a European protocol system. Typically, mobile telephone handsets are operable with only one, or perhaps two different communication protocol systems. This means that when the user

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 700 of 1360

moves to a different geographical area, he may be unable to operate his mobile telephone, if the communication protocol system for that area is incompatible with his handset. This is often a problem for travellers and yet travellers often only have access to mobile communications devices and need them most when they are on the move.

Some attempts have been made to overcome these problems using SmartCard technology. A conventional SmartCard is typically a rectangular piece of plastics material, of a similar size and shape to a credit card, which contains integrated circuits, microprocessors and/or read write memory. The use of SmartCards in radio telephones is known, for example, as described in UK patent application number 2267794 in the name of Alan Kilpatrick Conroy. This application describes a pre-payable mobile cellular phone. However, the specification gives no details on how the pre-payment is achieved.

UK Patent 2266798 in the name of Motorola Inc. describes an apparatus for accepting, retaining and making electrical contact between a SmartCard and a radio telephone handset. The SmartCards used in radio telephones have been limited to subscriber identification module (SIM) cards for use in the European market. SIM cards are available in two sizes; a full size card and a chip card. SIM cards for GSM currently provide subscriber information (e.g. subscriber phone number, service provider) and plug into a GSM compatible mobile telephone handset to configure that handset for a particular subscriber. These cards only reference the subscriber data and do not include radio frequency circuitry or protocol information. If the SIM card is removed from the handset incoming calls cannot be received.

International patent application number WO/97/05729 in the name of Telecom Italia Mobile S. P. A. describes a radio mobile terminal that is provided with two SIM card readers. One of the SIM cards is described as a prepaid card and this can be loaded into the additional reader. This system is disadvantageous because the mobile

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 701 of 1360

telephone handset needs to contain two SIM card readers which increases the cost and bulk of the terminal. Also the design of the handset is complex because two SIM card readers must be allowed for.

None of the above prior art provides either communications equipment or a method of operation which enables every would-be subscriber, regardless of creditworthiness to have access to a mobile phone on a pay-as-you-use basis.

It is accordingly an object of the present invention to provide a pre-payable communication device for use with radio communication networks and a method of using such equipment which overcomes or at least mitigates one or more of the problems noted above.

Summary of invention

According to the present invention, there is provided a portable radio communications apparatus comprising:

(i) a portable handset;

(ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit;

(iii) a recess in the handset adapted to accept the removable module;

(iv) a reading device in the handset adapted to determine a content of the electronic purse;

(v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse;

and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed. This gives the advantage that every would-be subscriber, regardless of creditworthiness can have access to a mobile phone on a pay-as-you-use basis. When the module is removed from the device, the communications apparatus is inoperable which helps to prevent fraud. The subscriber

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 702 of 1360

identification unit in the removable module provides "identification" for a particular subscriber, so that one subscriber can use several different handsets and configure these for his own use simply by adding the removable module. This helps subscribers when they travel between areas covered by different protocol systems. Such a traveller would be able to retain his or her removable module and simply insert this into a different handset that is operable with the new protocol system.

Preferably, the removable module comprises a SmartCard. This provides the advantage that the removable module is conveniently sized and shaped and can easily be stored and transported.

In one embodiment of the invention the subscriber identification unit comprises a conventional subscriber identification module. This provides the advantage that the subscriber identification unit can easily be obtained and is compatible with other known systems. Preferably the subscriber identification unit is adapted to be compatible with the Global System for Mobile Communications Protocol. This enables the communications apparatus to be used with a widely used European protocol system.

According to another aspect of the present invention there is provided a removable module suitable for use with a portable radio communications handset said module comprising an electronic purse and a subscriber identification unit, said module being adapted to be received in a recess in said handset, and wherein said module is adapted such that in use the handset is substantially inoperable when the module is removed from the communications apparatus. This provides the advantage that removable modules are provided which contain an electronic purse. Would-be subscribers can obtain a removable module, regardless of their creditworthiness, and use this to gain access to a mobile phone on a pay-as-you-use basis.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 703 of 1360

According to another aspect of the present invention there is provided a method of communicating using a portable radio communications apparatus said method comprising the steps of :

(i) purchasing air time from an air time provider or suitable intermediary;

(ii) charging said electronic purse with units equivalent to purchased air time;

(iii) inserting the removable module incorporating the electronic purse into the recess in the handset;

(iv) determining a content of the electronic purse;

(v) allowing substantial operation of the communications apparatus on the basis of the content of the electronic purse;

(vi) operating the communications apparatus and updating the content of the electronic purse on the basis of said operation. This provides the advantage that a service provider or air-time provider no longer needs to be responsible for the creditworthiness of all its subscribers. Individual subscribers may purchase air-time units using cash and "charge" a removable module in this way. The "charged" module can then be used to communicate using the mobile phone handset. The subscriber is then able to use the handset on a pay-as-you-use basis.

The present invention is intended to encompass both the removable module and the handset together and individually. The invention also encompasses a method for using the removable module and handset as well as a charging station for charging the removable module.

Description of the drawings

The invention will be further described, by way of example, with reference to the accompanying drawings in which:

Figure 1 is a flow diagram indicating a method of using the prepayable portable radio communications apparatus.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 704 of 1360

Figure 2 is a schematic diagram of a handset and removable module.

Figure 3 is a flow diagram showing a method of recharging a removable module.

Figure 4 is a flow diagram of actions and screen messages in a method of recharging a removable module.

Figure 5 is a flow diagram of actions and screen messages in a method of initialising a removable module.

Figure 6 is a schematic diagram of an external fraud detection system.

Figure 7 is a schematic diagram of an alternative external fraud detection system.

Description of preferred embodiments

Embodiments of the present invention are described below by way of example only. These examples represent the best ways of putting the invention into practice that are currently known to the Applicant although they are not the only ways in which this could be achieved.

Figure 2 is a schematic diagram of a portable radio communications apparatus 20 comprising a portable handset 21 and a removable module 22. The portable handset is shown as being similar to a conventional mobile telephone handset although any suitable type of handset may be used. In the example shown the handset comprises a display area 23, an aerial 24, a key pad 25 and a recess 26. The recess 26 is adapted to receive the removable module 22 as shown in figure 2. The handset may also comprise a microphone and a loudspeaker (not shown) as well as other elements typically contained in a conventional radio telephone handset. However, in one embodiment of the present invention, some components that would typically be contained in a conventional radio telephone handset are removed from the handset 21 and replaced by equivalent or alternative devices and circuitry in the removable module. This is explained further below.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 705 of 1360

The removable module 22 is shown as being generally rectangular in shape although any shape can be used. Preferably the removable module is a SmartCard and has a shape similar to that of a conventional credit card. The removable module comprises an electronic purse. The term "electronic purse" is used to refer to any form of memory that is capable of being read and updated, and which is capable of storing information about units of "air-time". Preferably, the electronic purse is rechargeable, that is once the units of "air time" that it contains have been used up, they can be replaced. However, this is not essential. The removable modules can be disposable, so that once the units are used up the module is simply replaced. Units of "air-time" are units of time for which a communications service is provided by a communications network service provider. The removable module 22 can be inserted into and removed from the recess 26 in the handset.

The removable module 22 also comprises a subscriber identification unit (not shown) which is preferably a conventional subscriber identification module (SIM). For example, the removable module 22 can be a SIM card which further comprises an electronic purse. When the removable module 22 is removed from the handset the SIM is also removed and this means that the communications apparatus 20 cannot be used to transmit or receive information. When the SIM is removed from the apparatus 20 there is no information in the handset about which subscriber is using the apparatus, for example, the user's telephone number. This means that the communications apparatus is substantially inoperable when the module is removed.

Figure 1 is a flow diagram indicating a method of using the prepayable portable radio communications apparatus. This represents one example of a method for using the prepayable portable radio communications apparatus; other methods may also be used. The user first obtains a removable module 22 and inserts this into the handset 22 and then a card validity check process 1 is carried out. The card validity check process

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 706 of 1360

involves checking whether the removable module is in anyway "data corrupt" or is not in credit. The handset contains a reading device adapted to determine a content of the electronic purse and also an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse. At this stage it is also possible for the subscriber to key in a personal identification number (PIN) to the key pad of the handset in order to allow use of the removable module. This provides extra security for the subscriber because it prevents unauthorised use of the removable module and/or the handset. However, use of a PIN number in this way is optional.

The next stage 2 involves a network authentication check by the airtime provider. This involves a check of the information provided in the subscriber identification unit or SIM (if a SIM is used). By making this check the service provider can help to prevent use of fraudulent removable modules. If the result of stage 2 is a "fail" i.e. the check is unsuccessful for any reason then the communications apparatus is not enabled as shown in box 3 in figure 1. That is, the enabling means prevents use of the communications apparatus. A warning message and instructions to the subscriber can be displayed on the display panel to indicate that access to the communications network by the service provider has not been granted.

If the result of stage 2 is successful then full functionality and dial facilities are granted by the service provider as indicated in box 4 of figure 1. The subscriber is then able to use the portable radio communications apparatus and as information is transmitted or received from the apparatus (indicated by box 7 in figure 1) the electronic purse is updated (as indicated by arrow 10 in figure 1). For example, as units of "air time" are used by the subscriber these are decremented from the electronic purse contents. Once the reading device determines that the electronic purse is empty the result of the airtime credit box 5 is a "fail" and the user is advised (box 6) and the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 707 of 1360

enabling device prevents use of the communications apparatus. At this point the user may remove the removable module from the handset and use a charging station to recharge the module. That is, the user may purchase more "air-time" units and store these in the electronic purse on the removable module.

This method provides the advantage that the service provider is not responsible for the creditworthiness of the subscriber. Also, the subscriber is able to use a mobile phone on a pay-as-you-use basis and is fully in control of his or her expenditure at any one time. It is not necessary for the whole mobile telephone to be configured for use specifically by one subscriber i.e. the telephone does not have to be configured for one telephone number. This is because the telephone number effectively "travels with" the subscriber within his removable module. When the subscriber moves between geographical regions over which different communications protocols are used the subscriber can simply obtain a new handset, that is preconfigured for the protocol of that area, and insert his removable module into the handset in order to configure that handset for his own personal use. For example, travellers could hire a telephone handset when they enter a new area.

The charging station comprises a recess which is able to accept a removable module and also means for entering "air-time" units onto the electronic purse on the module.

As described above, in one embodiment of the invention, some of the functionality from the handset is removed and placed onto the removable module. That is, the handset will typically contain electronic apparatus which will enable the handset to function as a radio communications apparatus when the electronic purse is "charged" and the subscriber identification unit is provided. This means that the handset is hugely more expensive relative to the removable module. However, in one embodiment of the invention, some of the functionality from the handset is removed and instead

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 708 of 1360

incorporated into the removable module or SmartCard. This increases the value of the removable module relative to the handset and may also ensure that the handset will not function without the removable module. Examples of functions that could be removed from the handset include the enabling means, the reading device and other features such as circuitry for converting the speech signal from the user into digital form. These are only examples of functions that could be incorporated into the removable module. Other functions could also be incorporated by making use of conventional circuit design techniques such as would be know to the skilled person in the art.

By making the removable module more expensive with respect to the handset itself, the risk of theft of the handset is reduced and the consequences of theft of the handset are less severe.

In one example, the present invention is made available as an integral component of a customer loyalty programme. The pre-pay mobile telephone is made available to loyalty card holders as an extension of any existing loyalty scheme, on the basis of reward for tenure and spend within the loyalty scheme. Users are able to earn loyalty points on airtime and also to redeem loyalty points against purchase of airtime.

In this example of the invention, the SmartCard for use with the pre-pay mobile telephone handset is also functional as a customer loyalty card. The SmartCard contains an amount of airtime included at the time of purchase and subsequent recharging of the card is possible upon each visit to the loyalty scheme provider's premises.

A number of advantages are provided to the loyalty scheme provider including:

- provision of an "added value" service to existing customers
- ability to attract new customers
- broad customer availability - no credit rating checks
- rechargeable only at loyalty scheme provider's retail outlet

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 709 of 1360

- minimal overheads and capital expenditure
- use of airtime derives gross revenues prior to month end settlement
- information about customers behaviour patterns is gained

Recharging the removable module

Figures 3 and 4 are flow diagrams which illustrate the process of recharging the removable module or SmartCard. When the user needs to recharge his or her SmartCard 34 he or she visits the loyalty provider's premises and at a point of sale till 31 carries out a credit transaction 41, 42 to pay for airtime units to be charged onto the SmartCard 34. After removal from the handset 43 the SmartCard 34 is then inserted 44, 45 into a SmartCard reader 33 that is connected to or integral with a secure personal computer 32. The personal computer 32 is connected to a local database 35 which contains information about the user's loyalty card and SmartCard 34. The local database 35 is in turn connected to a remote secure database 36.

A message 46 is displayed on the screen of the personal computer 32 which indicates the amount of pre-paid air time units that remain on the SmartCard 34. The amount of air time units that are to be credited to the card 34 is then entered onto the personal computer 46 and the personal computer updates the electronic purse in the SmartCard 34 accordingly using an encrypted transaction. The amount of units to be credited to the card can either be entered manually or can be transferred electronically from the till 31 to the computer. The updated amount of pre-paid air time units on the SmartCard 34 is displayed on the computer screen 47 and the SmartCard 34 is then returned to the user or customer 47. Finally the handset is returned to the customer 48. The encrypted transaction involves the following steps:

1. The secure personal computer obtains secret data that is specific to the SmartCard from the SmartCard itself and/or the local and remote databases and builds an encrypted update command.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 710 of 1360

2. The software within the card deciphers the encrypted command and updates the airtime counter or electronic purse within the SmartCard.

Such an encrypted transaction is recorded by the personal computer and when a batch of such records are obtained this batch is sent to the remote secure database 36 for storage and to update that database.

Initialising the removable module

Each SmartCard contains secure key information which is stored on the card during the manufacturing process. Information about these secure keys is held on the main database 36 and is accessible by the local database 35.

When a user first obtains a removable module or SmartCard 34 this is initialised by placing the SmartCard 34 into the card reader 33. Information from the card 34 which identifies the card and provides security information (i.e. the secure key) is read by the card reader 33 and checked by the personal computer 32 using information from the local and/or remote databases 35, 36.

If this check is successful the card if authenticated 55 and a screen message asking for loyalty card details to be entered is displayed 55. The loyalty card details are entered 52 to the personal computer 32 and then the card is initialised by the personal computer 53. Details linking the loyalty card details and the secure key are stored on the local and/or remote database 35, 36 and an initial amount of airtime credit is charged to the card. The card is then removed from the reader and returned to the customer 57 in order to be inserted into the customer handset 54.

External fraud detection system

A fraud detection system is provided that is external to the handset and removable module. This is provided in addition to any fraud detection system provided by the network operator. This system monitors traffic made on the pre-paid mobile telephone network and compares this traffic against information about recharging of

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 711 of 1360

SmartCards on the system. For a particular SmartCard, if more traffic is being created than is justified by the amount of credit on that SmartCard then possible fraud is identified. After checks have been made, if it is found that fraud is occurring then the SmartCard is prevented from accessing the network.

Figures 6 and 7 show two examples of an external fraud detection system. Pre-paid mobile phone handsets 62 are used to communicate over an operator or service provider's communications network 61. Each time a call is made a call detail record (CDR) is created and stored by the operator 61, as is known in the art. A call detail record contains information about the calling party, the called party, the duration of the call, the time when the call was made and other information about the call. At the end of a certain period of time, for example 12 hours, the call detail records for that 12 hour period are downloaded to database 66,71 in the fraud management system.

A SmartCard reader 64 or other removable module reader is provided that is connected to a till 63 such that the card reader 64 and till 63 are uniquely matched for security reasons. When a SmartCard or removable module is recharged using the card reader 64 and till or PC 63 information about the recharge is downloaded to a database 65, 71 in the fraud management system. Information about new users from the card initialisation process can also be downloaded. The information can be stored within the local database 35 before being downloaded in batches.

In the example shown in figure 6 the fraud detection system comprises two separate databases 65 and 66. One database 66 stores the call detail records and the other 65 stores information about credit data and new users. The information from these two databases is accessed and compared by a processor 67 in order to identify potential fraud cases. The processor 67 generates action requests and reports of fraudulent activity. These outputs can be provided directly to a human operator 69 or

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 712 of 1360

can be sent to the network operator 61. Information from the databases 65, 66 and processor 67 can also be provided to the clubcard database 68.

In the example shown in figure 7 a single database 71 is used which stores information about both call detail records and credit data. The network operator 61 has access to information from this database 71 as shown in figure 7. The database 71 also comprises a processor for analysing the data and producing management reports 73. Real time access 72 to the database 71 can also be provided.

Because there is a time delay whilst data enters the database(s) 71, 65, 66 then the database may state that no credit remains on a particular SmartCard, when in fact the user has recently recharged the SmartCard. Allowance is made for this in order to avoid detecting this situation as a case of fraud. This is described below.

The processor 71, 67 in the fraud management system is arranged to detect a potential case of fraud in situations such as:

- the total number of calls made for a particular SmartCard in a predetermined period exceed a threshold level;
- the total number of units used in a single call exceed a threshold level;
- the number of calls to a free helpline number exceed a threshold level;
- calls have been made by a user who has been barred or for whom a tamper alert has been generated by "in store" card reader systems;
- if a barred type of call set up is detected such as a call transfer;
- if the number of a certain type of outbound call events generated by a user or group of users exceeds a threshold;
- if the number of inbound verses outbound call events, in a given period, by a user or group of users falls within a certain range.
- if multiple use of a handset or SmartCard is detected from CDR data; and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 713 of 1360

- if geographically improbable use of a handset or SmartCard is detected from CDR data.

The interfaces to and from the fraud management system are now described.

Interfaces

- Imports of Call Detail Records (CDR) data from the network operator are performed on either a chronological push or pull basis at intervals that are viable by the system owner.
- Imports of "credit accumulated" data are performed on either a chronological push or pull basis at intervals that are variable by the system owner.
- Import of tamper alerts or "excess credit accumulated" general action requests for termination to the network operator.
- Export of management information reports and action requests to external systems located at the operator or at the system owners premises are performed on either a chronological push or pull basis at intervals that are variable by the system owner.

The fraud detection system itself is protected from unauthorised access by Firewall Security on call External Data Communications.

Security

- The fraud detection system is protected from unauthorised access by firewall security on all external data communications.
- Physical access to the system is only possible by authorised personnel who are required to pass security vetting procedures.
- Back up of the system data is performed at regular intervals and back up data is stored at a secure off site location.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 714 of 1360

Use of handset and removable module to monitor the duration of calls

Because the CDRs are downloaded to the fraud detection system at intervals, such as 12 hourly or 2 hourly intervals, then a time window is present during which fraudulent use of "unpaid for" airtime may occur. In order to reduce this problem the handset and removable module combination is able to monitor call durations during this time window. If more than a threshold level of total call duration is exceeded during this time window than a potential fraud is detected. In this event the communications apparatus is either shut down until the time window has passed or the network operator or security staff are alerted.

This is implemented by incorporating a timer mechanism into the removable module or SmartCard. At the start of a call a pulse signal is sent from the handset to the module and this activates the timer mechanism. At the end of a call another pulse signal is sent from the handset to the module to deactivate the timer. The timer thus monitors total call duration for all calls during a time window, after which it is reset to zero. A processor in the removable module or SmartCard compares the call duration value from the timer against a predetermined threshold and if the threshold is exceeded all outgoing calls are barred for the duration of the time window.

The time window, or exclusion time is set from within the handset/SmartCard combination. At the end of this time normal outgoing call usage is restored and the process counters are reset to zero time.

If the total call duration time as monitored by the handset and module is less than the prescribed threshold then no action is taken to terminate outgoing calls.

Emulation of advice of charging signals

In the situation that no pulses or signals are provided by the network operator which contain information about the current charging rates then the handset and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 715 of 1360

SmartCard combination is able to emulate these signals. For example, this is required when charging signals are blocked, disrupted or not provided.

A timer mechanism is provided in the handset or in the removable module in order to emulate the charging signals. This timer may be the same as the timer described in the section headed "use of handset and removable module to monitor duration of calls" above. This timer mechanism is activated by signals from the handset which are provided at the start and end of a call. Information about tariff rates is stored in the handset or removable module. For example, this information can be stored in the form of a look up table. Time information from the timer mechanism is then used in conjunction with the tariff information in order to determine the cost of the call. The electronic purse is then decremented accordingly.

Other security features

- The handset is provided with two personal identification number accesses. A first PIN access allows the handset to be activated and a second provides access to sub routings which can change values such as the value of charges or amount of charge time.
- Certain types of call, such as those to 0891 numbers may simply be barred to help prevent fraud.
- A particular handset and removable module or SmartCard are electronically "locked" together during the manufacturing process so that they may only be used in conjunction with each other. This is done by storing a secure key in either or both of the handset and the removable module or SmartCard. The secure key is a cryptogram or other encrypted code. Means for checking that this secure key is present and correct are provided in the handset or removable module. Each handset and module pair is given a unique key so that they will only function fully together. The term "key" is used to refer to stored cryptograms, encoded

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 716 of 1360

information and other electronic keys as well as physical apparatus which ensures that a particular handset can only be used with a module which is able to operate the key.

SmartCard

Details about the SmartCard are described below:

Functionality

The SmartCard provides the means for storing an amount of credit in agreed currencies or units of time up to predetermined maximum values, which are variable by secure communication to a SmartCard reader. The credit is debited by the operation of a mobile telephone or by a card reader in a point of sale terminal.

The SmartCard provides control over the mobile Handset functions of:

- Network authentication per the GSM protocols.
- Phone book directory per Handset implementation.
- Short message service.
- Handset welcome and permanent message display
- Confirm that the credit remaining prior to call set up is above a pre-set threshold value held on the SmartCard, and prevent call set up if below this value.
- Monitor credit remaining for a call in progress, decrement the credit at specific usage rates derived from an advice of charge, (AOC) trigger signal on the signalling channel and interrogate the tariff information stored on the SmartCard. The network operator sends out signals which provide information about the charging rate. Examples of these signals are AOC or CAI (charging advice information). Any such type of signal can be used to enable the credit to be decremented correctly.
- Monitor total duration of calls made in a period and prevent additional calls until this period is expired, excluding all zero rated calls.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 717 of 1360

- Monitor call in progress duration, provide user warning and tear down when threshold reached.
- Holding pre-determined call limits and monitoring all calls made over a given period, and of a given duration, to allow for call barring should these pre-determined thresholds be exceeded. This is described in detail in the section headed "use of handset and module to monitor the duration of calls"
- The SmartCard is able to place restrictions that allow single language selection only.
- Provide advice of charge (AOC) charging information to the handset, when AOC emulation is used in the handset firmware for those instances where AOC is not presented or supported by the network.
- The SmartCard is able to hold a secure electronic purse function that is capable of managing and controlling units of currency that are stored within it.
- The SmartCard is capable of storing loyalty or other retailer defined units as "points" which may have no monetary value placed upon them. These "points" are redeemable via the SmartCard reader as units to be used in Prepay systems.

Interfaces

- A set of interface protocols are defined for secure transactions between the Handset and the SmartCard, to prevent fraud either through spoofing, or tamper of either the Handset or the SmartCard.
- A set of interface protocols are also defined for secure transactions between the card reader and the SmartCard, to prevent fraud either through spoofing, or tamper of either the card or the card reader.

Security

- No information generated by the SmartCard to the Handset relating to prepay usage is transmitted to the network by the radio interface or by any other means.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 718 of 1360

- The SmartCard is capable of detecting unauthorised tampering and ceases to function until returned to a card reader and reactivated. For example, if the wrong personal identification number is entered three times during the card validity check process.
- The SmartCard protocols prevent no more than 3 unauthorised actions to access any secure area before complete termination of the SmartCard functions.
- A limited number of master SmartCards may be provided for use by point of sale operators, issued under strict controls in store.
- A number of secure access modules (SAM's) for use in the card readers at point of sale can be provided. A SAM is a fixed SIM which contains cryptograms for accessing the identity or secure key information from the SmartCards.

The SmartCard:

- Allows remote disablement of the Handset and SmartCard upon authenticated request by the network or by the card reader.
- Allows remote enabling of the Handset and SmartCard upon authenticated request by the network or by the card reader in combination with user PIN entry.
- Does not allow re-enablement of the SmartCard once it has been disabled.
- Allows remote individual update of the threshold values held in the SmartCard, either by the card reader or over the network.
- Does not allow manual user reset of the Advice of charge indicators via the Handset, or access to PIN2 of the handset.
- Does not suffer any electrical or physical damage if withdrawn from the Handset or Card reader, while power is applied. The SmartCard retaining unit, in one embodiment, has retaining pins that are close together. The retaining unit is specially designed such that these pins do not flex and contact each other, so creating a short circuit.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 719 of 1360

- Is delivered pre-registered with the network operator but not activated for use. Activation is only possible via the Card Reader.
- Permits Incoming calls when the credit has expired.

Standard Functions NOT required on the Card

Standard functions that are not required on the SmartCard, such as phone book options can be removed in order to make room for extra filters or algorithms for coding or decoding encrypted information.

- Phone Book Options

Form factor

- The SmartCard can be a full size SIM, mini SIM adapter based alternatives are also possible.
- The SmartCard can be delivered with a surface finish or other orientation mark to assist in identification of its correct insertion for visually impaired users.

Appearance

- The SmartCard can be capable of accepting various finishes e.g. silk screen printing for branding.
- In one embodiment each SmartCard is individually marked with a machine readable bar code and human readable serial number. Records of all SmartCard serial numbers and their distribution can then be kept.

SmartCard Reader

Functionality

The SmartCard reader:

- Allows SmartCards to be activated for first use and recharged with credit on a periodic basis. Allows SmartCards to be deactivated by the operator or automatically upon detection of tampering within the SmartCard by the SmartCard reader system.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 720 of 1360

- Allows the operator to read from a SmartCard remaining credit on a card inserted in the reader.
- Captures and temporarily stores the credit held on the card and the subscriber phone number to allow transfer to a replacement card.
- Allows transfer of credit remaining on the SmartCard to a new card or to a secure external system for point of sale transactions.
- Is intuitive to use by semiskilled checkout operators with a minimum of training, and employs the use of icons to indicate functions where possible.
- Is easily serviced by trained personnel, with a good supply of replacement parts and spares.
- The SmartCard reader allows a secure sign-on process at power on, user log on and log off. This process involves the use of master SmartCards coupled to PIN number entry.
- The SmartCard reader is capable of maintaining the system clock function to allow for daylight saving.
- The SmartCard reader is capable of recording the operator name and sign on/off date/times.
- The SmartCard reader has a supervisor login password for password administration.
- The SmartCard reader is able to hold a secure terminal key to identify each Card reader to the database to show where credit records have been generated.
- The SmartCard reader does not allow any new transactions to be made whilst, data is being transferred to the fraud detection system or remote database.
- The SmartCard reader is capable of creating batches of credit records with incrementing batch numbers.
- The SmartCard reader is capable of holding the previous 20 batches of credit records.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 721 of 1360

- Is capable of displaying simple text messages to prompt actions from operators to perform the following tasks:

    1. Authenticate new Card
    2. Apply credit to card
    3. Transfer credit between authenticated Cards
    4. Terminate Card after Credit transfer or discovery of fraudulent use.

Interfaces

- The card reader shall allow interaction to a PC or Point of Sale terminals via either a serial RS232 or other industry standard data transfer interface. The data transferred is encrypted according to a predetermined protocol.
- The card reader system allows remote polling of the system by an external data device, such as the fraud detection system, via modem dial up communications or network connection. This modem can be internal to the card reader system.
- The card reader system initiates communications with the external data device upon command by the program contained in the card reader system.
- The SmartCard reader is dismountable from a host PC if supplied as a separate unit, with minimal requirement for special tools or specialist knowledge by service personnel.
- The card reader is capable of arithmetically deriving SmartCard self identification or SRES based on algorithms held on a mini SmartCard held within the unit.
- The card reader unit is capable of supporting internal readers for plug-in SmartCards conforming to current industry standards.
- The card reader is capable of supporting a main card reader that takes full size cards. This reader has the following characteristics:
    - Push-pull reader with landing contacts;
    - MTBF of 250,000 insertion cycles (minimum);

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 722 of 1360

- Interface deactivation according to ISO 7816/3;
- Active short circuit protection for the SmartCard;

- The unit is capable of supporting Industry standard protocols, for communication between the SmartCard and the reader, including Asynchronous protocols: T=0, T=1;
- The unit has sufficient memory capabilities to support the requirements of the data capture and transfer routines.
- The unit is capable of supporting Industry standard programming languages that are downloadable over an RS232 interface.
- The card reader system is capable of supporting common point of sale (POS) protocols to accept data transfer from POS systems to allow for updating of the values to the SmartCard.

Security

- The SmartCard reader communications with any external data device are encrypted.
- The SmartCard reader is capable of providing PIN controlled access to all of its functionality including initial access to the screen prompts prior to any form of authentication or credit related actions.
- The SmartCard reader protocols allow no more than 3 unauthorised actions to access any secure area before complete termination of the SmartCard functions.
- The SmartCard reader can detect unauthorised tampering of the SmartCard and causes the SmartCard to cease to function, in this situation.
- The SmartCard reader system software is protected from unauthorised access by either the use of PIN protection only or by the use of PIN protection and a system specific mini SmartCard being read before access to the program is granted.
- Data held on the card reader system is only transferable to other systems or devices upon the entry of security codes or devices as described previously.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 723 of 1360

Form factor

- The SmartCard reader is capable of accepting full size SmartCards and/or mini SIM's held within full size card adapters.
- Secondary card readers are provided to accept mini SIM
- The SmartCard reader has an integral display capable of displaying either text or Icons to prompt the operator.
- The SmartCard reader is of a compact size, suitable for co-location with a POS terminal or PC on a customer services desk within a retail store.
- If the SmartCard reader system consists of a PC and card reader, the overall footprint (or size of the system on the desk) does not exceed that of a standard desktop PC. Any screen used in this configuration is not larger than 12" and ideally forms a single unit with the card reader and processor.

Environmental

- The SmartCard reader system supports dual voltage input and is suitable for installation in a number of European countries, with conformance to all relevant environmental requirements e.g. EMC, Noise, Operator ergonomics etc.
- The unit is capable of being hard wired to power supply units (including UPS systems)
- All data, power, telephony communications, and internal SAM connections are capable of being secured in place to prevent unauthorised disconnection of any service.
- The unit can have battery back-up capabilities.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 724 of 1360

Handset

Functionality

The Handsets used in this project provide the following functionality:

- Be driven by a SmartCard developed for the Handset so as to provide feedback to a user of the service of the credit remaining on the SmartCard, via the Handset display.
- The Handset display shows the amount of credit available at the start of each call, the end of each call, and by quick access via a hot key sequence. This display is in minutes, viz "Time remaining =? Minutes".
- The Handset is capable of emulating AOC information when none is presented by the network for reference by the SmartCard for charging information purposes.
- Allow calls to predefined numbers held on the card, eg Emergency services and help line number(s) without debiting the credit on the card. The help line number(s) may be allowed a pre-set number of transactions per period at which point additional use is denied until the period is expired.
- The extended menu option which gives access to PIN2 is set to the "OFF" position.
- Allow remote enabling of the Handset and SmartCard upon authenticated request by the network, in combination with user PIN entry.
- Allow remote individual update to the threshold values held in the SmartCard over the network.
- Provide speed dial access to the network operator's voice mail system.
- Call waiting, call swap (in which a call is transferred to another number) and call hold are allowed as long as any outbound call in progress continues to decrement the credit on the SmartCard. The SmartCard allows the barring of calls by Calling Party Category (CPC).

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 725 of 1360

- The Handset does not allow manual user reset of the Advice of charge indicators via the Handset, or access to PIN2.
- Roaming is not allowed by the Handset.
- The language default, ie the ability to access other network providers original is set to "English".
- The display is capable of displaying an alternating message in the style of "Emergency/Helpline Calls ONLY" and "Operator Name" when credit has expired.
- The display is capable of displaying the operator PLMN code rather than the operator name.
- Line 2 (ie a second line in a call swap) is not supported by the Handset.
- The Handset has the menu functions and associated GSM instruction sets removed or deleted, prior to despatch, for the following call types and menus:
  - Call Transfer;
  - Call forwarding (except Voice Mail);
  - Conference/Multiparty call set up;
  - Roaming facilities;
  - Restricted Dial lists;
  - Sub menu "Bar all incoming calls when roaming";
  - Call divert and sub menus;
  - Select phone line;
  - Call Charge settings;
- The purpose of this is to reduce fraud and costs. Also the space in the Handset that is otherwise used for these functions can be used for other things.
- In addition, the following call types and menus are removed because they cannot be provided by the pre-paid mobile phone system.
  - Change Greeting;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 726 of 1360

- All access to SIM memory for:
    - SMS;
    - Phonebook;
    - Capacity add or delete;
    - Copy functions;
    - One touch dialling;
    - Fixed Dialling;
    - Phone Status;
    - Network Selection;
    - Call Meters;

Also:

- The Master Reset or Clear functions are not able to reset or enable any features barred from use.
- Emergency 999/112 calls are allowed without a SmartCard being inserted into the Handset or when credit has expired.
- The Handset is capable of providing a user configurable decrement warning to indicate unit usage, in both visual and audible formats.
- The Handset is capable of providing a "Credit nearing expiry, please recharge" warning to the user in both visual and audible formats.
- The Handset is capable of providing a user warning and also of "tearing down the call" when credit is expired or when a threshold configurable via the card reader or over the radio interface is reached.
- The Handset is capable of providing a "Credit expired, please recharge", warning to the user in both visual and audible formats, and prevent call set up being activated except for emergency and helpline calls.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 727 of 1360

- The Handset supports voice calls and the Short Message Service. It supports restricted dialling, phone book, and diverts to voice mail.
- The default Caller line Identifier condition is set to "Present".
- The Handset is capable of being locked to a single network operator and to the SmartCard. These locks are not user addressable under any circumstances.
- The Handset has good standby battery life, in excess of 40 hours and talk time in excess of 90 minutes.
- The Handset supports one number dialling to the network voice mail service.
- The Handset display is easy to read and supports icons as well as text.
- The Handset is capable of supporting calls to pre-determined help line numbers on a toll free basis.
- The Handset manufacturer is able to unlock a SmartCard from its Handset in the repair centre. This is necessary if, for example, the Handset breaks when there is a large amount of credit on the SmartCard.
- The Handset permits Incoming calls when credit has expired.

Interfaces

- The Handset user interface is intuitive to the novice user and presents information in a logical and clear fashion. The use of multiple level menu access for the most common activities is avoided. Integral context sensitive user help is desirable.
- The Handset can support interfaces to data cards for connection from modem or laptop for example, and may have a connection for external power supplies.
- The Handset supports full size SIM cards and ideally contains a SIM release mechanism such that the user does not need to disassemble the Handset or battery to remove the SIM for recharging.
- The SIM does not suffer any harm due to withdrawal of the SIM while the Handset is switched on.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 728 of 1360

- The SIM to Handset interface supports insertion of the card with a duty cycle in excess of 5000 insertions before any degradation of the interface to the SIM is observed.

Security

- The Handset allows the suppression of access to PIN2 and other Handset menu functions by means of instruction from the SmartCard.
- The access control features are not addressable by the user from the Handset user interface, except for PIN1.
- The Handset has intrinsically good security to prevent unauthorised access to the data transfer between the SmartCard and the Handset.
- The physical design of the Handset is arranged to deter tamper or access to the contacts of the SIM. Ideally any attempt at access to the interior of the Handset leads to the destruction of the Handset.
- Preferably SIM card extenders which enable manipulation of a SIM card by keeping it outside the Handset cannot be with the Handset, when in operation.

Form factor

- The Handset supports full size SIM cards.
- The Handset is of a compact design and subject to evaluation on the basis of appearance, layout, clarity of markings, innovative features, user friendliness, audio quality etc.
- The Handset is of robust construction and provides good ergonomic operation to the user both in call set up and during a call.

Environmental

The Handset is capable of being marked with branding marks, on the front or on the keypad cover as appropriate.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 729 of 1360

Accessories

- A full range of accessories including car kits, desk top chargers, desktop hands free kits, data cards (if appropriate) and a range of battery options, can be used with the Handset.
- The Handset is supported by a manufacturer's User Guide, Frequently asked Question and Answer sheets.

Operational requirements

- The network supports advice of charge (AOC) or other suitable systems which can be used to decrement credit held on the prepay SmartCards.
- The network is capable of setting the AOC decrement interval to 10 seconds at delivery and can allow this interval to be configurable over the radio interface to the Handset.
- The network supports remote enabling and disabling of the Handset and SmartCard via authenticated request by the network to the Handset in combination with user PIN entry.
- The network is capable of monitoring the destinations of calls initiated and restrict calls to predefined destinations by National Number Group.
- The network is capable of barring all calls to premium or international destinations.
- The network is capable of preventing call transfer, call forwarding (except to voice mail), conference calls or any non standard or basic call types from being initiated.

The network is capable of allowing Data calls and Short Message Service (SMS) calls on the basis that these are charged at the same rate as voice calls. If this is not possible inbound data and SMS calls only are allowed. The network should be capable of barring these outbound calls if charging on the above basis is not possible.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 730 of 1360

Rating and tariff requirements

- A tariff or look up table to be stored in the SmartCard to generate AOC information to the Handset on the basis of flat rate charging is required from the operator.
- The network operator provides the facility to zero rate calls to specified numbers such as helpdesk numbers and emergency calls.
- Over time other tariffs may be introduced, and the network operator is able to support the introduction of new tariff plans via AOC in reasonable time scales.
- Call Detail Records (CDR) produced within the network by use of the present invention are segregated from the operator's other traffic and moved to a secure area for export to the fraud detection system. The frequency of the collation and export of the CDR data shall not exceed 12 hours and may be as frequent as hourly.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 731 of 1360

Claims

1. A portable radio communications apparatus comprising:

(i) a portable handset;

(ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit;

(iii) a recess in the handset adapted to accept the removable module;

(iv) a reading device in the handset adapted to determine a content of the electronic purse;

(v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse;

and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed.

2. A portable radio communications apparatus as claimed in claim 1 wherein the removable module comprises a SmartCard.

3. A portable radio communications apparatus as claimed in claim 1 or claim 2 wherein the subscriber identification unit comprises a conventional subscriber identification module.

4. A portable radio communications apparatus as claimed in any preceding claim wherein said handset and said removable module are electronically locked such that a particular handset and module pair only function fully together.

5. A portable radio communications apparatus as claimed in claim 4 wherein said handset and said removable module contain information about a secure key that is unique to a particular handset and removable module pair.

6. A portable radio communications apparatus as claimed in any preceding claim which further comprises a timer mechanism adapted to monitor call duration, said timer

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 732 of 1360

mechanism being adapted to be activated by signals from the handset at the start of a call.

7. A portable radio communications apparatus as claimed in claim 6 which further comprises a store of information about costs and a processor adapted to decrement the electronic purse on the basis of the cost information and the monitored call duration.

8. A portable radio communications apparatus as claimed in claim 6 which further comprises a processor adapted to compare the monitored call duration with a prespecified threshold value and to bar outgoing calls in the event that the threshold value is exceeded.

9. A communications network comprising at least one portable radio communications apparatus as claimed in any preceding claim.

10. A communications network as claimed in claim 9 comprising a fraud detection system, said fraud detection system comprising database means for storing information about calls made from the handset over the communications network, and information concerning the number of airtime units credited to the electronic purse associated with said portable radio communications apparatus.

11. A communications network as claimed in claim 10 wherein said fraud detection system further comprises a processor adapted to compare the information about calls and the information about electronic purse contents.

12. A removable module suitable for use with a portable radio communications handset said module comprising a rechargeable electronic purse and a subscriber identification unit, said module being adapted to be received in a recess in said handset, and wherein said module is adapted such that in use the handset is substantially inoperable when the module is removed from the communications apparatus.

13. A removable module as claimed in claim 12 which contains information about a secure key that is unique to the particular removable module and its handset pair.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 733 of 1360

14. A removable module as claimed in claim 12 or claim 13 which comprises a timer mechanism adapted to monitor call duration said timer mechanism being adapted to be activated by signals from the handset at the start of a call.

15. A removable module as claimed in any of claims 12 to claim 14 which further comprises a store of information about costs and a processor adapted to decrement the electronic purse on the basis of the cost information and the monitored call duration.

16. A removable module as claimed in any of claims 12 to claim 15 which further comprises a processor adapted to compare the monitored call duration with a prespecified threshold value and to bar outgoing calls in the event that the threshold value is exceeded.

17. A recharging system adapted to recharge an electronic purse of a removable module as claimed in any of claims 12 to 16.

18. A recharging system as claimed in claim 17 comprising a reader adapted to read the contents of the electronic purse and means for sending an encrypted update message to the removable module in order to update the electronic purse.

19. A recharging system as claimed in claim 17 or claim 18 comprising at least one database of stored subscriber information and means for comparing the subscriber identification unit with said stored information.

20. A recharging system as claimed in claim 19 comprising at least one local database and at least one remote database.

21. A recharging system as claimed in any of claims 17 to 20 wherein said reader and means for sending an encrypted update message to the removable module are connected to a point of sale apparatus.

22. A recharging system as claimed in claim 21 wherein said reader and said means for sending an encrypted update message to the removable module are electronically locked to the point of sale apparatus.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 734 of 1360

23. A portable radio communications handset adapted for use with a removable module as claimed in any of claims 12 to 16, said handset comprising a recess adapted to accept the removable module; and a reading device adapted to determine a content of an electronic purse in the removable module.

24. A portable radio communications handset as claimed in claim 23 wherein said handset is adapted to send a signal to the removable module at the start and end of a call.

25. A portable radio communications handset as claimed in claim 23 or claim 24 wherein said handset contains information about a secure key that is unique to the particular handset and its removable module pair.

26. A method of communicating using a portable radio communications apparatus as claimed in any of claims 1 to 8 said method comprising the steps of :

(i) purchasing air time from an air time provider or suitable intermediary;

(ii) charging said electronic purse with units equivalent to purchased air time;

(iii) inserting the removable module incorporating the electronic purse into the recess in the handset;

(iv) determining a content of the electronic purse;

(v) allowing substantial operation of the communications apparatus on the basis of the content of the electronic purse;

(vi) operating the communications apparatus and updating the content of the electronic purse on the basis of said operation.

27. A method as claimed in claim 26 wherein said step of updating the content of the electronic purse involves transmission of encrypted messages between the handset and removable module.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 735 of 1360

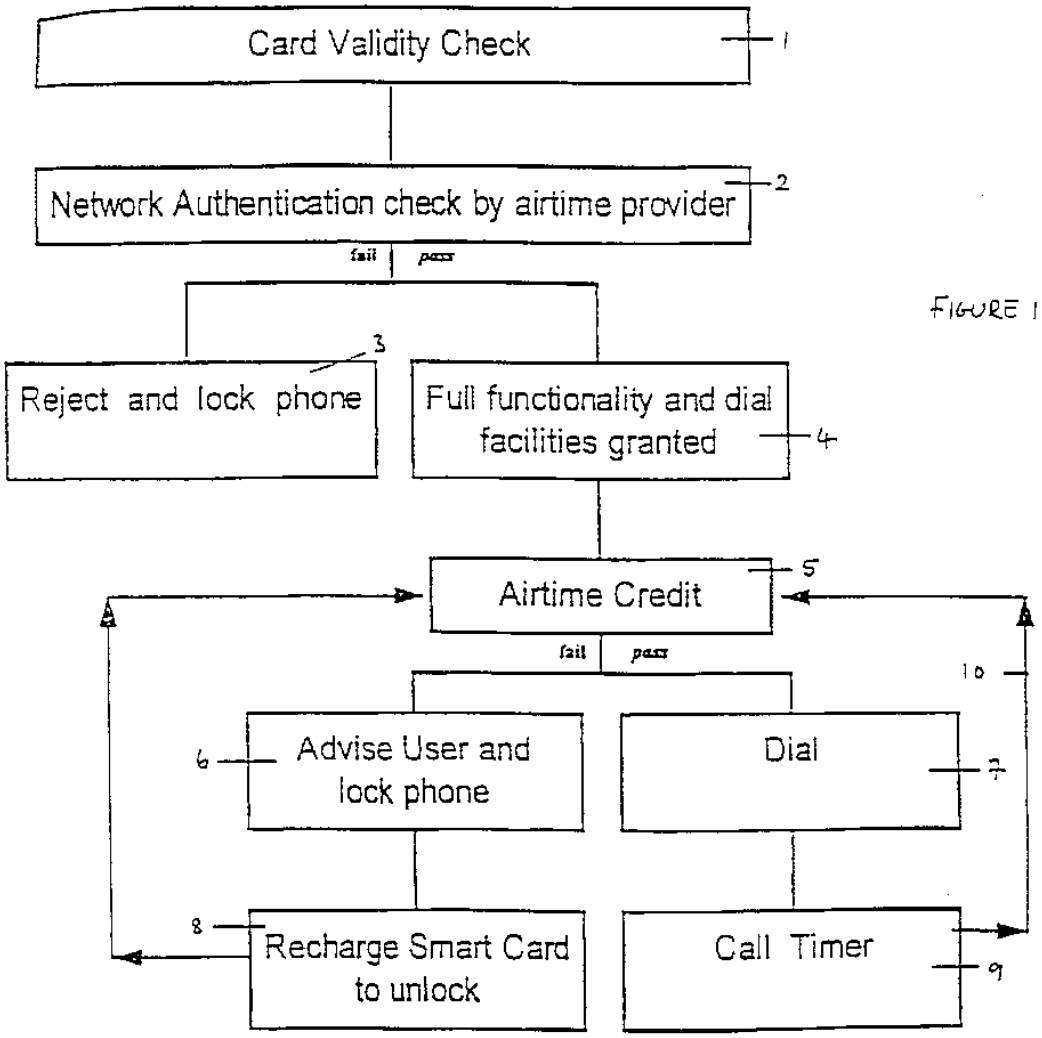


FIGURE 1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 736 of 1360

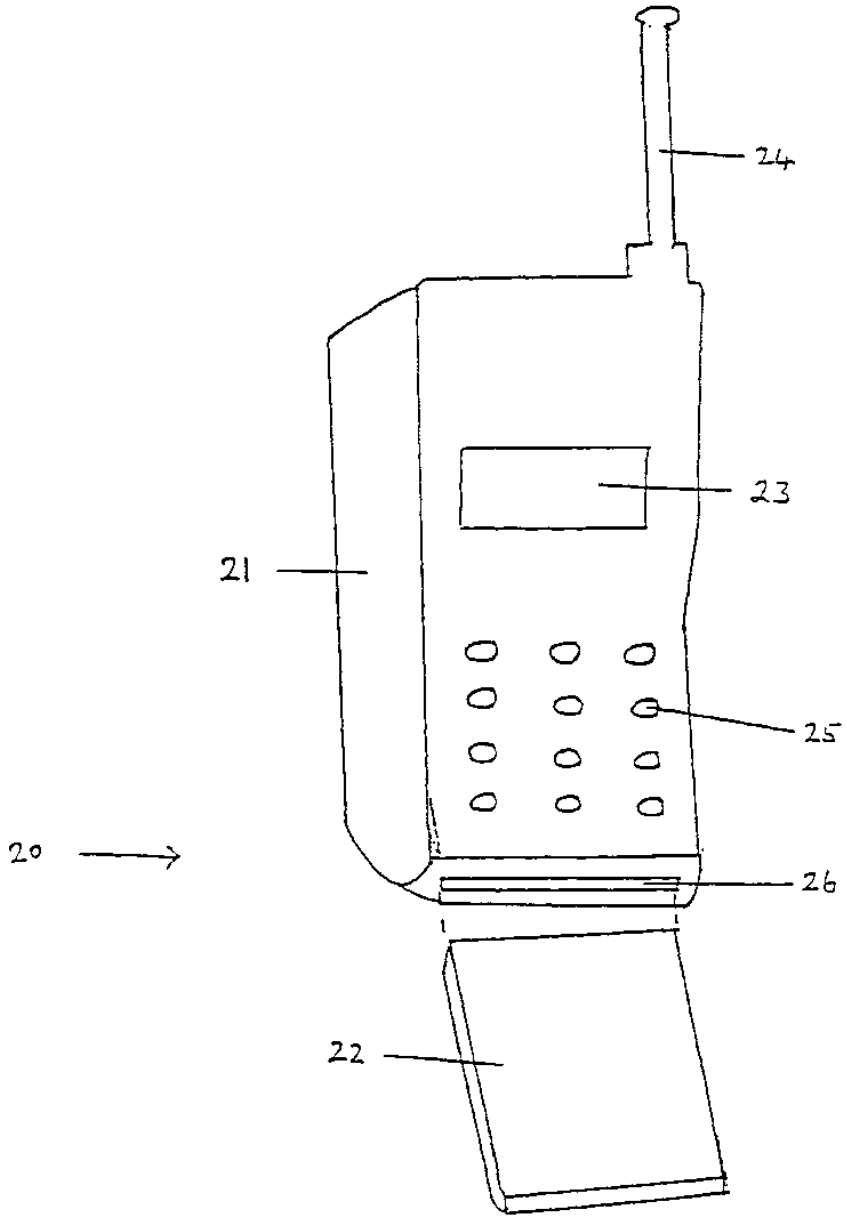


FIGURE 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 737 of 1360

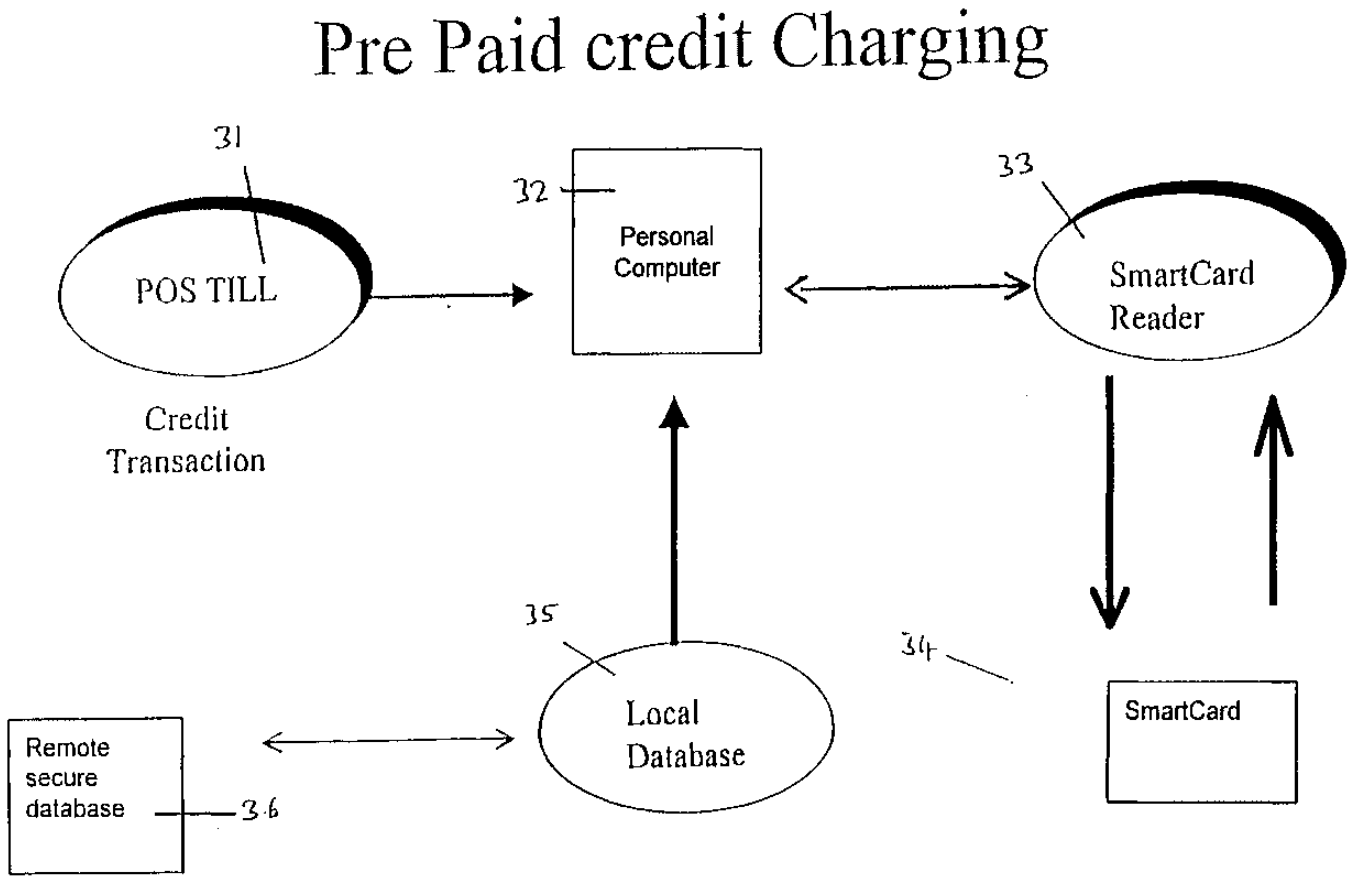

Pre Paid credit Charging
31
POS TILL
Credit
Transaction
32
Personal
Computer
33
SmartCard
Reader
35
Local
Database
34
SmartCard
Remote
secure
database
36

FIGURE 3

Credit Recharge

FIGURE 4

Card Initialisation

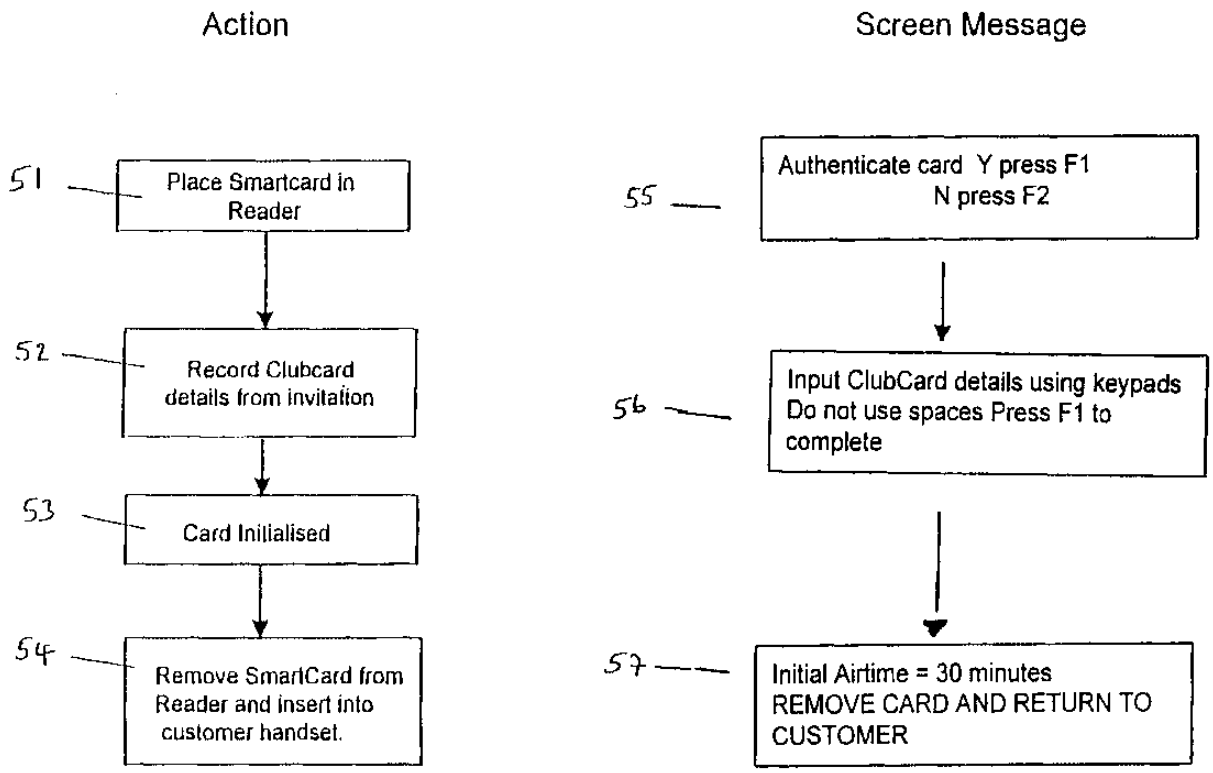


FIGURE 5

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 740 of 1360

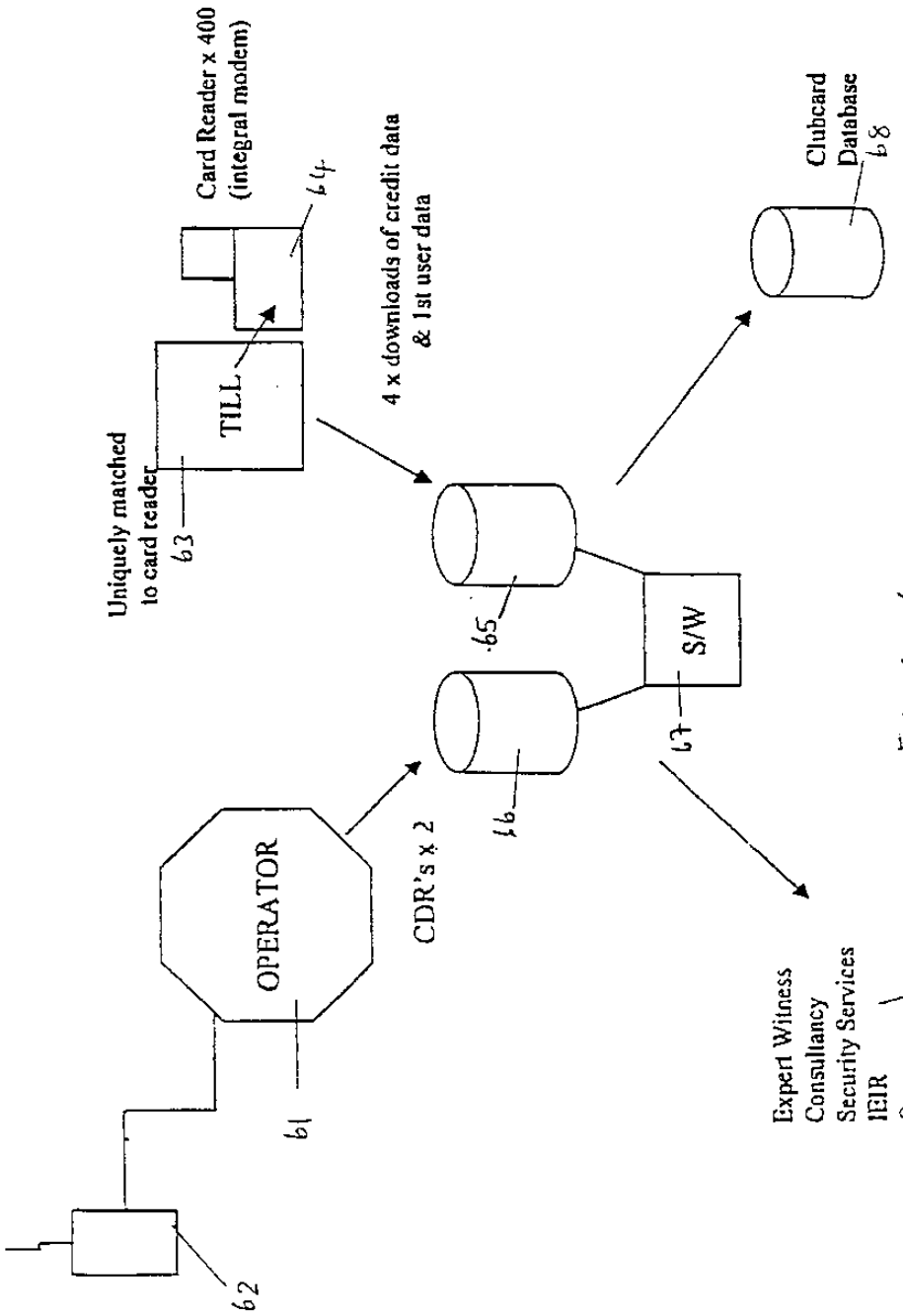


FIGURE 6

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 741 of 1360

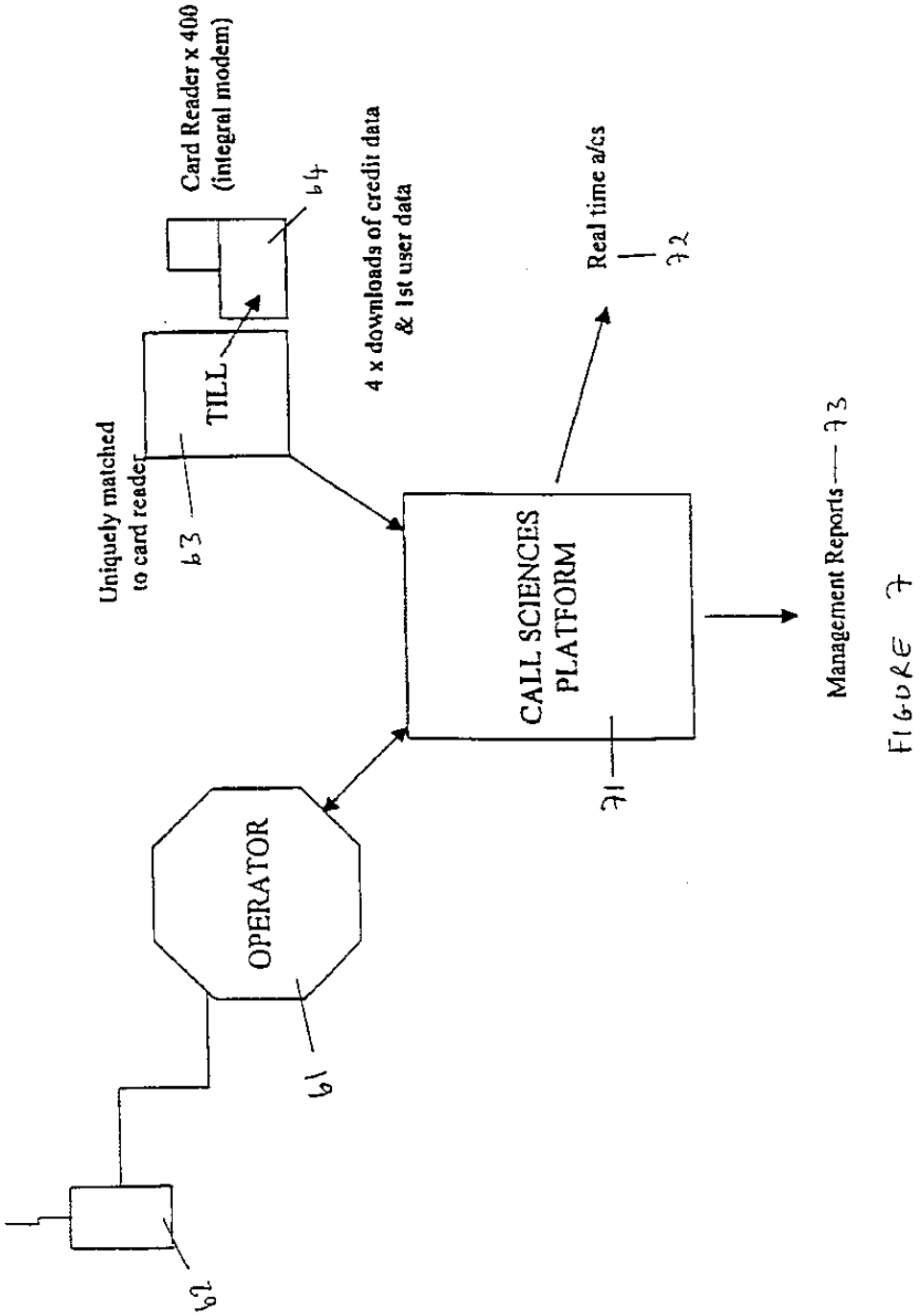


FIGURE 7

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 742 of 1360

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/GB 98/02729

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04M17/00 H04Q7/32

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 6 H04M H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 790 587 A (PHILIPS ELECTRONICS NV) 20 August 1997	1-3,6-9, 12, 14-17, 23,24, 26,27
A	see column 3, line 26 - column 4, line 21	10
X	WO 95 28062 A (NOKIA TELECOMMUNICATIONS OY) 19 October 1995	1-3,6-9, 12, 14-17, 23,24,26
	see page 3, line 1 - page 4, line 5 see page 8, line 24 - page 10, line 3 see page 11, line 35 - page 13, line 16	
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 December 1998	29/12/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx 31 651 epo nl, Fax: (+31-70) 340-3016	Neves Appelt, D

Form PCT/ISA/210 (second sheet) (July 1992)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 743 of 1360

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 98/02729

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 308 528 A (KARAGOEZLUE IBRAHIM MURAT ;RAMIS HARRY (GB)) 25 June 1997 see abstract see page 4, line 1 - page 6, line 27 see page 11, line 26 - page 12, line 22 see page 14	1-9, 12-17, 23-27
A	US 5 577 109 A (STIMSON CHARLES J ET AL) 19 November 1996 see column 1, line 59 - column 3, line 6	17-22
A	GB 2 267 794 A (CONROY ALAN KILPATRICK) 15 December 1993 cited in the application see page 3	1,2,5,9, 12,13, 17,23, 25,26
A	WO 97 05729 A (TELECOM ITALIA MOBILE S P A ;SENTINELLI MAURO (IT)) 13 February 1997 cited in the application see page 6 - page 7	1-3,6,7, 9,12,14, 15,23,26

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 744 of 1360

INTERNATIONAL SEARCH REPORT

information on patent family members

Inte[illegible]onal Application No
PCT/GB 98/02729

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0790587 A	20-08-1997	FR 2744822 A	14-08-1997
		CN 1168609 A	24-12-1997
		JP 9233541 A	05-09-1997
WO 9528062 A	19-10-1995	AU 691604 B	21-05-1998
		AU 2216795 A	30-10-1995
		CN 1151240 A	04-06-1997
		EP 0754394 A	22-01-1997
		FI 963996 A	05-12-1996
		JP 10501931 T	17-02-1998
		US 5748720 A	05-05-1998
GB 2308528 A	25-06-1997	NONE	
US 5577109 A	19-11-1996	US 5511114 A	23-04-1996
		AU 2770795 A	04-01-1996
		CA 2192310 A	14-12-1995
		WO 9534161 A	14-12-1995
		US 5721768 A	24-02-1998
GB 2267794 A	15-12-1993	NONE	
WO 9705729 A	13-02-1997	IT RM950521 A	27-01-1997
		AU 6667896 A	26-02-1997
		CA 2227340 A	13-02-1997
		CN 1192308 A	02-09-1998
		CZ 9800233 A	15-07-1998
		EP 0840973 A	13-05-1998
		NO 980341 A	26-03-1998
		PL 324646 A	08-06-1998

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 745 of 1360

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2008 (17.01.2008)

PCT

(10) International Publication Number
WO 2008/008735 A2

(51) International Patent Classification:
G06K 5/00 (2006.01) *G06K 15/00* (2006.01)

(21) International Application Number:
PCT/US2007/073082

(22) International Filing Date: 9 July 2007 (09.07.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/457,120 12 July 2006 (12.07.2006) US

(71) Applicant *(for all designated States except US)*: **IBREVA CORPORATION** [US/US]; 555 Bryant Street, Suite 322, Palo Alto, CA 94301 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **GIORDANO, Claeton, J.** [US/US]; C/o Ibreva Corporation, 555 Bryant Street, Suite 322, Palo Alto, CA 94301 (US). **GREEN, Donald, T.** [US/US]; C/o Ibreva Corporation, 555 Bryant Street, suite 322, Palo Alto, CA 94301 (US).

(74) Agents: **FARN, Michael** et al.; Fenwick & West Llp, Silicon Valley Center, 801 California Street, Mountain View, CA 94041 (US).

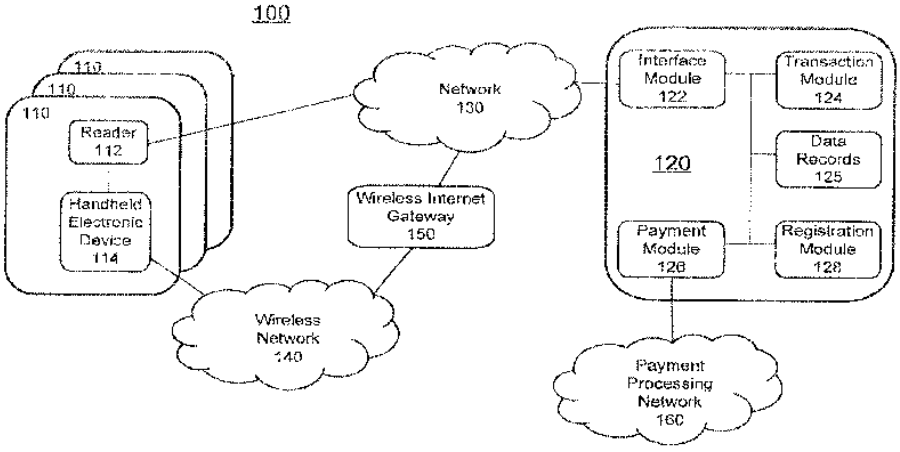
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: TRANSACTION USING HANDHELD ELECTRONIC DEVICES BASED ON UNOBTRUSIVE PROVISIONING OF THE DEVICES



(57) Abstract: A system and method enabling consumers to settle payments using a handheld electronic device. The handheld electronic device preferably is provisioned with a unique code in a manner that does not require specialized software or hardware. A reader receives the unique code from the handheld electronic device, determines a consumer ID, and transmits the consumer ID, a reader ID and a payment amount to a service center. The service center retrieves the consumer account and the merchant account based on the consumer ID and the reader ID, and settles the payment by transmitting the accounts and the payment amount to a payment processing network.

WO 2008/008735 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 746 of 1360

TRANSACTIONS USING HANDHELD ELECTRONIC DEVICES BASED ON UNOBTRUSIVE PROVISIONING OF THE DEVICES

INVENTOR(S):
Clacton J. Giordano
Donald G. Green

FIELD OF THE INVENTION

[0001] The present invention relates generally to transactions using handheld electronic devices, for example using mobile phones as payment instruments. More specifically, the present invention relates to the use of handheld electronic devices in a manner where the provisioning of these devices for these transactions can be accomplished in a relatively unobtrusive manner.

BACKGROUND

[0002] Mobile phones and other handheld electronic devices are becoming ubiquitous and are also rapidly becoming more powerful and functional. Many users carry their mobile phones more frequently and to more places than their wallets or car keys. Because mobile phones are becoming an inseparable part of daily life, there is an increasing interest in expanding the functionality of mobile phones beyond just phone calls. For example, there is some interest in enabling mobile phones to make payments or to facilitate other types of transactions.

[0003] One attempt to use mobile phones as payment instruments requires customers to establish and maintain a new account into which they transfer funds from their bank account or credit card account. The mobile phone effectively becomes a sort of prepaid cash card. One drawback is that this approach typically requires a separate dedicated account, meaning that the customer must take the initiative to open a new account and then must manage one more account. Also, because the new account typically is funded by the customer's existing accounts, he may have to pay a higher interest rate if the account is funded by transfer from a credit card account or accept a lower return if the new account is funded from a savings account. More accounts generally results in higher transaction costs, whether it be in the form of higher interest, lower returns or added fees.

[0004] Another approach requires the use of a mobile phone specially designed for use in payment transactions. While this approach may provide users with features specifically designed to make payments, it greatly limits consumers' choices in mobile phones. This is

especially problematic considering that many customers use their mobile phones as personal digital assistants (PDA), game consoles, MP3 players, cameras or other purposes. Requiring customers to use certain types of mobile phones forces them to forego the wider variety of mobile phones that might otherwise meet their specific needs. In addition, customers must purchase a new phone if their current phone is not one of the specially designed phones.

[0005] In a related approach, rather than requiring customers to use specific types of mobile phones, existing mobile phones are provisioned to support payment transactions by adding special technology (hardware and/or software) on an "after market" basis. While this approach avoids some of the drawbacks of the previous two approaches, it also inherits some of the drawbacks from both of the previous two approaches. Requiring the addition of special technology often means that the customer must take the initiative to have the technology added (or at least agree to its addition). In some cases, such as with specialized hardware, the customer will have to take the extra step of either adding the hardware himself (with all of the attendant problems) or making a special trip to a service center where the hardware can be added. In addition, the issue of compatibility almost always means that not all types of mobile phones will be supported, thus limiting the customer's choice. It is even possible that, as new updates of the specialized technology are released, a phone that was compatible with an earlier version may lose compatibility with the newer version and thus lose its payment transaction capability.

[0006] More generally than just payment transactions, a majority of the mobile phones currently on the market have some kind of network accessing capability, enabling mobile users universal access to the wireless Internet. The mobile network technologies are maturing rapidly and the deployed connection speeds are approaching those of DSL. The relevant mobile data services standards are also mature and have broad industry support. However, acquiring and manipulating content using mobile phones is still very inconvenient. This is partly because both the display and the input method of the mobile phone are restricted by its size, causing interactive Internet access using the mobile phone to be inefficient.

[0007] Therefore, there is a need for convenient and unobtrusive approaches to allow consumers to use mobile phones in payment transactions. More generally, there is a need to allow users of all sorts of handheld electronic devices to perform different transactions, including payment transactions and accessing and manipulating content or other relevant information.

SUMMARY

[0008] In certain embodiments of the present invention, consumers can use handheld electronic devices to settle payment transactions. The handheld electronic device is provisioned (preferably in an unobtrusive manner) with a unique code that is associated with the consumer's account that will be used to settle the payment transaction (e.g., a credit card account or bank account). For convenience, this account will be referred to as a payment account. The unique code preferably is not native to the handheld electronic device (e.g., it is not the serial number of the handheld electronic device). As a result, the need for physical access to the device and/or cooperation of device manufacturers is eliminated. A reader acquires the unique code from the handheld electronic device. The reader transmits a corresponding consumer ID based on the unique code and payment transaction data to a remote service center to authenticate the consumer and settle the payment.

[0009] In one embodiment, payments are settled using the Automated Clearing House (ACH) network using mobile phones. As part of the registration process, the mobile phone handset is provisioned by downloading a barcode (or data that can be used to generate a barcode) to the handset. Many handsets are capable of accepting this type of data so provisioning typically is unobtrusive and does not require the addition of specialized software or hardware. Furthermore, if the consumer's payment account in question is a pre-existing one, the inconvenience of establishing a new account can also be avoided. At the point of sale, the consumer displays the barcode on his handset and presents the handset to a reader. The reader optically reads the barcode, optionally acquires a PIN from the consumer, and acquires a transaction amount for the sale. The reader determines a consumer identifier (consumer ID) based on the barcode and transmits the consumer ID, optionally the PIN, the transaction amount and optionally also a reader identifier (reader ID) to a remotely located service center. The service center validates the consumer account identified by the consumer ID, optionally authenticates the identity of the consumer by the PIN, and retrieves a merchant account associated with the reader ID. If this is done successfully, the service center begins settlement of the payment transaction by submitting the identity of the accounts and the payment transaction data to the ACH network. The service center may transmit a confirmation to the reader and/or the mobile phone.

[0010] One advantage is that certain embodiments provide consumers with convenient payment methods. Certain embodiments are designed to work with existing mobile phones and existing consumer accounts. They do not require a hardware modification or application download. They also do not require the opening of a new account. Furthermore, consumers

can enroll in the payment service easily at many different locations. Once the service is activated, consumers can use their mobile phones like a PIN-protected debit card.

[0011] Another advantage of certain embodiments is security. Consumers need both the mobile phone handset and the PIN in order to make a payment. Therefore, an unauthorized person cannot use the mobile phone alone to make payments. Also, in this particular example, the unique code is optically acquired from the mobile phone handset by the reader, a mechanism which is not easily intercepted like a Bluetooth transmission. To further secure the payment system, communications between the reader and the remote service center can be secured. Furthermore, because the consumer's account information is stored at the remote service center, it is not accessible by merchants and is not transmitted between the merchant and service center. This reduces the risk of unauthorized use or disclosure of this sensitive information.

[0012] Still another advantage of embodiments that utilize the ACH network is that the ACH network has lower transaction costs compare to other payment processing networks such as credit card payment processing networks. The merchants also receive other benefits, including shorter check out times, lower fraud rates, and in some cases, an increase in sales.

[0013] The invention is not tied to just payments. For example, in another aspect of the invention, relevant content is transmitted to a user's mobile phone or other handheld electronic device upon the user's request. The user presents the unique code on his handheld electronic device to a reader. The reader transmits a corresponding user ID and reader ID to the remote service center. The service center determines content based on the user ID and reader ID, which provide information about the general context of the request. For example, the service center may retrieve a reader profile (e.g., this reader is located in a mall) and/or a user profile (e.g., this user likes sports) and return content based on the profiles (e.g., a list of sporting goods shops located in the mall).

[0014] Various advantages of this aspect are that various embodiments can determine a user's context and intention, retrieve relevant information based on the user's demand and/or push such information to the user. Another advantage is that certain embodiments deliver relevant information to the handheld electronic device without the need for bilateral relationships between users and merchants. Users do not need to sign up with each merchant or acquire merchant information to receive that merchant's content, and merchants do not need to sign up each user and acquire user information in order to deliver their content. When a new user joins the network, they have access to existing merchants and vice versa.

[0015] In another aspect of the invention, the payment and relevant content aspects are integrated to provide a system for the delivery of messages containing promotional incentives that are later automatically redeemed at the time of payment. Acquisition of the incentive is user-initiated, either at a device located within a merchant's store or elsewhere. The incentive can be activated, for example, via interaction with a web page (promotional) message, or via an SMS message, or by email sent from a handheld device or network connected computer. One advantage to this approach is that the user need not carry anything or recall any information to be supplied at the time of purchase in order to redeem the incentive. Examples of incentives include discounts, free products and the accrual of points. Another advantage is that the redemption of the incentive is integrated into the payment, enabling automatic application of the incentive to the purchase.

[0016] Another advantage is that the mechanism associates a specific presentation of an incentive to the user with a specific store visit and purchase. This enables measurement of the effectiveness of the medium for the presentation of that specific incentive and enables pay-per-action pricing of the medium. For example, an online advertisement might include a place for the user to enter their mobile phone number or instructions to send a number to the service center's SMS shortcode via SMS. The service center would record that a specific user had seen a specific ad and optionally be eligible for a specific promotional offer. A reader in a store could later retrieve this information. The user could receive the promotional discount, and the ad publisher could demonstrate that a specific ad resulted in a specific user's store visit and purchase, motivating premium pricing for that ad.

[0017] These features are not the only advantages of the invention, nor will every embodiment necessarily contain all of these features or advantages. In view of the drawings, specification, and claims, many additional features and advantages will be apparent.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Fig. 1 is a block diagram illustrating an architecture for one embodiment of the present invention.

[0019] Fig. 2 is a flowchart illustrating one embodiment of a registration process in accordance with the invention.

[0020] Fig. 3 is a flowchart illustrating one embodiment of a payment transaction process in accordance with the invention.

[0021] Fig. 4 is a flowchart illustrating one embodiment of a relevant content delivery process in accordance with the invention.

[0022] The figures depict embodiments of the present invention for purposes of illustration only. One skilled in the art will readily recognize from the following discussion that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the invention described herein.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0023] Preferred embodiments of the present invention are now described more fully with reference to the accompanying Figures, in which several embodiments of the invention are shown. The present invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather these embodiments are provided so that this disclosure will be complete and will fully convey various principles of the invention to those skilled in the art. For example, much of the discussion with respect to Figs. 1-3 focuses on an embodiment that uses barcodes on mobile phones to enable payment transactions on the ACH network. None of these aspects is required and other embodiments may not use barcodes, or mobile phone, or payment transactions, or the ACH network.

[0024] Fig. 1 shows a block diagram illustrating the architecture of a payment system 100 in accordance with an embodiment of the invention. The payment system 100 includes a service center 120, multiple readers 112 and handheld electronic devices 114. In this example, each reader 112 is located in a merchant location 110. The readers 112 are connected to the remotely located service center 120 through a network 130 (e.g., the Internet). The devices 114 are connected to the service center 120 through a wireless network 140, which in this case is connected to the service center 120 via a wireless gateway 150 and the network 130.

[0025] The service center 120 includes an interface module 122, a transaction module 124, a payment module 126, and a registration module 128, that can communicate with each other. The interface module 122 also communicates over the network 130 to the readers 112 and over the wireless network 140 (via the network 130 and wireless gateway 150) to the devices 114. The payment module 126 communicates with one or more payment processing networks 160.

[0026] Considering each of the components in turn, the handheld electronic device 114 is a physical device with wireless or cellular access capability. Examples of the device 114 include mobile phones, wireless enabled personal digital assistants (PDA) and other portable wireless handheld data devices. Further examples include Palmtop computers, handheld GPS navigation devices, iPods, handheld music players, and handheld picture and video players (some have wifi or gprs or other data services). In cases where the device does not have

wireless capability, other communications media (such as the wired Internet) can be used. In the example of Fig. 1, the device 114 is equipped and configured to be able to access the wireless network 140 and to save data received from the wireless network 140.

[0027] The handheld electronic device 114 is used to present a unique code that is then acquired by the reader 112. The unique code can be an image that is displayed by the device 114, for example on a screen of the device. Two examples of images are barcodes and alphanumeric strings. For security, the images preferably are copyrighted such that digital rights management features on the device will prevent forwarding it to another device. The image can be in color or in black and white. The image need not be visible to humans. For example, it can be an infrared image that is not perceivable by humans. Alternatively, the unique code can be an audible sound, for example a ring tone. Similar to visual images, audible sounds need not be detectable by humans.

[0028] The reader 112 is a physical device with network access capability. The reader 112 is configured to include sensors designed to detect the unique code presented by the handheld electronic device 114. Examples of such sensors include barcode scanners, imaging systems, character recognition systems and microphones. The reader 112 preferably also includes a device that allows additional input of data. In this way, the user can input a PIN or other authentication data.

[0029] In this particular example, each reader 112 is deployed in a merchant location 110. The merchant location 110 is a venue where consumers may want to make payments. Examples of the merchant location 110 include movie theaters, amusement parks, paid parking garages, and retail stores. Examples of readers 112 include point-of-sale devices and kiosks.

[0030] The network 130 may be a wired or wireless network. Examples of the network 130 include the Internet, an intranet, or a combination thereof. The wireless network 140 typically is a network different from the network 130. Examples of the wireless network 140 include a Global System for Mobile communication network (also called GSM network), a Code Division Multiple Access network, a Time Division Multiple Access network, a General Packet Radio Service network, a Wideband Code Division Multiple Access network, a Time Division Synchronous Code Division Multiple Access network, a Universal Mobile Telephone System, or a combination thereof. In this example, the network 130 and the wireless network 140 are connected by a wireless gateway 150, although this is not required.

[0031] Referring now to the service center, first note that although each "module" 122-128 is shown in Fig. 1 as a single box, this is for convenience and is not meant to imply that a

module must be implemented as a single device, in a single location, or separately from the other modules. The term "module" is used here generically to refer to any combination of computing and/or communications capability. Modules can be implemented as appliances, servers, software, distributed systems, and other combinations of hardware and/or software, to name a few examples.

[0032] The interface module 122 is the front end to the other modules and functions as a communication gateway into the service center 120. The interface module 122 can be implemented in many different ways. One example is a corporation virtual private network front end. It can also contain multiple components and even networks. For example, one set of components within the interface module 122 may interface to network 130 and readers 112, and a separate set of components within the interface module 122 may interface to wireless network 140 and devices 114. These two sets of components may be physically separate and may not even communicate with each other.

[0033] Furthermore, although the communication channels to the readers 112 and devices 114 overlap in Fig. 1 (both communication paths utilize network 130), this is also not required. For example, the service center 120 may communicate with the readers 112 through a dedicated private network and communicate with the handheld electronic devices 114 through a completely separate public wireless network. Nor is it required that the same communications channel be used to communicate to all readers 112 or to all handheld electronic devices 114. For example, a proprietary interface module 122 may be used to communicate with readers 112 on a proprietary network and a web server 112 to communicate with readers 112 on the Internet.

[0034] The transaction module 124 is the engine that processes the transactions. It typically has access to various data records 125, for example consumer profiles and merchant profiles. A consumer profile typically includes information such as the consumer's name, mobile phone number, consumer identifier (consumer ID), bank account information (e.g., bank name, routing number, account number), personal identification number (PIN), and the like. The consumer profile can also store information such as whether the consumer is in good standing, which can be determined by the consumer's payment history. The transaction module 124 can create, modify, and delete consumer profiles as transactions occur and based on consumers' requests. The consumer profiles can be stored in a database 125 and indexed by the user ID and the mobile phone number. The transaction module 124 preferably can also retrieve a consumer profile from the database based on a user ID.

[0035] The transaction module 124 also manages merchant profiles. Similar to a customer profile, a merchant profile typically includes information such as the merchant's name, merchant identifier (merchant ID), bank account information, and the like. The merchant profiles can be stored in the database 125 together with the customer profiles. The transaction module 124 can create, modify, delete merchant profiles, and retrieve a merchant profile from the database based on a merchant ID.

[0036] The transaction module 124 also receives and services requests from the other modules. For example, the interface module 120 receives requests for payment transactions and passes these to the transaction module, which then accesses the relevant records 125 and processes the requests.

[0037] The payment module 126 settles payment transactions between consumers and merchants. It provides the interface to the payment processing network(s) 160. The payment module 126 can support one or multiple different payment processing networks 160. In one embodiment, the payment module 126 interfaces to the Automated Clearing House (ACH) network. Debit card networks and credit card networks are examples of other payment processing networks 160 that might be supported by the payment module 126.

[0038] The registration module 128 is used for initial enrollment of consumer and merchants and provisioning of the consumers' handheld electronic devices 114.

[0039] The service center 120 can be configured on one or more conventional computing systems having a processor, memory, storage, network interfaces, peripherals, and applicable operating system and other functional software (e.g., network drivers, communication protocols, etc.). In addition, the modules 122-128 are logically configured to function together and can be configured to reside on one physical system or across multiple physical systems. One skilled in the art will recognize that the system architecture illustrated in Fig. 1 is merely exemplary, and that the invention may be practiced and implemented using many other architectures and environments.

[0040] In one specific embodiment discussed in further detail below, the payment system 100 uses barcodes on mobile phones to enable payment transactions on the ACH network. In this embodiment, the handheld electronic device 114 is a mobile phone handset and the reader 112 is a point-of-sale device installed at a retail location for example at the checkout of a grocery store. The unique code is a barcode displayed on the screen of the mobile phone handset and optically read by the reader 112. The reader 112 is connected via a wireless network router to the network 130, and contains a microprocessor, wireless internet card, barcode reader, and a ¼ VGA touch screen. The mobile phone 114 is connected to the

service center 120 via its normal wireless network connection 140. The payment processing network 160 is the ACH network.

[0041] One advantage of using barcodes and mobile phones is their ubiquity and ease of use. Mobile phones are carried almost everywhere and thus will be readily available for use at checkouts. Barcodes can be unobtrusively downloaded to mobile phones and easily displayed on the mobile phone screen at checkout. Barcodes are also familiar to consumers so no lengthy adaptation period is required.

[0042] One advantage to using the ACH network to settle payment transactions is low cost. The cost of using ACH network to settle payments is much lower compared to the cost of using other payment processing networks. For example, the cost of settling a payment transaction over a credit card payment processing network averages approximately 2.5% of the total transaction cost plus a flat fee ranging from 15 to 30 cents per transaction, while an ACH transaction typically costs somewhere between 2.5 and 25 cents. By using the ACH network, the payment system 100 can reduces retailer transaction costs by 50%.

[0043] Figs. 2-3 illustrate operation of the payment system 100 using this specific example. The operation can be divided into two parts: a registration process and a transaction process. During the registration process (Fig. 2), the consumer registers for the payment service and his mobile phone(s) are provisioned to make payments. The consumer typically also creates a profile for the payment system 100. During the transaction process, the consumer uses his provisioned device 114 to settle one or more payment transactions.

[0044] Fig. 2 shows a flow diagram depicting a registration process. In this example, the registration process is initiated by the consumer. The consumer uses a terminal 202 to send 210 a registration request to the registration module 128 through the Internet and the interface module 122. As part of the registration process, the consumer also provides 212 information about the consumer's identity (e.g., name, home address), the consumer's payment account (e.g., bank name, routing number, and account number if it is a bank account, credit card number and expiration date if it is a credit card account), the device 114 (e.g., phone number if the device 114 is a mobile phone, internet protocol address if it is a network enabled PDA). Note that the registration process establishes an account for the consumer with the service center. This account, which will be referred to as the service center account, typically will not be the same as the consumer's payment account.

[0045] The consumer also selects 214 a PIN. The PIN is designed to allow subsequent authentication of the consumer. Examples include a multiple-digit number or an alphanumeric string. The PIN provides additional security to the payment system 100.

Because unauthorized parties do not know the PIN, they cannot make a payment using the consumer's payment account even if they have access to the device 114.

[0046] The terminal 202 can be any conventional computing systems with user input device (e.g., keyboard), network interfaces, and applicable operating system and other functional software (e.g., network drivers, communication protocols, encryption software, etc.). The consumer can send 210-214 the request and related information by using a web browser to visit a web site hosted by the interface module 122. The consumer can also use email to send information to the registration module 128. Alternatively, the consumer can do so by using an application designed for the registration process, in which case the necessary application can be encoded as hardware in the terminal 202. The terminal 202 can be located in a merchant location 110 or elsewhere. In other embodiments, the consumer can choose to provide 210-214 relevant information over the phone or via other conventional communication channels (e.g., the postal system) to the service center 120. In order to keep the consumer's information confidential, sensitive information preferably is encrypted before sending 210-214 to the service center 120.

[0047] In some embodiments, the registration module 128 verifies 219 the provided consumer information. For example, the registration module 128 may verify the provided mobile phone number by sending a confirmation SMS message containing a confirmation code to the mobile phone. The consumer is required to send the confirmation code back to the service center 120 in order to be verified. Alternately, the registration module 128 may confirm with the payment processing networks 160 that the consumer's payment account is a valid account and that the consumer is the account holder.

[0048] The registration module 128 creates 220 a consumer profile for the consumer and stores the received consumer information in the consumer profile within database 125. The registration module 128 also assigns 222 a consumer ID to the consumer. The consumer ID may be newly generated or may be an existing identifier (e.g., the consumer's social security number or some account number).

[0049] The registration module 128 generates 230 a unique code for the consumer profile. The unique code is associated with the consumer ID and the corresponding consumer accounts, so that a reader 112 can determine the associated consumer ID from the unique code. The relationship between the consumer ID and the unique code can be secretive or apparent. In some cases, the unique code can be the same as the consumer ID or a derivative of the consumer ID. The unique code can be an image (e.g., a barcode image), a string (e.g.,

the consumer ID in binary format), a sound sequence (e.g., a ring tone), or any other format that the device 114 can make available to the reader 112.

[0050] The registration module 128 then provisions 240 the device 114 with the unique code. This can be done in a number of different ways. For mobile phones 114, the module 128 may download the unique code to the mobile phone via the wireless network 140 using existing data services. Alternately, if the unique code is the same as the consumer ID or a variation of the consumer ID, the registration module 128 might provision the device 114 by transferring the consumer ID to the device 114.

[0051] More generally, rather than transferring the actual unique code, the registration module 128 may provision the device by transferring data that can be used to generate the unique code. This data will be referred to as digital code data. For example, the digital code data might be a seed that is used to generate the unique code, or that is combined with other data (such as the time of day) to generate the unique code. The unique code may change over time, as would be the case when it is generated based on some combination of digital code data and the time of day. Alternately, the unique code may expire periodically or after each use. This would increase the security of the payment system 100. Different types of coding, compression, hashing and encryption can be used to relate digital code data with the actual unique code used for any particular transaction.

[0052] Provisioning 240 preferably occurs without requiring the alteration of software or hardware on the device 114. One example would be the download of data that can be used to generate the unique code by using only the device's native functionality. One advantage is that this makes the unique code more portable and possible to restore should it be deleted or inadvertently modified. If the consumer changes his mobile phone, it is simpler to provision the new phone and to deactivate the old phone. For example, if the unique code is a barcode, then provisioning the new phone merely requires the download of the barcode to the new phone since the barcodes is not a native part of phones. In contrast, if the unique code was the manufacturer's serial number, which is a native attribute of a phone, then provisioning a new phone would be more complicated since the native attribute of the new phone would have to be associated with the consumer's account credentials. This would require communication of the new phone's native attribute to some registry and some form of authentication and authorization such that only the consumer could initiate use of the new phone's native attribute, in order to prevent malicious changing of the consumer's authorized phone.

[0053] In contrast, provisioning the phone based on the non-native unique code decouples the phone from the authentication scheme by relying on possession of the unique code as opposed to possession of the phone. The phone is a means for carrying the unique code, much like a wallet is a means for carrying a magnetic stripe card. In contrast, if a native attribute of the phone (such as a manufacturer's serial number or a payload bound to some native characteristic of the phone) is used instead, then the phone itself becomes part of the authentication scheme and is subject to the necessary security constraints when changing a factor instance of an n-factor authentication scheme.

[0054] Using a non-native unique code has many advantages. For example, the form, bit depth, and size of namespace for a non-native unique code is neither fixed nor controlled by the phone manufacturer. As a result, the unique ID format can be upgraded without changing the device. In addition, different and appropriate representations of the unique code can be used on different devices. As another advantage, use of a native attribute means that the native attribute must be reliably acquired by a central authority in order to associate it with the consumer's account or identity. In contrast, provisioning a non-native unique code allows the central authority make the association and then send the unique code to the consumer's phone. As another difference, if a native attribute is somehow compromised (e.g. duplicated on another phone or associated with the account of the phone's prior owner not in good standing), it effectively cannot be replaced or otherwise modified. In contrast, an existing non-native unique code can simply be replaced with a new and different one using the same provisioning process that established the original unique code. Provisioning also allows the issuer to use unique codes that are uniform across all phone manufactures. In contrast, a native attribute cannot be controlled by the issuer and may not be uniform across all manufacturers.

[0055] In some embodiments, the registration module 128 may optionally send an application to the handheld electronic device 114. The consumer can install the application (or it may auto-install) and use it to generate the unique code from digital code data received from the service center 120 and stored in the device 114.

[0056] Upon completion of steps 210-240, the registration module 128 may optionally send 250 a confirmation to the terminal 202 through the Internet, indicating that the registration process is completed and the consumer can start using the payment system 100 through the device 114. If any of the steps 210-240 fails, the registration module 128 may notify the consumer that the registration process failed.

[0057] Fig. 3 shows a flow diagram depicting a transaction process. In this example, a consumer with a provisioned mobile phone 114 would like to make a purchase from a merchant that has a reader 112 at the point of sale. The consumer makes the payment transaction using payment system 100 rather than his credit card, cash, check or other means.

[0058] The consumer uses the device 114 to present the unique code, which is acquired 320 by the reader 112. In this example, the unique code is a barcode image. The consumer displays the barcode on the mobile phone and waves the mobile phone under the reader 112. The reader 112 optically reads the barcode. If the unique code were a ringtone, the device 114 would play the ring tone to the reader 112. The reader 112 hears the ringtone through its audio sensors (e.g., microphone). The reader 112 determines 322 the consumer ID corresponding to the unique code. In some cases, the consumer ID is the same as the unique code. The consumer is prompted for his PIN, which he enters at a keypad. The reader 112 receives 330 the entered PIN.

[0059] The reader 112 also receives 340 the payment transaction data. This payment transaction data includes a payment amount, and optionally includes descriptions of the products or services paid for by the transaction. The payment transaction data can be transmitted to the reader 112 from an electronic point of sale system. The reader 112 may confirm the payment transaction data with the consumer before submitting it to the service center 120.

[0060] The reader 112 sends 350 its reader ID, the consumer ID, the payment transaction data, and the PIN (or other consumer authentication data) to the transaction module 124 through the network 130 and the interface module 122. Because this transmitted data is sensitive information, communications between the reader 112 and service center 120 preferably occur over a secure communications channel. For example, the reader 112 can encrypt the data before sending 350 it to the transaction module 124.

[0061] The transaction module 124 validates 360 a consumer payment account identified by the consumer ID, confirming for example that the account is still valid and the payment amount is not over the account limit. The transaction module 124 may also determine the consumer's standing based on the consumer's past payment transactions and make appropriate responses.

[0062] Transaction module 124 also authenticates 370 the consumer based on the received PIN. The module 124 compares the received PIN with the PIN stored in the consumer profile identified by the consumer ID. If the two PINs match, the consumer is authenticated.

[0063] Similarly, the transaction module 126 can validate the reader ID and merchant account.

[0064] Subject to proper validation 360 of the consumer account and authentication 370 of the consumer (and validation of the merchant account if that step is also taken), the transaction module 124 provides 380 the relevant payment transaction data (e.g., consumer account, merchant account, payment amount) to the payment module 126. The payment module 126 settles the payment transaction by submitting 382 the consumer account, the merchant account, and the payment amount to the payment processing network 160.

[0065] After the payment module 126 receives a confirmation that the payment transaction is authorized from the payment processing network 160, the transaction module 124 sends 390 a confirmation to the reader 112. The reader 112 sends a transaction-approval message to the point of sale, which finishes the payment transaction by printing a receipt for the consumer. If the transaction is not authorized by the payment processing network 160, the transaction module 124 sends a negative response to the reader 112.

[0066] The transaction module 124 can also send 395 a separate confirmation to the handheld electronic device 114 via the wireless network 140, for example a text message to the mobile phone stating that the transaction has been approved. Optionally, the transaction module 124 can also store the payment transaction data in database 125, and can then provide the payment transaction history to the consumer upon demand.

[0067] In one implementation, the payment processing network 160 is the ACH network. In this case, each transaction results in an ACH entry that includes the consumer account, the merchant account, and the payment amount. The ACH entries are aggregated. Periodically, a batch processing request is sent to the ACH network for debiting consumer accounts and crediting merchant accounts. The service center may also debit the merchant account (or consumer account, depending on who pays the transaction fee) and credit its own account for the transaction fee. The ACH entries are sent over the ACH network to an Originating Depository Financial Institution (ODFI), who can be any financial institution who does ACH origination. The ODFI deducts the payment amount from the consumer account, and sends the ACH entry to an ACH Operator (usually the Federal Reserve) and is passed on to a Receiving Depository Financial Institution (RDFI), where the merchant account is issued a credit of the payment amount.

[0068] Figs. 2-3 are based on an example in which system 100 uses barcodes on mobile phones to enable payment transactions, for example on the ACH network. The system 100 is not limited to this example and can be used for many other purposes. The system 100 can

also be configured to provide relevant information and content to handheld electronic devices 140 upon the users' request.

[0069] Similar to the mobile phone based payment system described above, overall operation can typically be divided into a registration process and a transaction process. The details of implementation of the processes will depend on the specific application. The registration process can be similar as described above except, for example, users may not provide their payment account information and PIN if payments are not being made.

[0070] In a generic transaction process, assuming the unique code is a barcode image, the user displays the barcode on the device 114 and presents it to the barcode reader 112. The reader 112 determines the user ID (i.e., analogous to the consumer ID except that the user may not be a consumer) from the barcode and transmits the user ID and the reader ID to the service center 120. The service center 120 might retrieve the corresponding user profile and reader profile. The reader profile typically will either expressly or implicitly provide information about the user's location and intention, based on the location and other facts about the reader. For example, if the reader location is known, then the approximate location of the user is also known. The user profile may include information about the user's preferences. The service center 120 determines relevant content based on the user ID and reader ID and pushes the content to the device 114. The content provided can be static or a mobile web application page with which the user can interact via the device 114.

[0071] For example, a user waves his mobile phone 114 with barcode in front of a kiosk 112 located by the entrance to a theater. The service center 120 determines that the user probably intend to receive some information about movies shown on that theater, and pushes information about the five movies starting in the next 15 minutes at that particular theater to the mobile phone. If the reader 112 also implemented payment capability, the user could select a movie and authorize payment for the movie tickets using the mobile phone.

[0072] Fig. 4 is a flowchart illustrating one embodiment of a relevant content delivery process in accordance with the invention. In this example, a consumer with a provisioned mobile phone 114 would like to obtain "relevant" content based on his current context. The consumer receives the content using a modified version of system 100. In the modified version, the payment module 126 is not required if no payments are being made. An additional content module 127 (not shown in Fig. 1) is used to determine the relevant content.

[0073] The consumer uses the device 114 to present the unique code, which is acquired 420 by the reader 112. The reader 112 determines 422 the consumer ID corresponding to the unique code. In some cases, the consumer ID is the same as the unique code. The reader 112

sends 450 its reader ID and the consumer ID to the transaction module 124 through the network 130 and the interface module 122. Because this transmitted data is sensitive information, communications between the reader 112 and service center 120 preferably occur over a secure communications channel. For example, the reader 112 can encrypt the data before sending 450 it to the transaction module 124.

[0074] The transaction module 124 validates 460 a consumer account identified by the consumer ID. In this case, the relevant consumer account may be the consumer's account with the service center, rather than an independent payment account. The transaction module 124 determines 470 consumer context data based on the consumer account and the reader ID. For example, the reader ID may provide information about the consumer's locality (e.g., facing the entrance to a movie theater) and/or intention (e.g., would like to see a movie). The consumer account may provide information about the consumer's preferences (e.g., prefers R-rated action movies over G-rated animation), which may be entered directly by the consumer or determined indirectly by analysis of the consumer's past behavior, for example.

[0075] Subject to proper validation 460 of the consumer account, the transaction module 124 provides 480 the relevant consumer context data (which may be just the reader ID and consumer ID) to the content module 127. The content module 127 determines 482 the relevant content (e.g., a listing of movies that will start in the next 30 minutes, with the R-rated action movies listed before the G-rated animation). This content is sent 495 back to the transaction module, for further transmission to 496, 497 to the reader 112 and/or device 114 for display to the consumer. Note that the content may be transmitted between devices by sending tags, pointers or other identifiers, rather than sending the actual content itself.

[0076] Additional transactions may occur. For example, the consumer may purchase tickets to one of the listed movies (e.g., using the process of Fig. 3). Alternately, the consumer may select a follow-up action, such as requesting a list of other movie theaters within 30 minutes driving (if the consumer does not like any of the listed movies) or a list of restaurants in the local vicinity (if the consumer has decided to eat dinner first).

[0077] Note that the transaction module 124 and content module 127 can be implemented in a distributed fashion by multiple entities and/or interact with other modules or databases operated by other entities. Consider an example where the consumer is in a grocery store and readers are located at different points in the grocery store. The service center may be able to determine only that a specific reader is part of the grocer's account but may not be able to determine the exact location within the grocery store. Instead, the transaction module 124 might send the reader ID to an outside database (e.g., the grocer's backend system), which

returns the product displayed at that location as being Tropicana Juice. Similarly, the service center may not have complete profile information for the consumer. Instead, the transaction module 124 might send the consumer ID (or some other identification for the consumer) to a third party, such as a merchant POS data warehouse, which returns the consumer's relevant purchase history. The content module 127 uses this information to decide to send a marketing promotional message with a discount for the Calcium Fortified version of Tropicana Juice (women in 50's who has prior purchases of calcium supplements) or for the 12-Pack of 12 oz pkgs for lunches (women in 30's with purchasing history of competing Ocean Spray and JuiceBox lunch drink products for children).

[0078] Once a unique consumer ID has been established for a consumer via the provisioning process and the establishment of an account with the service center, a large number of transactions can be enabled. These include various types of payment; implementation and management of loyalty programs; in-store and out-of-store messaging; promotions; print, broadcast, and internet advertising; and the tracking of a consumer's purchase activity across stores. This approach to mobile identity can be used to bring together the various elements of the customer experience by establishing a single identity for each consumer (based on the consumer ID and unique code), thus reducing their ID requirements for a broad range of services to just their phone (or, more generally, to just their handheld electronic device).

[0079] The same consumer ID can also be used for transactions using other devices, for example purchases made over the Internet from a wired desktop computer. Alternately, devices can be provisioned with the unique code using a communications media other than wireless or cellular access. As one example, iPods can be provisioned with the unique code when they are synced with a computer connected to the Internet.

[0080] All of the information associated with a particular consumer ID, be it payment credentials, loyalty status, purchase history, or demographic information, can be stored on servers at the service center and is associated with a given consumer via their mobile phone. When a customer swipes their phone, information about the location and purpose of that device comes together with information about that customer to perform a payment transaction, a coupon redemption, an information push, a update of the person's profile and/or all the above.

[0081] Loyalty programs are one example. Loyalty programs are established by merchants primarily to help them identify and reward their best customers. Existing programs suffer from a number of problems, including the difficulty of registering the

customer, the requirement that the customer carry a program specific identity in the form of a card or a key fob, and the inefficiency of capturing and recording separate payment and loyalty information from the customer. Though all customers must pay, because of these problems, a much lower percentage of customers participate in loyalty programs.

[0082] The approach described above can solve these problems by using the phone for both payment and loyalty. Customers who sign up for a loyalty program do not need to carry anything additional to enjoy the benefits of loyalty participation. When the customer presents his phone for payment, the service center is able to determine that he is a member of that merchant's loyalty program and his account is automatically adjusted to reflect the current purchase. If he is eligible for a reward, that information can be presented on the payment terminal and the customer can decide whether or not he wants to redeem it. In any case, the customer automatically accrues benefits that he is entitled to based upon the current purchase. Typically, this will be done when the consumer pays for the purchases using the mobile phone and unique code, but this is not required. There may be situations where the service center tracks a consumer's loyalty status, though he uses a different payment option. Signing up for additional loyalty programs becomes simple, because the customer need only swipe his phone across a reader at the new merchant, and he can be asked if he wants to join the program. This can be configured such that the consumer is only asked the first time. Alternately, he can be asked more times.

[0083] A merchant's existing loyalty program can be implemented on the platform described above. Alternately, a new loyalty program can be established. Additionally, because the same "token" (phone) is used across all merchants, cross-store programs or general purpose (e.g. point system) loyalty programs can also be implemented. Because the "token" has wireless connectivity, more advanced functions, such as notification to the consumer of his current loyalty status, or one time or limited time member only offers can be automatically transmitted to the consumer in real time.

[0084] For merchants, advantages include greater loyalty participation; automatic, real-time tracking of program status; and more accurate information. For consumers, it is easier to participate in the programs and therefore easier to garner the rewards.

[0085] Out of store promotion/messaging can also be supported by this platform. Merchants can use a range of promotions, including coupons and direct mail. These programs are established to increase store visits and increase the dollars spent during a given visit. The redemption rate of coupons and direct mail promotions are typically low because of poor targeting, the lack of differentiation between programs, and the difficulties in

redemption. For example, a consumer who is mailed a coupon must notice it in a sea of like solicitations, they must be interested in what is offered, and they must remember to bring the coupon to the store to redeem it.

[0086] The approach described above can solve these problems by sending notice of the promotion directly to a consumer's phone via SMS or MMS. Then, when the phone is used for payment, the redemption is automatic. This can be achieved by noting in the service center database that this person is entitled to a given benefit. A message describing the benefit and conditions (locations, time limits, etc) is sent to the customer. When the customer comes into the store and purchases the advertised item (for example), he automatically receives the benefit.

[0087] Using this capability, merchants can target down to the individual customer level. Because this is a new channel for consumers, they are more likely to notice it. In addition, because they do not need to do anything to enjoy the benefits (no coupon clipping, no carrying something extra with them, etc), they are more likely to redeem the benefit.

[0088] For merchants, this means more targeted, lower cost programs with higher conversion rates. It also means that the time between program conception and an increase in customers coming into the store is reduced. (i.e. it tightens up the promotion loop at a lower cost). For consumers, they get more promotions that they are interested in, the consumers are always "carrying" the promotions with them, redemption is automatic and they enjoy the promotion benefits.

[0089] A variation of this type of program is that the promotion could be initiated by the manufactures that supply to the merchants rather than by the merchants themselves. So, for example, a manufacture of soft drinks could send a two for one promotion to a number of consumers in a given area, which they could redeem if they buy the soda within a set number of days at a given merchant. This would drive a large number of customers into that merchant's store.

[0090] In store promotion/messaging can also be supported. Similar to the out of store promotions described above, if a consumer presents his phone to a reader in the store prior to check out, promotions based upon his profile can be sent to him while he is still in the store. These can be restricted to use during a very limited time (e.g. while the customer is still in the store) and they can be automatically redeemed upon check out. The customer gets the benefit of the promotion. The merchant gets a larger dollar sale and improves the customer experience.

[0091] Business intelligence can also be supported. Many merchants and consumer goods manufactures spend significant time and money to sort through their inventory, payment and loyalty data to better understand who is buying what, when and why. Historically, this related date is gleaned from separate sources resulting in a fragmented and incomplete picture of the consumers' behavior. For example, from POS data, merchants typically know what items are selling and when, but they do not know to whom. Similarly, from loyalty data, merchants might know customer spending levels, but not what those dollars were spent on. In addition, it is nearly impossible for a merchant to determine what the consumers' spending habits are outside of the merchant's own sales to the consumer.

[0092] However, because consumers who use the system described above can have a single unique identity across merchants and transaction types (purchases, loyalty, etc), a more holistic view of a given consumer and his behavior can be constructed. Though this data will typically only be shared on an aggregate basis, it will be of higher value in that it will incorporate purchase and loyalty information, response rates to promotions, and advertisements across a wider set of customer transactions. For example, it would be possible for a grocer to learn that a large number of his customers who do not buy meat in fact buy it at a competitor's, and that a significant number of them are responsive to print advertising but not broadcast advertising.

[0093] This platform can also be used to "close the loop" on print, broadcast, and internet advertising. For example, a print ad could have a promotion code associated with it (e.g. a number printed on the ad) which the customer sends to the service center via SMS (or they could e-mail it if it is an online ad). The service center would know who it came from based upon the phone number (or the e-mail address). The service center database would store the item the consumer is interested in and the benefit that he is entitled to at that merchant based upon the advertisement. When the customer then purchases the item or service in the store, he automatically gets the benefit. This could be extended such that the consumer in fact also authorizes payment for the item or service and the merchant either sends it to the consumer, or he can pick it up but it is already paid for. It would also be possible for the consumer to forward the promotional code to someone else for them to use. This allows merchants to determine which ads are driving traffic into their stores and which are not.

[0094] Finally, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes, and may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the

disclosure of the present invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the claims.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 768 of 1360

WHAT IS CLAIMED IS:

1. A method for carrying out a payment transaction using a handheld electronic device operated by a consumer, the method comprising:

receiving a consumer ID from a remotely located reader, the consumer ID corresponding to a unique code that is acquired by the reader from the handheld electronic device, wherein the unique code is not native to the handheld electronic device;

receiving payment transaction data from the reader;

validating a consumer payment account identified by the consumer ID; and

subject to validation of the consumer payment account, submitting the payment transaction data and an identity of the consumer payment account to a payment processing network for settlement.

2. The method of claim 1, wherein the payment processing network comprises the ACH network.

3. The method of claim 1, further comprising:

receiving consumer authentication data from the reader, the consumer authentication data acquired by the reader from the consumer;

authenticating the consumer based on the consumer authentication data; and

wherein the step of submitting the payment transaction data is further subject to the authentication of the consumer.

4. The method of claim 1, further comprising:

receiving a reader ID from the reader; and

validating a merchant account identified by the reader ID; and

wherein the step of transmitting comprises, subject to validation of the consumer payment account and the merchant account, transmitting the payment transaction data, the identity of the consumer payment account and an identity of the merchant account to the payment processing network for settlement between the consumer payment account and the merchant account.

5. The method of claim 1, further comprising, before carrying out any of the other steps:

associating an existing consumer payment account with the handheld electronic device; and

provisioning the handheld electronic device with the unique code.

6. The method of claim 5 wherein the step of provisioning the handheld electronic device comprises:

transferring digital code data corresponding to the unique code to the handheld electronic device for storage on the handheld electronic device, wherein the handheld electronic device presents the unique code to the reader for acquisition based on the stored digital code data.

7. The method of claim 6, wherein the handheld electronic device is provisioned with the unique code by transferring the digital code data to the handheld electronic device and without altering software or hardware of the handheld electronic device.

8. The method of claim 6, wherein the handheld electronic device comprises a mobile phone handset and the mobile phone handset is provisioned with the unique code by downloading the digital code data over a wireless network connection to the mobile phone handset.

9. The method of claim 5 further comprising:

upon request by the consumer via a handheld electronic device, web site or phone call, re-provisioning the handheld electronic device with the unique code.

10. The method of claim 1, wherein the steps of receiving a consumer ID, payment transaction data and consumer authentication data from the reader occur over a secure communications channel.

11. The method of claim 1, wherein the unique code comprises an image and the reader optically reads the image displayed on the handheld electronic device.

12. The method of claim 1, wherein the unique code comprises a barcode and the reader optically reads the barcode displayed on the handheld electronic device.

13. The method of claim 1, wherein the unique code comprises an alphanumeric string and the reader optically reads the alphanumeric string displayed on the handheld electronic device.

14. The method of claim 1, wherein the unique code comprises an audible sound and the reader aurally acquires the audible sound generated by the handheld electronic device.

15. The method of claim 1, wherein the unique code comprises a ringtone and the reader aurally acquires the ringtone generated by the handheld electronic device.

16. The method of claim 1, wherein the reader comprises a point-of-sale device.

17. The method of claim 1, wherein the reader comprises a kiosk.

18. The method of claim 1, wherein the handheld electronic device comprises a mobile phone handset.

19. The method of claim 1, wherein the handheld electronic device comprises a portable, wireless handheld data device.

20. The method of claim 1, wherein the payment transaction data comprises a payment amount.

21. The method of claim 1, wherein the consumer authentication data comprises a PIN (personal identification number) entered by the consumer, and the step of authenticating the consumer comprises authenticating the consumer based on the entered PIN.

22. The method of claim 1, wherein the payment processing network comprises a debit card network.

23. The method of claim 1, wherein the payment processing network comprises a credit card network.

24. The method of claim 1, wherein the step of receiving payment transaction data from the reader occurs after the payment transaction data is confirmed by the reader to the consumer.

25. The method of claim 1, further comprising:

subject to successful settlement of the payment transaction data, transmitting a confirmation message to the reader; and

subject to unsuccessful settlement of the payment transaction data, transmitting a notification message to the reader.

26. The method of claim 1, further comprising:

receiving consumer authentication data from the reader, the consumer authentication data acquired by the reader from the consumer;

authenticating the consumer based on the consumer authentication data, wherein the step of submitting the payment transaction data is further subject to the authentication of the consumer; and

subject to successful authentication of the consumer, transmitting a confirmation message to the reader; and

subject to unsuccessful authentication of the consumer, transmitting a notification message to the reader.

27. The method of claim 1, further comprising:

subject to successful settlement of the payment transaction data, transmitting a confirmation message to the handheld electronic device via a communications channel different from a communications channel used to communicate with the reader; and

subject to unsuccessful settlement of the payment transaction data, transmitting a notification message to the handheld electronic device via said different communications channel.

28. The method of claim 1, wherein the handheld electronic device comprises a mobile phone handset, and the mobile phone handset is provisioned with the unique code by downloading digital code data corresponding to the unique code over a wireless network connection to the mobile phone handset without altering software or hardware of the mobile phone handset.

29. The method of claim 28, wherein the unique code comprises a barcode, and the reader optically reads the barcode displayed on the handset.

30. The method of claim 28, wherein the payment processing network comprises the ACH network, the payment transaction data comprises a payment amount, and the step of transmitting payment transaction data comprises submitting a debit transaction for the payment amount from the consumer payment account to the ACH network.

31. The method of claim 30, wherein the consumer authentication data comprises a PIN entered by the consumer, and the step of authenticating the consumer comprises authenticating the consumer based on the entered PIN.

32. The method of claim 28, wherein the payment processing network comprises a debit card and/or credit card network, the payment transaction data comprises a payment amount, and the step of transmitting payment transaction data comprises submitting a debit transaction for the payment amount from the consumer payment account to the debit card and/or credit card network.

33. A method for providing content to a handheld electronic device operated by a user, the method comprising:

receiving a user ID from a remotely located reader, the user ID corresponding to a unique code that is acquired by the reader from the handheld electronic device, wherein the unique code is not native to the handheld electronic device;

receiving a reader ID from the reader;

determining content based on the user ID and the reader ID; and

transmitting the content to the handheld electronic device and/or the reader.

34. The method of claim 33, further comprising, before carrying out any of the other steps:

transferring digital code data corresponding to the unique code to the handheld electronic device and without altering software or hardware of the handheld

electronic device, the digital code data to be stored on the handheld electronic device, wherein the handheld electronic device presents the unique code to the reader for acquisition based on the stored digital code data.

35. The method of claim 34, wherein the handheld electronic device comprises a mobile phone handset and the mobile phone handset is provisioned with the unique code by downloading the digital code data over a wireless network connection to the mobile phone handset.

36. The method of claim 33, wherein the unique code comprises an image and the reader optically reads the image displayed on the handheld electronic device.

37. A method for providing relevant content to a handheld electronic device operated by a user, the method comprising:.

receiving a user ID from a remotely located reader, the user ID corresponding to a unique code that is acquired by the reader from the handheld electronic device, wherein the unique code is not native to the handheld electronic device;

receiving a reader ID from the reader;

determining relevant content for a context based on the user ID and the reader ID; and

transmitting the relevant content to the handheld electronic device and/or to the reader.

38. A system for carrying out payment transactions using handheld electronic devices, comprising:

an interface module for:

receiving a consumer ID from a remotely located reader, the consumer ID corresponding to a unique code that is acquired by the reader from the handheld electronic device, wherein the unique code is not native to the handheld electronic device; and

receiving payment transaction data from the reader;

a transaction module in communication with the interface module for validating a consumer payment account identified by the consumer ID; and

a payment module in communication with the transaction module for, subject to validation of the consumer payment account, transmitting the payment transaction data and an identity of the consumer payment account to a payment processing network for settlement.

39. The system of claim 38 wherein:

the interface module is further for receiving consumer authentication data from the reader, the consumer authentication data acquired by the reader from the consumer;

the transaction module is further for authenticating the consumer based on the consumer authentication data; and

the payment module transmits the payment transaction data and an identity of the consumer payment account to a payment processing network further subject to authentication of the consumer.

40. The system of claim 38, further comprising:

a registration module in communication with the interface module, for:

associating an existing consumer payment account with the handheld electronic device; and

causing the interface module to provision the handheld electronic device with the unique code.

41. A computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism including:

instructions for receiving a consumer ID from a remotely located reader, the consumer ID corresponding to a unique code that is acquired by the reader from the handheld electronic device, wherein the unique code is not native to the handheld electronic device;

instructions for receiving payment transaction data from the reader;

instructions for receiving consumer authentication data from the reader, the consumer authentication data acquired by the reader from the consumer;

instructions for validating a consumer payment account identified by the consumer ID;

instructions for authenticating the consumer based on the consumer authentication data; and

instructions for, subject to validation of the consumer payment account and authentication of the consumer, transmitting the payment transaction data and an identity of the consumer payment account to a payment processing network for settlement.

100
110
110
110
Reader
112
Handheld
Electronic
Device
114
Network
130
Wireless Internet
Gateway
150
Wireless
Network
140
Interface
Module
122
Transaction
Module
124
120
Data
Records
125
Payment
Module
126
Registration
Module
128
Payment
Processing
Network
160

FIG. 1

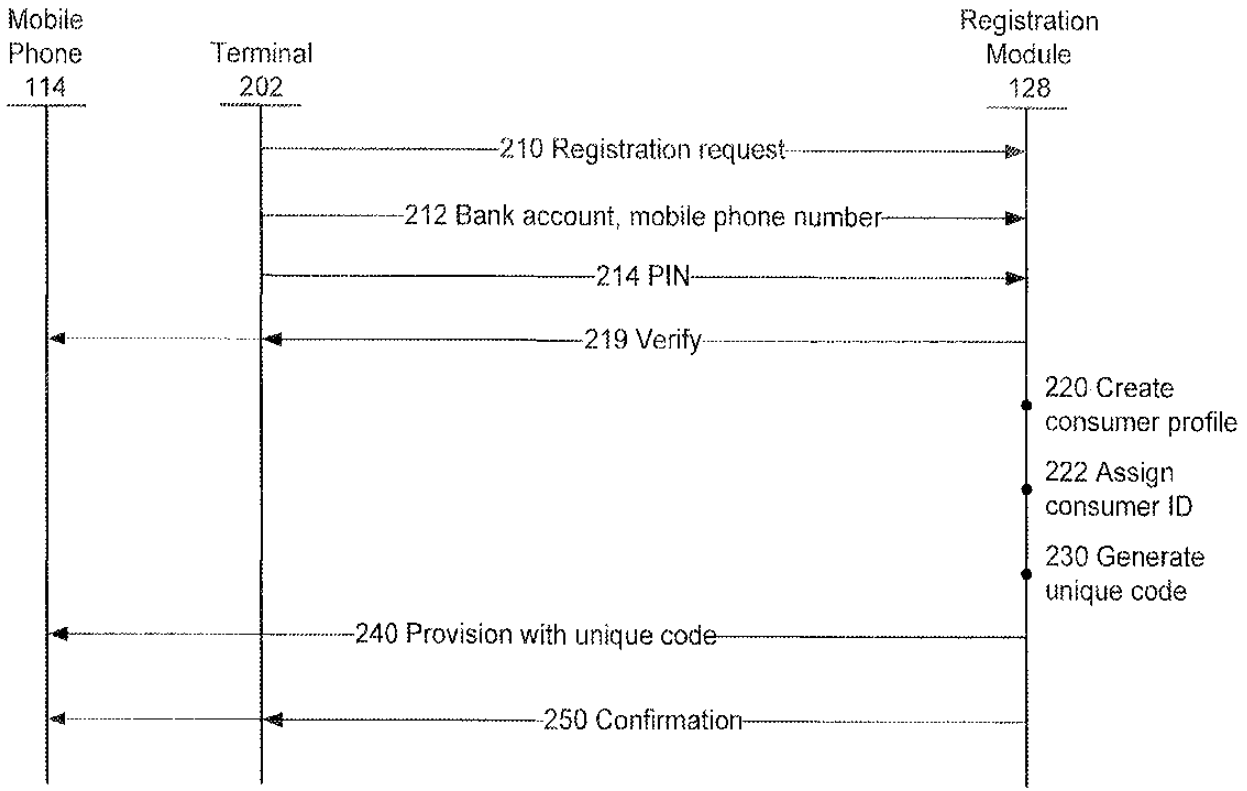


FIG. 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 776 of 1360

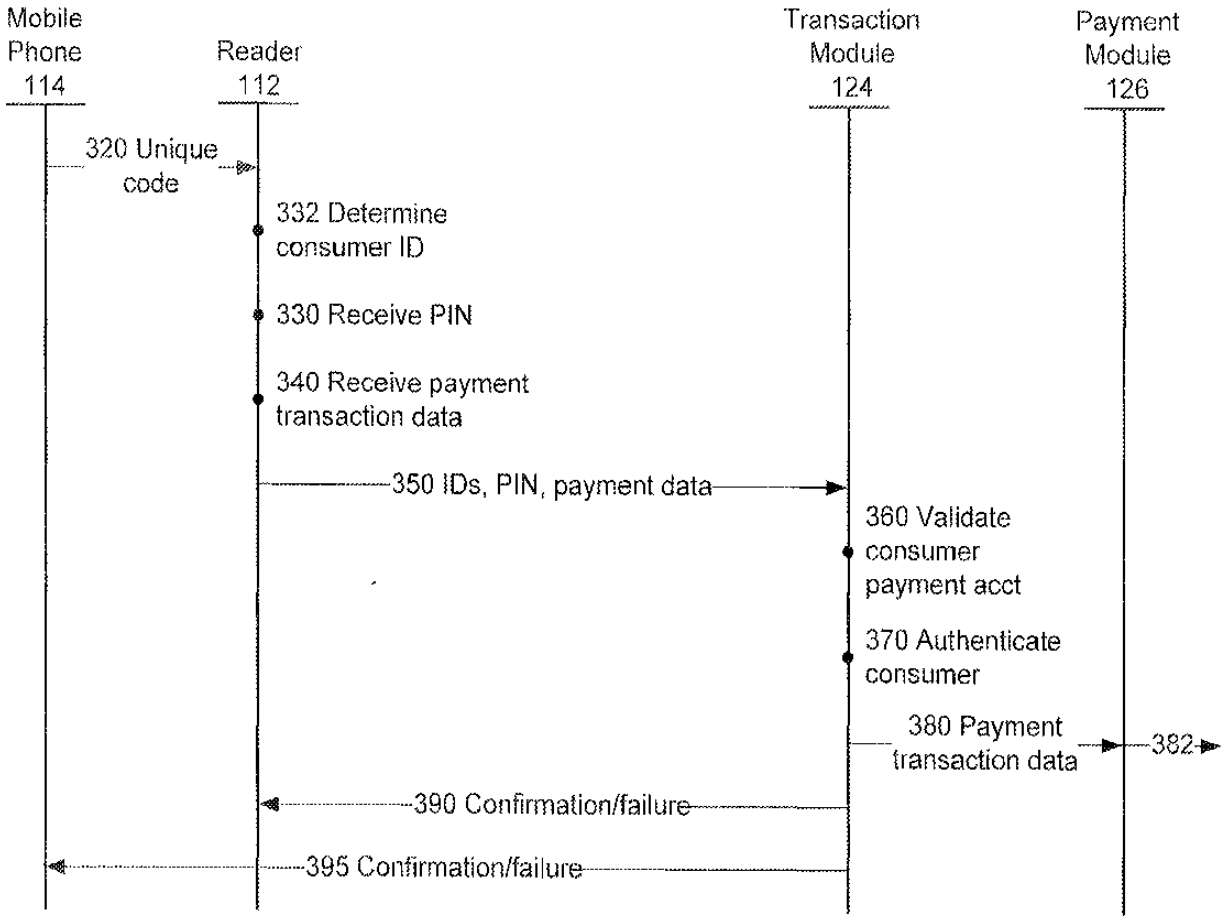


FIG. 3

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 777 of 1360

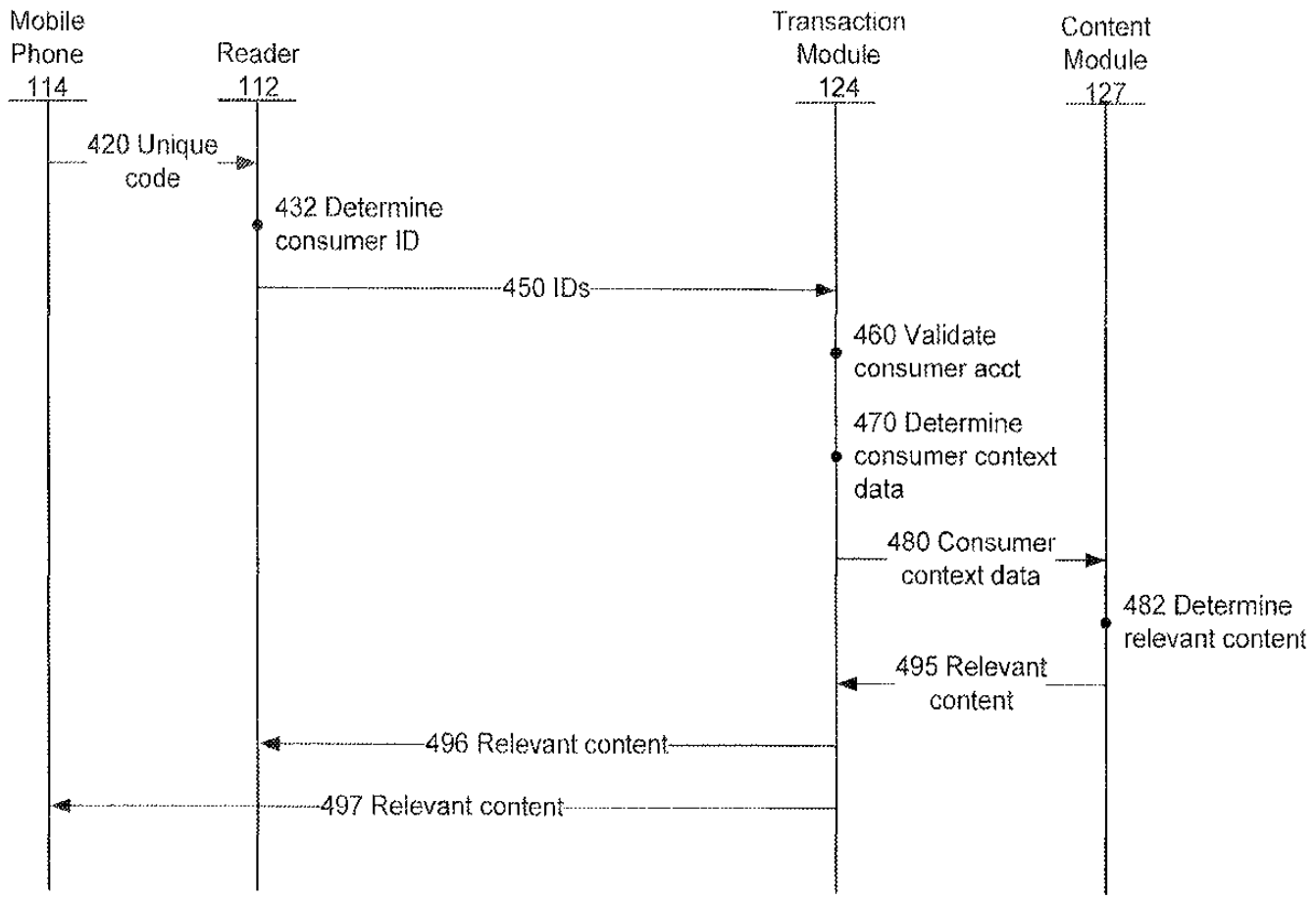


FIG. 4

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 778 of 1360

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2666616 A1 2008/04/24

(21) 2 666 616

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2007/10/19
(87) Date publication PCT/PCT Publication Date: 2008/04/24
(85) Entrée phase nationale/National Entry: 2009/04/15
(86) N° demande PCT/PCT Application No.: AU 2007/001599
(87) N° publication PCT/PCT Publication No.: 2008/046161
(30) Priorité/Priority: 2006/10/19 (AU2006905829)

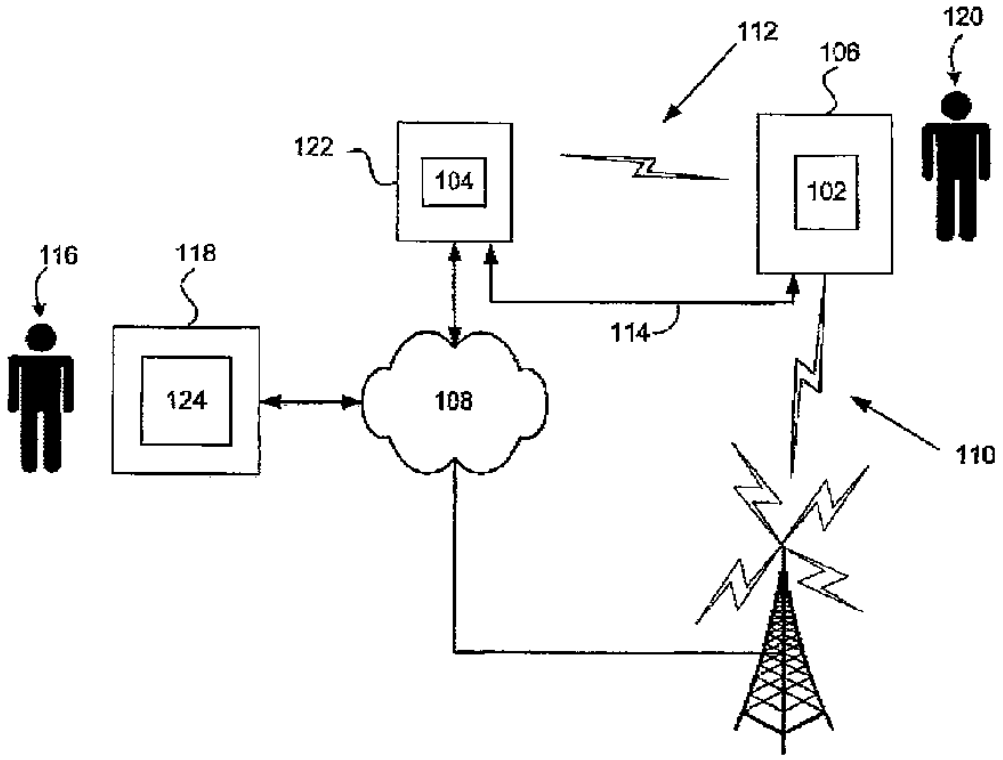
(51) Cl.Int./Int.Cl. *H04W 4/12* (2009.01), *H04W 12/02* (2009.01), *H04W 12/06* (2009.01)

(71) Demandeur/Applicant:
FRUITFUL TECHNOLOGIES PTY LTD, AU

(72) Inventeur/Inventor:
NGO, DUC ANH, AU

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : SYSTEME ET PROCEDE INTERACTIFS
(54) Title: AN INTERACTIVE SYSTEM AND PROCESS



(57) Abrégé/Abstract:
A method of delivering an instruction (206) to a mobile user device (106) connected to a network (110) is disclosed. The method comprising the steps of receiving an interactive workflow (202), translating the interactive workflow into the instruction (206) in a form executable by the mobile user device (106), and sending a message (208) including the instruction (206) to the mobile user device (106).

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 779 of 1360

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2008 (24.04.2008)

PCT

(10) International Publication Number
WO 2008/046161 A1

(51) International Patent Classification:
H04Q 7/22 (2006.01) *H04M 3/493* (2006.01)

(21) International Application Number:
PCT/AU2007/001599

(22) International Filing Date: 19 October 2007 (19.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2006905829 19 October 2006 (19.10.2006) AU

(71) Applicant *(for all designated States except US)*: **DELOITTE SERVICES PTY LTD** [AU/AU]; Level 1, 225 George Street, Sydney, NSW 2000 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **NGO, Duc, Anh** [/AU]; 2/9 Fabian Court, Maribyrnong, VIC 3032 (AU).

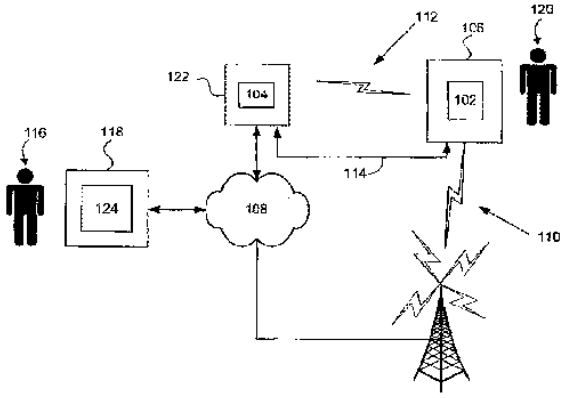
(74) Agent: **BLAKE DAWSON WALDRON PATENT SERVICES**; Level 35, Grosvenor Place, 225 George Street, Sydney, NSW 2000 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) Title: AN INTERACTIVE SYSTEM AND PROCESS



(57) Abstract: A method of delivering an instruction (206) to a mobile user device (106) connected to a network (110) is disclosed. The method comprising the steps of receiving an interactive workflow (202), translating the interactive workflow into the instruction (206) in a form executable by the mobile user device (106), and sending a message (208) including the instruction (206) to the mobile user device (106).

WO 2008/046161 A1

AN INTERACTIVE SYSTEM AND PROCESS

FIELD OF THE INVENTION

The present invention relates generally to a method of delivering an instruction to a mobile user device connected to a network.

BACKGROUND

Amongst the wide variety of portable electronic devices available today, mobile phones have become particularly pervasive, with more than double the penetration of the Internet. These devices have rapidly advanced in capability and can do far more than Voice and SMS. Using these capabilities to deliver and execute applications that provide customisable interactivity to mobile phones and other devices is highly desirable but continues to be a challenging endeavour due the varied types of largely incompatible devices and platforms on the market.

Most interactive applications for mobile phones involve either Short Message Service (SMS) or the development of dedicated applications that address specific business requirements. SMS interactivity suffers from poor usability (the user has to be familiar with idiosyncratic commands) and security issues (SMS source addresses can be faked), thus limiting their usage to simple, non-sensitive transactions. Furthermore, an organisation wishing to use SMS to interact with its customers needs to come to some commercial arrangement with the telecommunications provider in order to establish billing procedures and so on. This can be inconvenient for the organisation, and may also be quite expensive, both to set up and also to operate on an on-going basis.

The dedicated applications are an attempt to address these shortcomings by developing programming code that is executed by the mobile device to perform a specific task. This involves significant amounts of time, at least because mobile phones from different manufacturers are not usually binary compatible and cannot execute the same executable applications. Additionally, these applications are limited to the functionality required at the time of development, and thus may not support additions or modifications to that functionality. As can be appreciated, distributing changes to these applications is similarly quite a tedious process, typically requiring the user to manually download and install an updated version of the application on their telephone.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 781 of 1360

SUMMARY OF THE INVENTION

According to one aspect of the invention there is provided a method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

According to another aspect of the invention there is provided a method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

According to yet another aspect of the invention there is provided computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

Preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language. More preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

Preferably the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device. More preferably the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 782 of 1360

step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

Preferably the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

Preferably the step of translating the interactive workflow includes tailoring the instruction to the specification.

Preferably the step of translating the interactive workflow includes tailoring the instruction to a device operating system.

Preferably the step of sending the message includes the step of sending a unique message identifier. More preferably the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

Preferably the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network. More preferably the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS. Alternatively, the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

Preferably the method further comprises the step of the mobile user device receiving the set of instructions and the unique message identifier. More preferably the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

Preferably the method further comprises the step of receiving a response to the instruction from the mobile user device. More preferably the step of receiving a response includes the step of receiving a response identifier from the device. Even more preferably the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 783 of 1360

Preferably the method includes the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow from the external or third party. More preferably the method includes the step of sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow from the external or third party.

Preferably the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface from the external or third party. More preferably the step of receiving a request for an Application Programming Interface is received from the external or third party. Even more preferably the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

Preferably the method also comprises the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

In accordance with the present invention, there is also provided an interactive process executed by a computer system or device, the process including:

receiving one or more SMS messages including instruction data representing one or more instructions for execution on said system or device to determine information;

executing said one or more instructions to determine said information; and

sending one or more SMS messages including response data representing said information.

Advantageously, said information may include system information determined from said system or device and/or user information determined from a user of said system or device.

Preferably, said execution causes generation of an interactive user interface on a display of said system or device, and the process includes receiving response data representing said information from a user of said system or device in response to said interactive display.

Preferably, said one or more instructions are executed by a virtual machine of said system or device.

The present invention also provides an application component for a system or device, the applicationcomponent including:

a message receiver for processing one or more received SMS messages to generate one or more instructions for execution on said device to determine information;

an execution component for executing said one or more instructions of said application data to determine said information; and

a message sender for generating one or more SMS messages including response data representing said information.

Preferably, the application component further includes a data management component for storing sets of instructions on non-volatile storage means and for retrieving a selected one of the stored sets of instructions for execution.

Preferably, said execution component is adapted to generate an interactive display for a user of said system or device, and to receive response data representing said information from a user of said system or device in response to said interactive display.

The present invention also provides an interactive process for execution by a system or device, including:

receiving message data including header data and encrypted payload data;

selecting one of a plurality of encryption keys on the basis of said header data; and

decrypting said payload data using the selected encryption key.

Preferably, said header data includes index data representing an index for said plurality of encryption keys.

Advantageously, said payload data may represent one or more instructions for execution on said system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions on a remote system or device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 785 of 1360

The present invention also provides an interactive process for execution by a system or device, including:

generating payload data for sending to a remote system or device;

selecting one of a plurality of encryption keys;

encrypting said payload data using the selected encryption key;

generating message data for sending to said remote system or device, said message data including header data and the encrypted payload data, wherein said header data includes data representing an index for said plurality of encryption keys to allow said remote system or device to determine the selected encryption key and thereby to decrypt said payload data.

Advantageously, said payload data may represent one or more instructions for execution on said remote system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions.

Preferably, the process includes generating said plurality of encryption keys and sending said plurality of encryption keys to said remote system or device.

Preferably, the process includes associating said plurality of encryption keys with an identifier of said remote system or device.

The present invention also provides an interactive process, including:

receiving programming instructions for generating an interactive display on a remote system or device;

compiling said programming instructions to generate compiled instruction data;

sending said compiled instruction data to said remote system or device to generate an interactive display on said second remote system or device;

receiving response data representing at least one user response to said interactive display; and

sending response data representing said at least one user response.

The present invention also provides an interactive process, including:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 786 of 1360

receiving workflow instructions from a plurality of entities;

processing said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

sending said interactive applications to said user devices for execution.

Preferably, said interactive applications are sent to said user devices using short message service (SMS).

Preferably, said user devices include mobile telephones.

The present invention also provides an interactive system for managing interaction with users of remote systems and/or devices, the interactive system being adapted to:

receive workflow instructions from a plurality of entities;

process said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

send said interactive applications to said user devices for execution.

The present invention also provides a system having components for executing any one of the above processes.

The present invention also provides a computer-readable storage medium having stored thereon program instructions for executing any one of the above processes.

The present invention also provides an interactive system, including:

a gateway component for processing received workflow data to generate instructions for generating an interactive display on a user device, the gateway component being adapted to send said instructions to said user device for execution; and

an execution component of said user device to receive and execute said instructions to generate said interactive display, to receive response data representing at least one response of said user to said interactive display; and to send said response data to said gateway component.

Preferably, said user device is a mobile telephone.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 787 of 1360

Advantageously, the instructions may be sent to said gateway component in one or more SMS messages.

Advantageously, said user response data may be sent to said user device in one or more SMS messages.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a schematic diagram of a preferred embodiment of an interactive system;

Figure 2 is a schematic diagram of the high level process and data flow of an interactive process of the interactive system;

Figure 3 is a block diagram of a mobile telephone on which a client application of the interactive system is installed;

Figure 4 is a block diagram of the client application of the interactive system;

Figure 5 is a flow diagram of the life cycle of an interactive application generated by the interactive process and system;

Figure 6 is a block diagram of an application gateway of the interactive system;

Figure 7 is a block diagram of a computer system on which the application gateway is installed;

Figure 8 is a schematic diagram of the process and data flow of an opt-in process of the interactive system;

Figure 9 is a schematic diagram illustrating the use of encryption key sets to establish an encrypted communications channel between the client application and the application gateway;

Figure 10 is a schematic diagram of the process and data flow involved in conducting secure communications between the client application and the application gateway;

Figure 11 is a schematic diagram illustrating the default behaviour of the interactive system and process whereby a particular application gateway transmits instructions to a particular client application, and the resulting response data is returned to the same application gateway that sent the instructions;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 788 of 1360

Figure 12 is a schematic diagram similar to that of Figure 11, but illustrating the redirection of response data to a different application gateway from the application gateway that sent the corresponding instructions;

Figure 13 is a schematic diagram illustrating the structure of messages exchanged between the application gateway and the client application;

Figure 14 is a schematic diagram illustrating the structure of payload data of the messages shown in Figure 13;

Figure 15 is a schematic diagram illustrating the structure of each data part of the payload data of Figure 14;

Figure 16 is a schematic diagram illustrating the fifteen different types of instructions supported by the interactive system and process;

Figure 17 is a schematic diagram illustrating the structure of an SMS message generated by the interactive system and process;

Figure 18 is a schematic diagram illustrating how the interactive system uses multiple SMS messages to transmit instructions constituting an application whose length is greater than 133 bytes;

Figure 19 is a flow diagram of an SMS transmission process of the system;

Figure 20 is a flow diagram of an SMS receiving process of the system;

Figure 21 is a flow diagram of an application execution process executed by the execution engine of the system;

Figure 22 is a schematic diagram illustrating the structure of response data sent from the client application to the application gateway;

Figure 23 is a schematic diagram illustrating how the system uses parameter names provided in instructions to label corresponding responses;

Figure 24 is a schematic diagram illustrating execution branching in the client application;

Figure 25 is a schematic diagram illustrating the use of branch domains to label responses having the same parameter name;

Figure 26 is a schematic diagram illustrating the use of a branch name stack to determine control flow;

Figure 27 is a schematic diagram illustrating the user interface components resulting from selecting different branches of an interactive application;

Figure 28 is a schematic diagram illustrating the inclusion of a 'back' button on each user interface display;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 789 of 1360

Figure 29 is a schematic diagram illustrating the use of an executed instruction stack to implement the 'back' button of Figure 28;

Figure 30 is a screen shot of a user interface of the application gateway for entering scripting language instructions and for submitting those instructions to an instruction compiler of the application gateway;

Figure 31 is a source code listing of a function illustrating how the system APIs can be used to send details of a booking to a mobile telephone for display to a user, and to receive the user's response indicating whether they user accepts or rejects the booking;

Figure 32 is a partial listing of a scripting language application, illustrating the use of control flow branches in the scripting language;

Figure 33 is a schematic diagram illustrating the user interface components generated from the scripting language example of Figure 32;

Figure 34 is a schematic diagram illustrating the use of nested user interface displays generated by the system;

Figures 35 and 36 are schematic diagrams illustrating the appearance and structure of general user interface displays generated by the system;

Figure 37 is a schematic illustration of a slider control display generated by the system;

Figure 38 is a schematic diagram illustrating the use of single and multiple selections in user interface displays generated by the system; and

Figure 39 is a schematic diagram illustrating how the branch names of nested menus are used to label parameter data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As shown in Figure 1, an interactive system includes at least one client application 102 and at least one application gateway 104. Each client application 102 is a component of a corresponding user device 106 that can communicate with the at least one application gateway 104 via one or more of a variety of communications means supported by the device 106, preferably including a combination of (i) an IP-based communications network 108 such as the Internet, (ii) a wireless wide-area communications network such as the global system for mobiles (GSM) telephone network, (iii) a local wireless network or link between the device 106 and the at least one application gateway 104, such as an infra-red link, Wi-Fi or Bluetooth network 112, and/or (v) a direct cable connection 114

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 790 of 1360

using a standard communications protocol such as RS-232, universal serial bus (USB), or FireWire (IEEE 1394). The interactive system allows an application developer 116 using a standard computer system 118 to rapidly develop and deploy an interactive workflow or application for execution on one or more user devices 106 in order to interact with the users 120 of those devices 106, and to receive response data representing at least one response of each user 120 to the interactive application.

The interactive workflow or application includes a set of instructions for presenting information to a user 120 of each mobile device 106 in an interactive display or user interface, and for retrieving each user's response(s) to that information. Typically, the information presented to a user 120 will include one or more questions displayed on a display screen of the user's device 106 (and possibly also audio played on a sound transducer of the device 106), and each of the user's responses is provided by the user interacting with one or more user-interface (UI) components or input controls of the interactive display. Each response can be in the form of freeform text typed into a textbox, or the result of the user interacting with another type of input control, such as radio buttons, check boxes, sliders, simple menus, nested menus, and so on. To some extent, these possibilities are determined by the capabilities of the device 106. However, because the workflow supported by the system also includes control flow features similar to those provided by high-level programming languages, the workflow instructions generated by the system are also considered to constitute an interactive software application that is executed on the user device 106.

In the described embodiment, the user device 106 is a mobile telephone, but alternatively could be some other type of portable or handheld device such as a personal data assistant (PDA), and hence is also referred to hereinafter as "the mobile device 106". However, even though the device 106 is described as being "mobile" or "portable", it will be appreciated by those skilled in the art that the systems and processes described herein could alternatively be used in conjunction with other types of devices and systems that need not even be portable. For example, the client application 102 could even be installed on a standard personal computer system (rather than the portable device 106) in order to rapidly develop and deliver interactive applications to a standard personal computer, for example.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 791 of 1360

In the described embodiment, the client application 102 is a software application that is stored on the mobile device 106, either as part of the device manufacturing or configuration prior to sale, or subsequently deployed as required via GPRS, Bluetooth, Infrared or a phone specific channel (*e.g.*, a data cable), allowing it to be installed on a wide variety of different types of device. However, it will be apparent to those skilled in the art that the client application 102 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

Similarly, the application gateway 104 is a software application that is installed on and executed by a standard computer system 122, such an Intel™ IA-32 computer server executing a Windows™ operating system. The computer system 122 includes standard hardware components 702, and software components 704. The hardware components 702 include at least one processor 706, a communications interface (*e.g.*, network interface card) 708, random access memory 710, non-volatile (*e.g.*, hard disk storage) 712, user input device (*e.g.*, keyboard, mouse or other pointing device) 714, and a display adapter and device 716, all interconnected by a system bus 720. The software components 704 include the application gateway 104, and a standard operating system 718 such as Microsoft Windows. Additionally, a third party application 124, shown as being installed on the developer's computer 118, may additionally or alternatively be installed on the same computer system 122 on which the application gateway itself is located 104, as shown. However, although the application gateway 104 is described as being a software application, it will be apparent to those skilled in the art that the application gateway 104 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

The client application 102:

(i) verifies a set of instructions sent by the application gateway 104;
(ii) interprets these instructions;
(iii) interacts with the user device 106 and/or the user 120 in accordance with the set of instructions; and
(iv) sends responses back to the gateway 104 or other computer system or device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 792 of 1360

The application gateway 104 is effectively a backend component that:

(i) maintains a database of user devices of the interactive system (*i.e.*, devices on which the client application 102 has been installed);

(ii) generates and delivers interactive applications to the mobile device 106 via any one of a wide range of communication channels;

(iii) ensures the integrity and authenticity of outgoing and inbound messages to and from the mobile device 106; and

(iv) provides application programming interfaces (APIs) to allow third-party applications 124 to deploy an interactive application to the mobile device 106 and to receive corresponding responses generated by the client application 102 on the mobile device 106.

Figure 2 is a schematic diagram illustrating the high level operation of the interactive process of the system in relation to the various components shown in Figure 1. At step 202, an external or third-party application 204 executing on the developer's computer system 118 (or, alternatively, on the gateway computer system 122) calls an API 616 of the application gateway 104 to describe the workflow that the developers of the device 106 want to deploy. In general, the workflow includes the steps of displaying information to a user, and then retrieving at least one response to that information. For example, a typical workflow might be to display a message on the mobile device 106, ask the user to enter their age, then display another message, and send the age back to the developer. These steps or instructions constitute an interactive application for execution on the mobile device 106.

The workflow defines:

(i) one or more addresses of respective user devices 106;

(ii) the steps to be performed on the one or more user devices 106;

(iii) the address of an alternate gateway server (if any) 104 to which responses are to be sent; if no address is given, then the responses will be sent to the same gateway server 104 that sent the application instructions;

(iv) how the response data returned to the application gateway should be processed (*e.g.*, returned to the developer's application 124, sent to the developer 116 by email, stored in a file, etc.); and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 793 of 1360

(v) the communication method(s) that are to be used to send the instructions to the user device 106 and to receive the corresponding response data.

At step 206, the application gateway 104 transforms the workflow described by the developer into a compressed, encoded, and encrypted format for transmission to the mobile device 106. The application gateway 104 also inserts a unique identifier or ID into the message and stores data associating that ID with the destination (*e.g.*, phone number, or network address) to which the workflow is to be sent.

The application gateway 104 transforms the message so that it can be transmitted via the appropriate communication means. For example, if the message is to be transmitted via SMS, the application gateway 106 splits a large message into smaller messages to comply with the GSM standard. All this is hidden from the developer. At step 208, the application gateway 104 then transmits the message to the device 106 specified by the developer.

At step 210, the client application 102 receives, un-compresses and decrypts the message(s), thereby verifying their integrity. If valid, at step 212 the client application 102 interrupts the user and requests that they complete the workflow. With the user's cooperation, the client application 102 interprets each instruction and performs a corresponding operation *e.g.*, display a message, collect the user's age, etc. that in most cases involves interacting with the user of the device 106.

At the end of the workflow, the client application 102 sends back to the application gateway 104 all the collected response data via the response channel specified in the workflow instructions by the application gateway 104. For example, if the response is to be returned via SMS, a response SMS is sent back to a phone number provided in the initial message(s). The client application 102 also encrypts the response message(s) and includes the unique message ID to ensure authenticity of the response.

When the application gateway 104 receives the response message at step 216, it decrypts the message and determines whether the ID of the message is valid for the phone number it was received from, using the destination and ID association stored previously. If the message is valid, then it is processed as specified by the developer *e.g.*, passes it on to a third-party application, emails the developer, stores it in a file, etc.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 794 of 1360

In addition to the above, the interactive system also provides capabilities for (i) storing (and subsequently updating) a set of instructions as a permanent or semi-permanent application stored on non-volatile storage of the user device 106 for execution at any time; *i.e.*, the application persists on the user's device; (ii) the distribution of encryption keys; and (iii) opt-in mechanisms to ensure that the mobile device 106 is not sent unsolicited applications, *e.g.*, if the application gateway 104 is shared by multiple vendors.

The interactive system and the interactive process executed by the interactive system are described in detail below.

As shown in Figure 3, the mobile device 106 is a standard mobile phone including hardware components 302 and software components 304. The hardware components 302 include a processor 306, read-only memory 308, random-access memory 310, flash memory 312, user interface components including user input components 314 (*e.g.*, microphone, keyboard, and, in some devices, touch-screen), output components 316 (*e.g.*, display screen, speaker), and one or more communications interfaces 318 allowing the device 106 to communicate with a mobile phone network 110, and, in some devices, also Bluetooth and/or Wi-Fi local wireless networks or an infrared link 112. In the preferred case of the mobile device 106 being a telephone, the device 106 also includes a SIM card 320. The software components include an operating system 322 such as the closed, proprietary operating systems installed on mobile telephones sold under brands such as Nokia and Motorola, Java platform Micro-edition (Java ME) 324, and the client application 102. However, if the operating system 322 is a more sophisticated operating system such as Symbian, Linux, Microsoft SmartPhone, PocketPC, Windows CE, or Windows Mobile, that provides sufficiently powerful application programming interfaces (APIs), then the J2ME component 324 can be omitted. As shown in Figure 4, the client application 102 includes a message sender component 402, a message receiver component 404, user interface (UI) widgets 406, a workflow execution engine 408, instant data storage 410, and permanent data storage 412. The client application 102 is a native application that is executed by the mobile device 106. The client application 102 can be installed by any one of a number of means, including WAP push, IP data packets (GPRS or 3G networks), Bluetooth, Infrared, or a phone-specific channel such as a data cable. The

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 795 of 1360

client application 102 can be provided as a preinstalled application on the mobile phone 106 when purchased.

The message sender 608 sends response messages to the application gateway 104 in a format understood by the application gateway 104. It encrypts the message and includes ID provided with the initial application to confirm its authenticity.

The message receiver 606 decrypts and uncompresses instruction sets received from the application gateway 104. It implements message reception via a number of channels, including Bluetooth, Infrared, IP networks (GPRS or 3G), and SMS. The message receiver 606 also invokes the workflow execution engine 408 to process the instruction set.

The UI Widgets 406 are pre-built user interface components that instructions sent by the application gateway 104 can use to interact with the user.

The workflow execution engine 408 is responsible for running and maintaining state for the instructions currently being processed. It associates instructions with UI widgets as well as storing input from the device 106 and its user. It is also responsible for invoking the message sender 402 once the workflow is completed to initiate sending the response to the application gateway 104. The workflow execution can also be invoked by a timer if an instruction asks to be run at a specific time.

The client application 102 can simultaneously receive multiple workflow applications at any one time, and the instant data store 410 is effectively a first-in, first-out queue that stores these applications and processes them one by one until the instant data store 410 is empty.

The interactive system has the ability to make a sequence of instructions persistent on the mobile device 106 as an application. These sequences are identified by a unique label and are stored in the permanent data store 412, being in this embodiment the non-volatile flash memory 312. The application gateway 104 can issue commands to update or delete applications in the permanent data store 412.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 796 of 1360

Figure 5 is a flow diagram illustrating the life cycle of an execution instance of the client application 102 following receipt of an instruction from an application gateway 104. However, the client application 102 can be invoked at step 502 by either a new data event or a timer event. A new data event occurs when the client application 102 is activated by the mobile device 106 when new payload data addressed to the client application 102 is received. Timer events are set by a specific instruction that suspends execution of the instruction to a later date/time. The workflow engine 408 is responsible for scheduling the client application 102 to start and process the instruction set at that date/time.

Once invoked, at step 504 the instruction sequence is retrieved either reading data from the instant data store 410, in the case of a Timer event, or from the input channel in the case of a new data event. If the instruction data is retrieved from the input channel and is encrypted, at step 506 the client application 102 decrypts and verifies it as described below. If the data is valid, the workflow execution begins at step 508.

The workflow execution 508 processes the instructions step by step. This may or may not involve user interactions (as some instructions described in the Appendix can be handled without user interaction). Upon execution of a timer instruction specifying that execution should be postponed to a later time, further execution of instructions of the workflow application is suspended and the instruction set is stored placed in the instant data store 410 pending resumption at the specified time.

Once the workflow execution 508 is complete, the workflow application is removed from the instant data store 410. If the application is marked as persistent, the instruction set is saved to the permanent data store 412. The user can then invoke the instruction set at any time.

At step 510, the information collected by the workflow execution 508 is sent back to the application gateway 104 as response data. The client application 102 encrypts the response data in addition to including the unique message ID that verifies the authenticity of the response data.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 797 of 1360

As shown in Figure 6, the application gateway 104 includes an instruction compiler 602, a key manager 604, a message receiver 606, a message sender 608, an opt-in manager 610, persistent storage 612, and an application programming interface (API) 616.

The instruction compiler 602 translates workflow descriptions received from the developer 116 into a format that is optimized for delivery to and execution by the client application 102. The workflow description is written in a scripting language that is compiled by the instruction compiler 602. The developer can enter the workflow description directly into a text box and submit its contents to the compiler 602. This is typically used to rapidly prototype the look and feel of a workflow application. Alternatively, the workflow description can be submitted by making an API call to the compiler 602 from a high-level programming language such as C#, Java, or TCL, thus providing end-to-end application integration.

The message sender 608 encrypts the workflow instruction set. The encryption relies on requesting the key manager 604 to provide a random index and an encryption key that is specific to a particular user device 106 on which the instructions are to be executed. The index is sent in cleartext to the client application 102, which uses the index to look up the appropriate encryption key to decipher the message. The message sender 608 also generates a unique random identifier for the workflow application. The random identifier is a combination of a random identifier and an identifier of the party who sent the workflow description.

The message sender 608 uses the transport adapter 614 to deliver the actual message(s) containing the workflow application. The message sender 608 first checks with the Opt-in manager 610 to ensure that the client application 102 does not receive unsolicited applications which it has not opted into, as described below.

The transport adapter 614 abstracts the various methods of delivering an instruction set to the client application 102 on the mobile device 106. It uses device capability information stored in the persistent storage 612 to determine the capabilities of the device 106 and hence the best communication channel to deliver the message(s).

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 798 of 1360

The transport adapter 614 provides plug-in support for new channel types dynamically by providing a set of messaging APIs and by allowing dynamic loading of compiled code that implements a new messaging interface. If required, the transport adapter 614 reformats the instruction payload so that it can be delivered via a particular channel. In particular, an application delivered by SMS may have to be divided into two or more smaller messages due to SMS message size limitations.

The key manager 604 is responsible for generating, distributing and managing the encryption keys issued to the portable device 106, as described below. It also provides encryption and decryption facilities for the message sender 608 and the message receiver 606.

The opt-in manager 610 provides an opt-in, opt-out process to allow client applications 102 select the entities they are willing to receive instruction sets from. This is desirable because the application gateway 104 may be shared by multiple parties and the client application 102 will otherwise execute any received instruction set as long as it is valid. The opt-in manager 610 maintains in the persistent data store 612 associations between parties and the phone numbers (or, in the case of devices other than telephones, other form of address or identifier of the destination device) they are allowed to send applications to. The process for creating these associations can be dynamic to allow users to selectively block or allow instructions from particular parties. For example, Figure 8 shows the message flow for an opt-in process.

At step 802, a party uses the external application 124 executing on the computer system 118 to send a workflow description to the application gateway 104, which at step 804 compiles and formats the instructions in preparation for sending them to a client application 102 that has not opted in. At step 806, the message sender 608 first checks whether the client application 102 has opted in. If not, at step 808 it asks the opt-in manager 610 to determine the opt-in status for this party and this user device. At step 810, the opt-in manager 610 sends an opt-in request message to the user, asking whether they agree to receive applications from this party. If the response is yes, at step 812 the opt-in manager 610 stores this information in the persistent data store 612 and then at step 814 instructs the message sender 608 to send the instruction set at step 816. Otherwise, if the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 799 of 1360

response is no, then the message sender 608 fails and notifies the party at step 818 that the user has not opted in.

Alternatively, the opt-in process could be performed manually, for example, by using a form that enables the user to directly add entries to the persistent data store 612. Alternatively, an analogous process could be used to opt-out of receiving applications from a particular party.

The message receiver 606 receives messages from the client application 102 and communicates with the transport adapter 614 to receive responses via any of the supported transport channels and protocols, including GPRS, IP network, Bluetooth, and SMS. For example, the instruction set of the interactive system allows instructions to be received by one physical channel/protocol (*e.g.*, SMS), and a corresponding response to be delivered by another (*e.g.*, Bluetooth).

When a message is received, the message receiver 606 first logs the message for audit purposes. Then it checks the authenticity of the message by deciphering the message using the key manager 604, and examining the unique message ID and the party ID to confirm that they match what was sent out.

Once the message authenticity is established, the message receipt is logged for billing and auditing purposes. Finally, the response message is processed as required by the party. This may include emailing the party; logging it to a file for the party to collect; and/or making a request to a third-party application to process the message. The actual method(s) used to process the response message can be specified when calling the API. If the API call does not specify a processing method, then the response is processed using the default method configured for the corresponding developer, determined when the developer establishes an account with the provider of the interactive system.

The persistent storage 612 is a non-volatile storage component that is used by:

(i) the key manager 604 to store the encryption keys for the various mobile devices;

(ii) the message sender 608 to store the addresses of user devices 106 (*e.g.*, phone numbers in the case of the device 106 being a telephone), together with the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 800 of 1360

delivery mechanisms that each user device 106 supports. It also stores the identifiers of the messages that have been sent out, for verification purposes;

(iii) the message receiver 606, to store received messages for audit and billing purposes; and

(iv) the opt-in manager 610, to store opt-in data representing each user device 106 and the third party applications that are authorised to send instructions to each user device 106.

Encryption keys

As described above, each installed instance of the client application 102 on a user device 106 is identified by a unique client identifier (also referred to herein as the client ID number) that is associated with its phone number. When a client application 102 is first installed on a mobile device 106, a number of private encryption keys are generated and associated with the client ID.

As shown schematically in Figure 9, these encryption keys are then used by the client application 102 to authenticate the payload data and to encrypt the response data. On each payload or response data packet or message, the index of the appropriate encryption key is indicated in the header of the payload.

Figure 10 is a schematic diagram illustrating the message and process flow for generating and updating encryption keys on a client application 102 and an application gateway or backend system 104. The process is initiated by the client application 102 making a secure communication activation request to the application gateway 104 at step 902. In response, the application gateway 104 generates and stores a set of private encryption keys, and associates these with the client ID at step 904. At step 906, the application gateway 104 sends these newly generated private keys to the client application 102. The client application 102 stores the received private keys on the persistent storage 412 at step 908, and returns an acknowledgement to the application gateway 104 at 910, confirming that the private keys have been stored (or updated if the keys had been previously stored). This completes the generation/update steps and secure communication is activated at step 912. This involves encrypting a message payload using one of the private encryption keys, which can be selected at random or on any other basis at step 914. At step 916, the secured payload encrypted with the selected key is sent to the client application 102, together with

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 801 of 1360

a message header specifying the index of the selected encryption key. At step 918, the client application uses the encryption key index indicated in the header to select the appropriate private key, and uses that key to decrypt the payload data at step 918. After performing the application instructions specified by the payload, the client application 102 then encrypts the response at step 920. The response can be encrypted using the same key, as shown in Figure 10, or any other of the stored keys. The secured response is sent to the application gateway 104 at step 922, and the response is decrypted using the appropriate response key at step 924. As will be understood by those skilled in the art, the use of private encryption keys greatly improves the security of communication, and the use of a set of encryption keys, rather than a single key, further increases this security.

When sending a response message, the client application 102 uses the source address of the corresponding payload data by default. This effectively provides multiple client-server communication channels in between the backend 104 and the client application 102. For example, Figure 11 shows an arrangement whereby two instances of the client application 102, a first instance 1002 and a second instance 1004, are in communication with two instances 1006, 1008 of the application gateway 104, via a wireless communications network 110. A message 1010 sent from the first backend system 1008 to the second client application 1004 includes an address 1012 of the first backend system 1008 in the header of the message 1010 so that when the client application 1004 sends the corresponding response 1014, it is addressed to the first backend system 1008.

In contrast, Figure 12 shows the same arrangement whereby a message 1102 also includes the address 1012 of the first backend system 1008. However, workflow instructions contained in the payload data can alter this default behaviour by redirecting the response to another backend server instead. This mechanism is activated by a DIVERT command in the payload data, described further in the Appendix. Specifically, in this message 1102 the payload 1104 includes a divert instruction with the address of the second backend system 1006. Consequently, after the second client application 1004 executes this instruction, the response 1106 is addressed to the second backend system 1006, rather than the first backend system 1008 that originated the message 1102 containing the instructions. Because the second backend system 1006 does not have direct access to the client ID and message ID pair, or the encryption keys for the client application 102, the second backend system 1006 calls an API of the first backend system 1008 to check the integrity and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 802 of 1360

authenticity of the response data. If the payload was encrypted, then the first backend system 1008 decrypts the payload and sends it back to the second backend system 1006 over a secured communications channel (using SSL, for example). In an alternative embodiment, the encryption keys are stored in a centralised component of the interactive system, and all encryptions and decryptions are performed in this manner.

Communication data payload

The payload exchanged between the client application 102 and the backend system 104 is binary data - a sequence of bytes. The communication channel for this payload can include SMS or Cell Broadcast Service (CBS) messages; IP/TCP data packets (over GPRS, 3G or other type of data networks); and/or Bluetooth data packets.

As shown in Figure 13, each data payload is prefixed with a header 1204 which indicates whether the payload is encrypted with an encryption key. The header data contains the index of the encryption key stored in the client application key-storage, thereby allowing the client application 102 to decrypt the payload data.

As shown in Figure 14, plain payload data (either unencrypted or after being decrypted) contains a series of variable-length data parts that instruct the dynamic workflow execution engine 508 of the client application 102 to construct the user UI workflow.

As shown in Figure 15, each data part includes type 1402 and length 1404 data fields, followed by the actual instruction data 1406. The type field is a single octet or byte that defines the type of workflow instruction that follows. The length indicates the number of octets or bytes of the instructor data 1406.

As described above, the interactive system is able to use one or more of a variety of different communication channels for sending and receiving messages and responses between the application gateway 104 and the client application 102. For most of these different communication channels, the communication itself is straightforward, using the standard methods and libraries available and known to those skilled in the art. However, the interactive system supports message and response delivery via the short message service, or SMS. SMS is defined in the GSM 03.40 specification, which defines an upper limit on the size of each SMS message. Specifically, each SMS message is capable of

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 803 of 1360

containing up to 140 bytes of data, equivalent to 160 ASCII characters when using 7-bit encoding, as shown in Figure 17. The interactive system sends SMS messages including 8-bit (binary) data and including a 7-byte user data header or UDH 1702, as described in the GSM 03.40 specification. The UDH 1702 consists of a length field or UDHL 1704, specifying the length of User Data Header in bytes as specified in GSM 03.40, and a 6-byte User Data Header field 1706 specifying the destination address of the payload data 1708.

The UDH data 1702 - specifying the destination of the binary message - is interpreted by the mobile device to deliver the payload data to the client application 102. Excluding UDH data 1702, each SMS message is capable of carrying 133 bytes of payload data 1708.

If the payload data exceeds this length, the payload data is sent in two or more SMS messages 1804, each message containing up to 127 bytes of payload data 1806, 1808, as shown in Figure 18. These SMS messages 1804 have a section of User Data Header indicating that they all belong to a concatenated message, as described in the GMS 03.40 specification. A byte padding mechanism is used by the backend system 104 and the client application 102 when the payload is sent in multiple SMS messages. In this mechanism, a padding or termination byte 1810 with value 0xFF is appended to the end of each payload data fragment 1806, 1808 when sent out from the backend system 104. The client application 102 removes these padding bytes 1810, which appear as stuffed bytes 1812 in the concatenated payload data before passing the payload data 1814 to the workflow execution engine 408. The byte padding mechanism is used to eliminate problems found in a number of mobile phone models that strip out the last byte of every concatenated data fragment.

The instruction compiler 602 creates the payload data from the compiler output to generate binary SMS messages. Construction of binary messages includes splitting the payload data 1802 into multiple SMS messages 1804 if the data length exceeds the single message capacity of 133 bytes. Figure 19 is a flow diagram showing the steps involved in this process.

As shown in Figure 19, when delivering a message or a response via SMS, at step 1902 a check is performed to determine whether the size of the payload data exceeds 133 bytes. If

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 804 of 1360

not, then at step 1904 a user data header is added, and a single SMS message is composed and sent at step 1906. Alternatively, if the payload length does exceed the maximum size that can be sent in a single SMS message, then at step 1908 a concatenated message identifier is generated, and at step 1910 the number of concatenated messages that are required to accommodate the payload data is determined. Then, a processing loop consisting of steps 1912 to 1920 composes the appropriate number of SMS messages as follows. At step 1912, the next payload portion is selected and copied to the payload of the current SMS message. At step 1914 a user data header is added, including the identifier indicating that the SMS message is part of this SMS message set. At step 1916, a padding or termination byte is appended to the payload data, as described above. Finally, at step 1918 the resulting SMS message is sent. These steps 1912 to 1918 are repeated until the test at step 1920 determines that the last part of the payload data has been sent, and the process then terminates.

Removal of stuffed bytes in the payload data is handled by the client application 102 by searching for the specific stuffed byte octet value (0xFF in this embodiment) and removing it from the payload data, as shown in Figure 20.

Figure 16 is a schematic diagram showing the fifteen different instructions supported by the interactive system, showing the respective type bytes identifying each instruction type, and the structure of the corresponding instruction parameters. Further details on the various instructions are provided in the Appendix.

Dynamic workflow execution engine

The client application 102 presents to the user a number of user interface (UI) widgets 406 as well as executing user-invisible routines. This allows the client application 102 to display information as well as capture device information and/or user inputs.

The UI widgets 406 typically include the following type of user interface components and controls:

(i) Message screen: to show textual information;

(ii) Selection menu: to ask for the user's selection of one of a number of defined choices (*i.e.*, radio buttons);

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 805 of 1360

(iii) Multiple choices: to ask for user's one or more choices (*i.e.*, check boxes);

(iv) Textual input: to retrieve free form text input from the user (textbox);

(v) Numeric or date inputs: to retrieve user input data, restricted by type; and

(vi) Widgets displayed when branching and jumping amongst execution steps.

However, this list of UI widgets 406 and their actual screen layouts can vary depending on the platform (*i.e.*, on each combination of device hardware and operating system software) on which the client application 102 is installed.

The client application 102 implements a workflow execution process 2100, as shown in Figure 21, on each invocation to execute a workflow application. The workflow execution process 2100 begins after the client application 102 is invoked at step 2102, and a test is performed at step 2104 to determine whether the invocation has resulted from the receipt of new payload data from the application gateway 104. If so, then at step 2105 the new payload instructions are retrieved, and then parsed at step 2110. Otherwise, if the invocation was not due to the receipt of new payload data, then a test is performed at step 2106 to determine whether instructions are contained in the instant data storage 410. If so, then the instructions are retrieved from the instant data storage 410 at step 2108, and then parsed at step 2110. Otherwise, another test is performed at step 2132 to determine whether any sets of instructions have been saved as applications in the permanent data storage 412. If not, then at step 2134 an information message is displayed to the user indicating that there are no applications (instant or permanent) in the queue. Once the user acknowledges this information message, or when a corresponding timeout period has elapsed, the client application 102 is terminated. Alternatively, if the permanent data storage 412 contains one or more permanently stored sets of instructions (*i.e.*, applications), then at step 2136 these are displayed to the user, and the process 400 pauses at step 2137, awaiting the user's selection of one of these, or selection of a quit option. If, at step 2138, it is determined that the user has selected the quit option, then the client application 102 terminates. Otherwise, the user has selected a permanently stored set of instructions, and these are retrieved at step 2140, and then parsed at step 2110.

Following parsing of the workflow instructions at step 2110, the first or next workflow instruction is read at step 2112, and executed at step 2114. If it is determined at step 2116 that the instruction is a UI instruction, then the process waits to receive user input at step 2118. Once the user's response has been received, at step 2120 the UI widget

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 806 of 1360

displayed on the screen of the device 106 is removed, and any user input is stored at step 2122. At step 2124, a test is performed to determine whether the instruction was the last in the workflow. If not, then the process loops back to step 2112. Otherwise, once all of the instructions have been executed, then a response message is composed at step 2126, and sent at step 2128. If the workflow instructions executed are stored in the instant data storage 410, then they are deleted at step 2130. This terminates the workflow execution process 2100.

Parsing workflow instructions and response data

The workflow execution engine 408 of the client application 102 interprets the payload data parts and generates the dynamic UI workflow accordingly.

The data parts from the payload data are indexed sequentially when read by the workflow execution engine 408, and, this is also the default order of workflow execution 508. As shown in Figure 22, the response data includes each response in the same order as the corresponding instructions were received and executed. When a workflow instruction is executed and response data is to be retrieved, a parameter name is included in the instruction data, and the user response or system response is associated with this parameter in the response. All the instruction responses are included in the response data when the workflow is completed, as shown in Figure 23.

Jumping and Branching in the workflow

The workflow execution engine 408 provides a mechanism to allow branching and jumping in the sequence of instructions.

Branching

Because an instruction might be involved in different branches through out the workflow, the workflow execution engine 408 differentiates the instruction response data for different branches using branch domains. A branch domain specifies the address of a workflow instruction in the workflow tree. When setting the instruction response data, the response parameter name is prefixed with the corresponding branch domain, separated by a period character. For example, an instruction to retrieve user input for a numeric-valued parameter with the parameter name "number" could be called from two different branch menus: one named "First branch", and the other named "Second branch". In both of these

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 807 of 1360

cases, the instruction returns the same parameter name "number" but with different values. The workflow execution engine 408 associates a branch domain with the parameter name to differentiate the two response values. Thus in this example, the first value is returned as "First branch.number = xxx" and the second value as "Second branch.number = yyy", where "xxx" and "yyy" represent the actual values entered by the user. Figure 25 shows a more complex example where menu selections are nested.

Additionally, the branch domain is appended with a branch name on selection of a branch menu. For example, in an application with two nested branch menus 3902 "Service Request" and 3904 "Water Service" as shown in Figure 39, when the user selects item 3910 "Water" in menu 3902, and then selects item 3912 "Pipe Burst" in the subsequent branch menu 3904 "Water Service", and then fills out 3914 with "John Doe" in the text input screen 3906 "Your name", the client application 102 will internally send the response as "Water.Pipe burst.name=John Doe". When the BRANCH_BACK command is executed, the previous branch name is removed. The workflow execution engine 408 uses a branch name stack to maintain the order of branch names as they are selected.

For usability reasons, when working with a multiple branch menu, it is important for the user to know whether or not a branch has already been visited by the user. To this end, the workflow execution engine 408 indicates visited branch menu items by displaying an image adjacent to those branches to indicate that they have already been visited by the user. For example, as shown in Figure 27.

When the user has visited user input screen 2702 to enter data 1, an image icon 2706 is displayed adjacent to the first branch menu item 2704 is marked with distinct. This allows user to visually distinguish those parts of the workflow that have been visited from those parts that have not been visited. Alternatively, the visited branches could be displayed in a different colour, as used by web browsers to indicate that a hyperlink has been visited.

Backward navigation

As shown in Figure 28, all of the user interface screens include a "Back" navigation button 2802 to allow the user to return to the previous screen within the workflow. The position of this back button can change depending on the specific mobile device platform executing

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 808 of 1360

the client application 102. As shown in Figure 29, the workflow execution engine 408 maintains an ordered list or stack of instructions that cause a change in the screen or display, and selection of the "Back" button causes the execution to return to the previous instruction.

Sending a workflow description to the Instruction Compiler

As described above, a developer 116 can send a workflow description to the instruction compiler 602 of the application gateway 104 by submitting programming instructions written in the programming language supported by the instruction compiler 602, using a hypertext transport protocol (HTTP) interface of the instruction compiler 602. For example, Figure 30 is a screenshot of an HTML webpage generated by the application gateway 104. The webpage includes a scrollable text box 3002 into which the developer 118 can directly enter commands in the scripting language, and a compile button 3004 which, when pressed, submits the text in the scrollable text box 3002 to the instruction compiler 602 for compilation.

The scripting language of the interactive systems is a high level language for describing the workflow of an interactive application. It is similar in vein to BASIC and can be learnt quickly by a programmer who has a basic knowledge in programming.

Alternatively, a workflow description can be sent to the instruction compiler 602 by invoking API calls to the application gateway API 616. For example, Figure 31 shows a source code listing of a J2ME function `SendWorkflowRequest` that is used to generate and send workflow instructions to the mobile telephone 106. In this example, the workflow instructions are to display booking details to the user 120 and then retrieve the user's response indicating whether the user 120 accepts or rejects the booking, together with the user's name and telephone number. The workflow API is first initialised by creating (at 3102) a new J2ME Command() object named `WorkflowCommand`. A workflow header, as described below, is then added at 3104. Workflow instructions are then added in the order of desired execution by calling APIs that are provided as methods of the `WorkflowCommand` object. Each type of workflow instruction is added by calling a corresponding API function with a set of parameters. For example, the object method `AddInfoMessage` is used (at 3106) to add an instruction that displays a screen of

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 809 of 1360

information to the user. The first argument to this method provides a title for the screen, and the second argument provides the actual text information that is displayed. Similarly, the method `AddSingleMenu` adds (at 3108) an instruction that displays a single-level menu (*i.e.*, radio buttons) to the user, allowing the user to select one item from a list of items provided as a parameter to the method. In this example, the two items are displayed as "Accept", and "Reject", and the user's response indicates whether the user 120 accepts or rejects the booking.

The method `AddUserInputCmd (at 3110 and 3112)` displays a text string to the user, together with a textbox, prompting the user to enter an appropriate input value. The first parameter to this function finds the name of the parameter that will be associated with the returned input value. The second argument provides a string that is displayed to the user, and a third argument allows the developer to restrict the type of input; for example, to a phone number, email address, and so on.

Finally, the `AddRedirectHeader` method (at 3114) defines a return address or phone number to which the response will be redirected, as described above. The communication channel to be used (*e.g.*, whether by SMS, IP network, Bluetooth, etc) is also specified in the header.

Once the workflow instructions are added, the workflow API is called again (at 3116) to compile the instructions and build the payload data to be sent to the client application. The workflow API is called as many times as needed (at 3118) to send multiple messages if required.

Scripting Language Overview

- Instructions are written line by line.
- Comment lines start with //
- Label lines start with #
- String parameters are delimited by double quote characters ""

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 810 of 1360

Workflow-programming Structure

Commands are processed sequentially line by line. Three instructions are provided to create tree structures of the workflow: BRANCH_TO, BRANCH_BACK, and GOTO. BRANCH_TO and BRANCH_BACK are used in combination to create a subroutine for the compiled program. GOTO is a jump instruction that allows program execution to jump to a specified line in the script. Comment and blank lines are ignored by the instruction compiler 602.

Command line syntax

A command is a line in the script which has the following structure:

<Command Name> <String Parameter> <String Parameter> <Label>

Where:

- <Command Name> is a command.
- <String Parameter> is a qualified string value, *i.e.*, delimited by double quote characters. For example, "User name" is a string parameter. There can be more than one string parameter in each command.
- <Label> is the name of the label that is associated with the command. Labels can only be used with the GOTO command and the ITEM command when used in conjunction with BRANCH_TO command.

Comment

There is no block comment in the language. Comment lines are lines that start with // (two forward slash characters followed by a space character).

Example:

// this is a comment line

Label

A label is a way to mark a line number so that it can be referred to in GOTO and BRANCH_TO 's ITEM commands. A label line starts with # (hash) character, followed by a space character. The label name is the next word from the # character.

Example:

For label START, the line looks like this:

START

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 811 of 1360

The label name is mapped to the index (*i.e.*, relative position in the script) of the command immediately following the label line.

Labels in a script must be unique, a compile error occurs if a duplicate label is detected. All labels are parsed in the first pass of the compiler, building a mapping of label and command index to be used in the second pass.

Backward navigation

As described above, a "Back" navigation button is attached to all displayed screens by default. This button allows backward navigation of the workflow executed on the user device 106. On most mobile phone platforms, this "Back" button is mapped to the right action key. However, this can change depending on the type of phone.

Tree navigation

A combination of the BRANCH_TO command, labels, and the BRANCH_BACK command allows the workflow to support a tree like execution structure, as shown in the source code listing of Figure 32 and the resulting display screens of Figure 33. A detailed description is provided below. When a user is navigating thought workflow screens, the state of each screen (item selection and user inputs) is not remembered.

Example

The following is a source code listing that is used to generate an interactive application for execution on a user device such as the mobile telephone 106. The source code defines a workflow that allows the user 120 of the mobile telephone 106 to generate a service request for water, electricity, and/or gas services. The listing is arranged in four groups of commands or paragraphs under respective labels. The first paragraph, labeled START, results in display of a main screen 3402, as shown in Figure 34. The BRANCH_TO command has two parameters. The first, "serv" defines a branch name for this branch, and the second parameter, "Service Request" defines the title that is displayed at the top of the main screen 3402. The subsequent three commands define items that can be selected by the user to invoke corresponding workflow branches. For example, the first ITEM command has two parameters. The first parameter, "Water", defines the text 3404 that is displayed on the main screen 3402, and that can be selected to invoke the corresponding workflow branch. The second parameter, in this case "WATER", is a label of the corresponding

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 812 of 1360

workflow branch, in this case referring to the second group or paragraph of commands grouped under that label. Thus if the user navigates the main screen 3402 to select the first item 3404, the workflow jumps to the SELECT ITEMS, causing display of a water service selection screen 3406. In this case, the three items are simply menu selections (rather than workflow branches), and thus selection of any one of these items causes the appropriate parameter, in this case named "water" to be assigned a value defined with the corresponding item. For example, if the user selects the second item, "Leaking" 3408, then the parameter "water" is assigned the value "Leaking". Once this item has been selected, the workflow proceeds to the following command, which in this case is the BRANCH_BACK command, which returns control to the main screen 3402.

In this manner, the user can select the Electricity item 3410 to branch to the ELECTRICITY workflow, resulting in display of a Electricity service screen 3412. Similarly, the user can select the "Gas" request item 3414 to cause a Gas service screen 3416 to be displayed. Once the user is satisfied with the service requests thus defined, selection of the Next button 3418, or the OK button 3420 causes execution to continue to execute in this example the command "GOTO CONTACTS", which causes the workflow to jump to the command following the CONTACTS label, being in this case an INPUT command displaying a name input screen 3422, and subsequently a Contact number screen 3424. Once the OK button 3426 on the Contact numbers screen 3424 has been selected, a MESSAGE command causes display of a Service Info screen 3428 providing informational feedback to the user, in this case confirming that the service request will or has been sent to an appropriate party for processing the user's request.

```
// Start of program
# START
BRANCH_TO     "serv" "Service Request"
ITEM          "Water" WATER
ITEM          "Electricity" ELECTRICITY
ITEM          "Gas" GAS
GOTO          CONTACTS

# WATER
SELECT        "water" "Water service"
```

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 813 of 1360

```
ITEM            "Pipe Burst"
ITEM            "Leaking"
ITEM            "New connection"
BRANCH_BACK

# ELECTRICITY
SELECT      "elect" "Electricity service"
ITEM            "Fire"
ITEM            "New connection"
ITEM            "Disconnection"
BRANCH_BACK

# GAS
SELECT      "gas" "Gas service"
ITEM            "Leaking"
ITEM            "New connection"
ITEM            "Fire"
BRANCH_BACK

// This is like a subroutine
# CONTACTS
INPUT           "name" "Your Name" ANY
INPUT           "phone" "Contact Number" NUMERIC
// message is sent here
//# END
MESSAGE     "Service Info" "Your request will be sent to XXXX"
```

Script commands and syntax

HEADER command

The HEADER command is used to include a specified piece of text at the beginning of the response message when the workflow has been executed. This command is invisible to the

user of the user device. This command is used as a context identifier for server-client conversation.

There can be multiple header commands in the script. When using the HEADER command in conjunction with the BRANCH_TO command, different response message prefixes can be set, based on the user's selection.

Syntax

HEADER <header>

- <header> is a string parameter to be prepended to the response text message.

Example

HEADER "timesheet"

Response

<header> is attached to the beginning of the response message. If there are multiple headers to be included in the response message, the response headers are prepended based on their execution order in the workflow.

DIVERT command

The DIVERT command is used to redirect a response message to a telephone number or address different from that of the source of the original instructions. Normally, the response message is sent back to the source address of the payload, but the response message can be sent back to another number instead by including a DIVERT command in the workflow. This command is invisible to the user. There can be multiple DIVERT commands in the script, but the last one that is executed in the workflow takes effect. When combining this command with the BRANCH_TO Command, the workflow can send a response message to a source number selected by the user.

Syntax

DIVERT <address>

- <address> is a string parameter representing the mobile number of the redirected address.

Example

DIVERT "+61418366896"

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 815 of 1360

MESSAGE command

MESSAGE command shows a message with a title and message content to the user.

Syntax

MESSAGE <title> <message content>

- <title> is a string parameter for of the title of the message to be displayed.
- <message content> is a string parameter.

The end result is display of a screen as shown in Figure 35.

Example

MESSAGE "Hello" "Hello world"

Response

This GUI screen does not collect any user input and no response data is associated with it.

INPUT command

This command displays a GUI screen with a text input box 3602 to the user to retrieve user inputs, as shown in Figure 36. A parameter name is provided in the command to set the name of the user input data when included in the response message. A default input value can be provided as an input parameter. If desired, the user input data can be restricted to a certain types such as numeric, decimal or a phone number. However, the implementation of user input restriction depends on the capability of the user device executing the client application 102.

Syntax

INPUT<return parameter> <label> <type> <default value>

- <return parameter> is a string parameter for the name of the entered value to be set in the return message.
- <label> is the title of the input text box
- <type> is the type of the input to be captured, these types are available:
  - ANY
  - EMAILADDR
  - NUMERIC

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 816 of 1360

- PHONENUMBER
- URL
- DECIMAL

- <default value> is an optional string parameter to be set to the input text box when the screen is visible to the user. If omitted, the default value of the input text box is left empty.

Response

User input data is included in a response message associated with a parameter name specified in the corresponding instruction. If the INPUT command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<return parameter>=<value> (without domain path)

<domain path>.<return parameter>=<value>

Where:

- <value> is a string value that user enters. This can be an empty value.
- <domain path> is the path of branches that lead to this INPUT command in the workflow.

GAUSS command

This command results in the display of an interactive screen having a slider or "gauss" control 3702 to prompt the user to provide corresponding response data, as shown in Figure 37. The user is able to slide the slider control from a minimum value to a maximum value specified on the command line. The resulting data is included in the response message associated with the parameter name given.

Syntax

GAUSS <parameter name> <minimum value> <maximum value> <default value>

- <parameter name> is a string parameter for the name of the gauss value to be set in the return message.
- <minimum value> is the minimum value the user can select.
- <maximum value> is the maximum value the user can select

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 817 of 1360

- <default value> is the default value if the user does not select any value. This parameter is optional so if it is not present, the default value is empty.

Example

GAUSS "temper" "1" "10" "5"

Response

If this command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<parameter name>=<value> (without domain path)

<domain path>.<parameter name>=<value>

GOTO command

This command allows the workflow execution engine 406 to jump to a specific workflow instruction, rather than proceed to the next instruction in sequence. A parameter of this command is the label of the instruction for the workflow execution to be directed to. There is no user screen or response data associated with this instruction.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 818 of 1360

Syntax

GOTO <label>

- <label> is the label name indicating the index the command that the workflow execution jumps to after executing this command.

Example

....

GOTO Hello // The program jumps to message hello world after executing this command.

...

...

Hello

MESSAGE "Hello" "Hello world"

...

SELECT, SELECT_MULTI command

As shown in Figure 38, these commands display a screen with a list of items to select from. The SELECT command allows single item selection, and the SELECT_MULTI command allows multiple item selection screen. The user selection is included in the response message identified by the parameter name. In case of multiple selection list, the selected values are separated by a delimiter character in the response value data.

Syntax

SELECT or SELECT_MULTI command is followed by ITEM definitions (one per line).

SELECT <parameter name> <title>
ITEM <item name>
ITEM <item name>
ITEM <item name>

SELECT_MULTI < parameter name> <title>
ITEM <item name>

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 819 of 1360

ITEM <item name>
ITEM <item name>

Where:

- < parameter name > is a string parameter specifying the return parameter id for the SELECT screen.
- <title> is a string parameter specifying the title of the screen.
- <item name> is a string parameter specifying the item to be displayed on the screen.

Example

```
// This example allows the mobile user to select one of the option listed
SELECT "tsk" "Select task"
ITEM "Administration"
ITEM "Service desk"
ITEM "Client meeting"

// This example allows mobile user to select one or many of user names in the list
SELECT_MULTI "name" "Select users"
ITEM "User 1"
ITEM "User 2"
ITEM "User 3"
```

For multiple select command, each of the items in the select list is displayed adjacent to an icon that indicates whether or not the item has been selected by the user. On most mobile devices, a "Mark" button is displayed to allow user to mark the selection of the highlighted item. A "Next" button is also attached to this screen to allow the user to navigate to the next workflow instruction. On some mobile device platforms, the Next button is mapped directly to one of the mobile phone buttons.

Response

SELECT command:

<parameter name>=<item>

SELECT_MULTI command:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 820 of 1360

< parameter name >=<item>;<item>;<item>

Where:

- <item> is the item name as selected

The multiple select response can be empty.

BRANCH_TO command

This command provides users a list of items to select, and on selection of an item, execution of the workflow is branched to the specified command. The behavior of this screen is similar to the SELECT screen described above. Once the workflow execution starts executing from the new target instruction, it follows the default sequential order. When the BRANCH_BACK command is executed, the workflow execution engine returns to the previous BRANCH_TO command to execute. However, the BRANCH_TO command does not require a BRANCH_BACK command to operate. The workflow can consequently branch to the last command without returning to the branch menu.

To progress to the next screen from a BRANCH_TO command, a "Next" button is provided. On some phones, this button is mapped to one of the phone keys on the mobile device. On most phones however, this button is mapped to a soft-key named "Next" when the user select Options on the BRANCH_TO screen (similar to SELECT_MULTI command).

There is no specific user value attached to this screen in the response message. The selected branch item is however appended to the branch domain path. This domain path is then appended to the parameter name of any input screens being executed in the branch target.

Syntax

BRANCH_TO command is followed by ITEM definitions (one per line).

BRANCH_TO <parameter name> <title>
ITEM <item> <label>
ITEM <item > <label>
ITEM <item > <label>

Where:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 821 of 1360

- < parameter name > is a string parameter specifying the return parameter id for the BRANCH_TO screen.
- <title> is a string parameter specifying the title of the screen.
- <item > is a string parameter specifying the item to be displayed on the screen.
- <label> is a valid label name as specified in the workflow with "#" character.

Examples

```
...
# EnterBetAmount
INPUT "bet" "Enter bet amount" DECIMAL
BRANCH_BACK
....
# SelectBetAmount
SELECT "bet" "Select bet amount in dollars"
ITEM "100"
ITEM "200"
ITEM "300"
BRANCH_BACK
....
BRANCH_TO "b" "Select team to bet"
ITEM "Melbourne" EnterBetAmount
ITEM "Geelong" SelectBetAmount
GOTO END
...
# END
MESSAGE "Info" "Please select Yes to allow response message to be sent"
```

Response

- The domain path is appended with <item> selected in the branch menu.
- This domain path is then appended to the parameter name of any input screen executed in the branch target. In the example script, the "bet" amount parameter name when appearing in the response message is: Melbourne.bet=<bet value>.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 822 of 1360

BRANCH_BACK command

This command is invisible to the user, it provides the capability to navigate back from branching. A workflow could have multiple branches wired up and the result is a tree like structure. BRANCH_BACK command allows navigation upwards in this tree structure. Combination of label and BRANCH_BACK command allows combining a group of workflow commands in to a routine, which can be referred to multiple times during the workflow execution.

Syntax

BRANCH_BACK

STORE_PERMANENT command

This command instructs the workflow execution to store the whole payload data to persistent storage. A title is set in the parameter of this command allows the client application to display the stored payload data to the user. This command does not result in any user data in the response message.

Syntax

STORE_PERMANENT <title>

Where:

- <title> is a string parameter indicating the title of workflow payload data to be displayed in the persistent list. This persistent list is displayed to the user when the client application is started manually by the user and no instant payload data is waiting to be executed.

Example

STORE_PERMANENT "Message one"

CLEAR_PERMANENT command

This command clears all the persistent workflow payload data previously saved by STORE_PERMANENT command. Execution of this command does not result in any data in the response message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 823 of 1360

Syntax

CLEAR_PERMANENT

EXECUTE command

This command makes a request to the mobile device operating system to retrieve an URL address. The results could be making a phone call or launching the internet browser on the phone to the specified URL address. Behavior of this command might varies across different device models due to device capabilities.

Syntax

EXECUTE <url_address>

Where:

- <url_address> is a string parameter describing the URL address of the request to be sent to the J2ME platform.

Example

To make a mobile phone call to +61418366896 mobile number

EXECUTE "tel:+61418366896"

To launch the internet browser on the mobile phone to access ACME mobile website

EXECUTE "http://mobile.acme.com"

Response

If making a mobile phone call is required, the mobile device will ask user if a mobile phone call can be made. If launching of the internet browser is required, the application will ask for the user's permission to open the internet connection to the specified URL.

CONFIGURATION command

The response message is constructed from the user/system data. A number of default delimiter characters are used to separate the data parts as well as name-value separator. This command when included in the payload data can change the delimiter characters of the response message as well as specifying whether or not the name part is included in the response message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 824 of 1360

Syntax

CONFIGURATION <configuration_string>

Where <configuration_string> is composed of configuration characters:

- 1st character: Include parameter in the response, if set to '0', the response message only has values, set to '1', the response message has Name=Value
- 2nd character: Response part delimiter, the default is ','
- 3rd character: Equal character, the default is '='
- 4th character: Multiple selection options, the default is ';'
- 5th character: Screen path delimiter, the default is '.'

Example

CONFIGURATION "0,=;."

This configuration command instructs the workflow execution to exclude parameter names from the response message.

SYSTEM_PROPERTY command

This command instructs the workflow execution to read a system property and return the result in the response. The parameter name that is associated with the response data is the system property if parameter name is omitted.

Syntax

SYSTEM_PROPERTY <property_name> <parameter name>

Where:

- <property_name> is the system property to be read. On the J2ME platform, examples of these properties are:
  - microedition.profiles
  - microedition.configuration
- <parameter name> is an optional string parameter. If omitted, property name is used as parameter name in the response instead.

Examples

SYSTEM_PROPERTY "microedition.profiles"

SYSTEM_PROPERTY "microedition.profiles" "midp"

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 825 of 1360

Response

The value of the system property is included in the response message as name=value pair. All the rules applied to the name-value pairs are applied. These include changing of delimiter parameters and whether or not to include the name part in the response message.

<system property>=<value> (if parameter name is omitted)

<parameter name>=<value> (if parameter name is present)

NOP command

This is a no-operation command. It is useful when used in conjunction with labeling.

Syntax

NOP

SET_KEYS command

A command to set the encryption key specified by the index of the key on the mobile device.

Syntax

SET_KEYS <key_index> <key>

Where <key_index> is a string parameter indicating the index of the key to be set on the client application 102. <key> is a string parameter containing the actual key to be updated.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as hereinbefore described with reference to the accompanying drawings.

It will be apparent from the description above that the interactive system and process described herein allow a developer to dynamically send on demand customisable workflow instructions to one or more user devices 106 such as mobile telephones. The generation, secure delivery, execution, and secure return of response data to the developer are all handled transparently by the interactive system, thus hiding all the details of these aspects from the developer, greatly simplifying the provision of interactive applications and quasi-real-time interactions with one or more users. The provision of workflow instructions via

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 826 of 1360

SMS is particularly advantageous as it can be assumed to be supported by all mobile telephones available today. Moreover, since the SMS communications are all managed by the interactive system, any premium SMS services that may be required can be established by the operator of the interactive system, thus freeing the developer from needing to establish their own independent premium SMS services. This greatly simplifies the provision of new interactive applications, and also allows the operator of the interactive system to provide these services at a lower cost by leveraging the substantial volume of SMS traffic resulting from the aggregation of SMS traffic or all developers using the interactive system.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 827 of 1360

CLAIMS:

1. A method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

2. A method as defined by claim 1 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language.

3. A method as defined by either of claims 1 or 2 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

4. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device.

5. A method as defined by claim 4 wherein the step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

6. A method as defined by claim 5 wherein the step of sending the message includes the step of sending a unique message identifier.

7. A method as defined by claim 6 further comprising the step of the mobile user device receiving the set of instructions and the unique message identifier.

8. A method as defined by claim 7 wherein the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

9. A method as defined by either of the claims 7 or 8 further comprising the step of receiving a response to the instruction from the mobile user device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 828 of 1360

10. A method as defined by claim 9 wherein the step of receiving a response includes the step of receiving a response identifier from the device.

11. A method as defined by claim 10 wherein the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

12. A method as defined by any one of the preceding claims wherein the step of translating the instruction includes tailoring the instruction to a device operating system.

13. A method as defined by any one of the preceding claims wherein the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

14. A method as defined by claim 13 wherein the step of translating the interactive workflow includes tailoring the instruction to the specification.

15. A method as defined by any one of the preceding claims wherein the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

16. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network.

17. A method as defined by claim 16 wherein the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS.

18. A method as defined by any one of the claims 1-15 wherein the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 829 of 1360

19. A method as defined by any one of the preceding claims also including the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow.

20. A method as defined by claim 19 wherein the step of checking involves sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow.

21. A method as defined by claim 3 wherein the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface (API) from the external or third party.

22. A method as defined by claim 21 wherein the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

23. A method as defined by any one of the preceding claims also comprising the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

24. Computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

25. A method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 830 of 1360

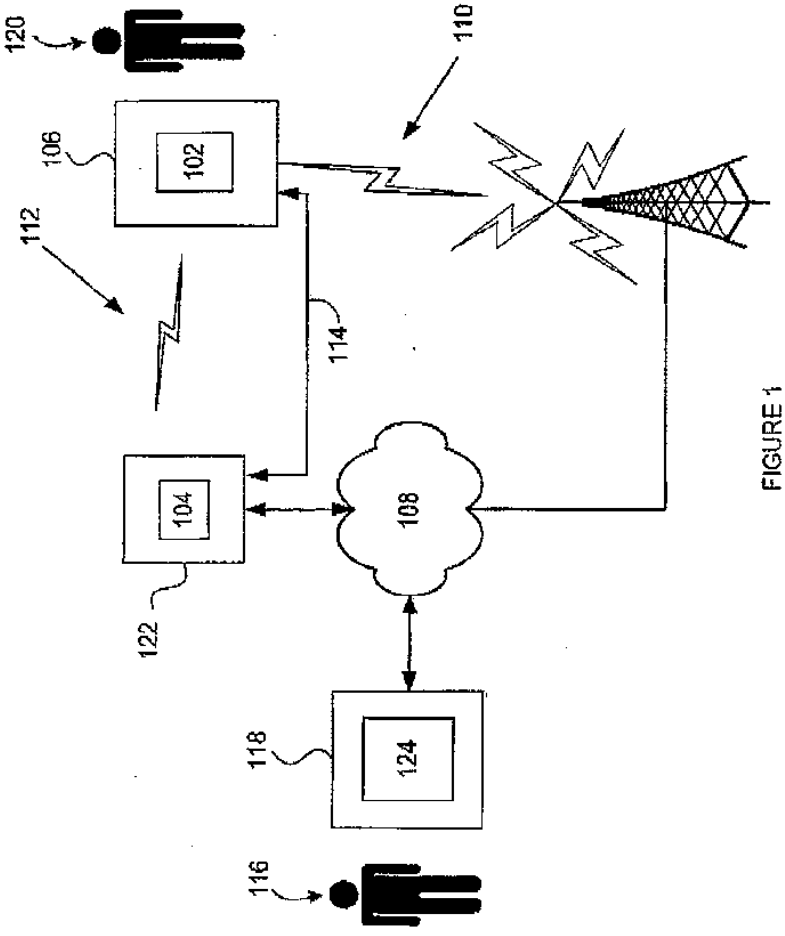


FIGURE 1

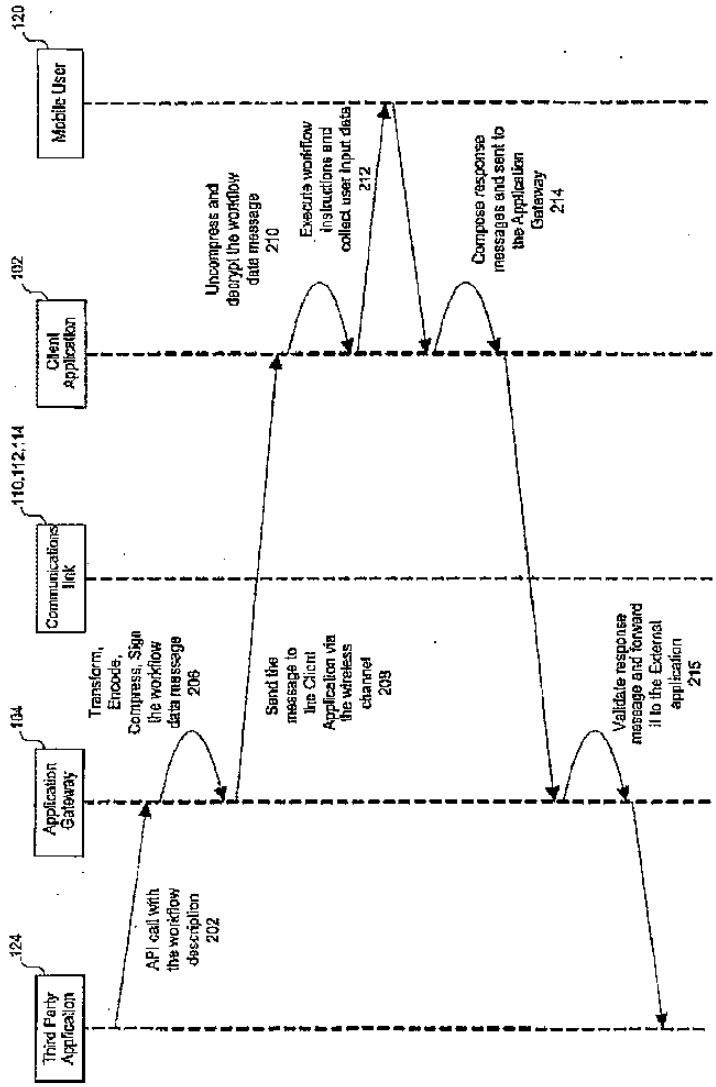


FIGURE 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 832 of 1360

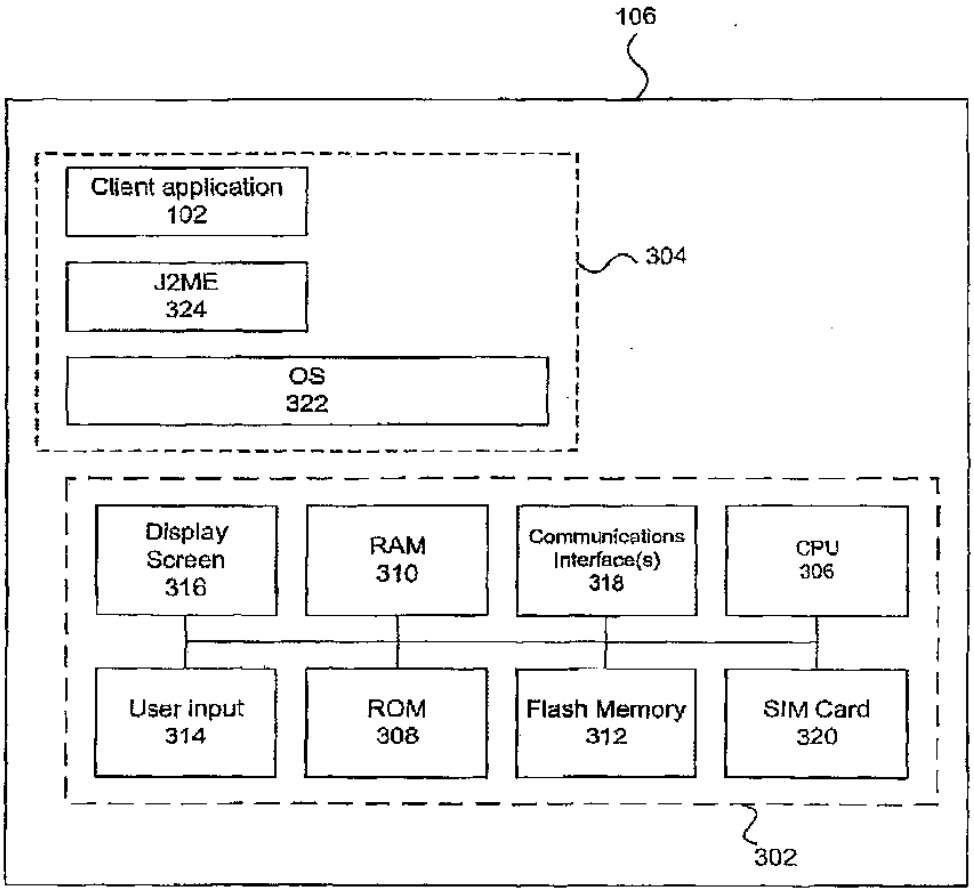

106
Client application
102
J2ME
324
OS
322
304
Display
Screen
316
RAM
310
Communications
Interface(s)
318
CPU
306
User input
314
ROM
308
Flash Memory
312
SIM Card
320
302

FIGURE 3

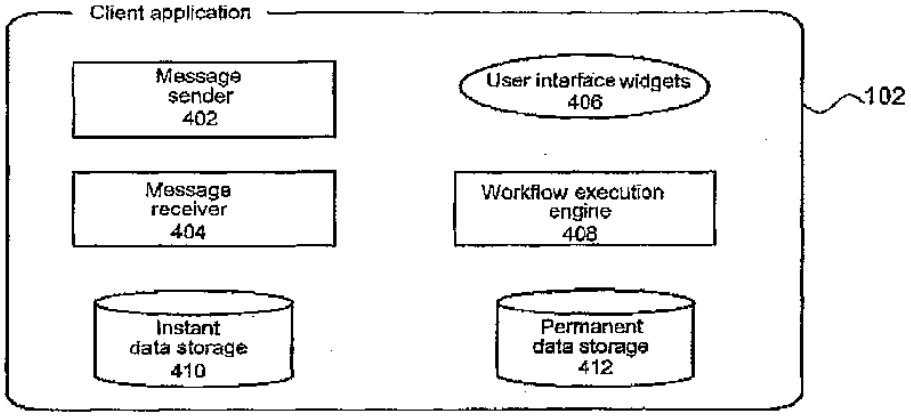


FIGURE 4

FIGURE 5

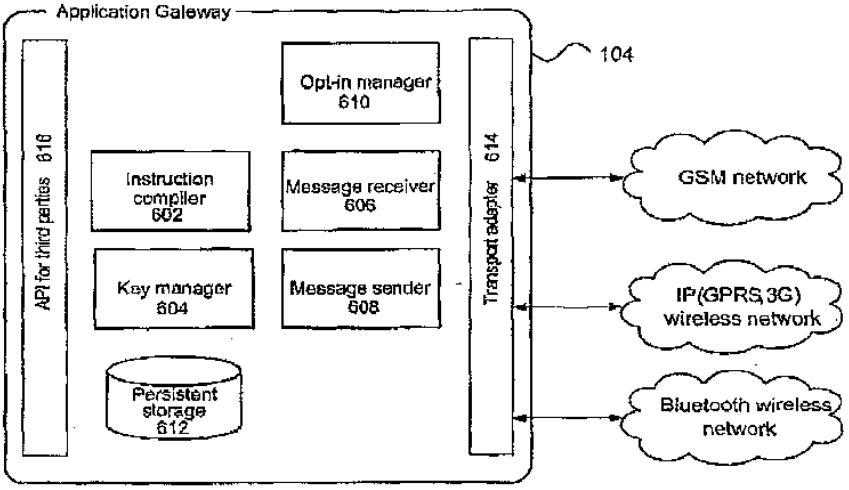

Application Gateway
API for third parties 616
Opt-in manager 610
Instruction compiler 602
Message receiver 606
Key manager 604
Message sender 608
Persistent storage 612
Transport adapter 614
104
GSM network
IP(GPRS,3G) wireless network
Bluetooth wireless network

FIGURE 6

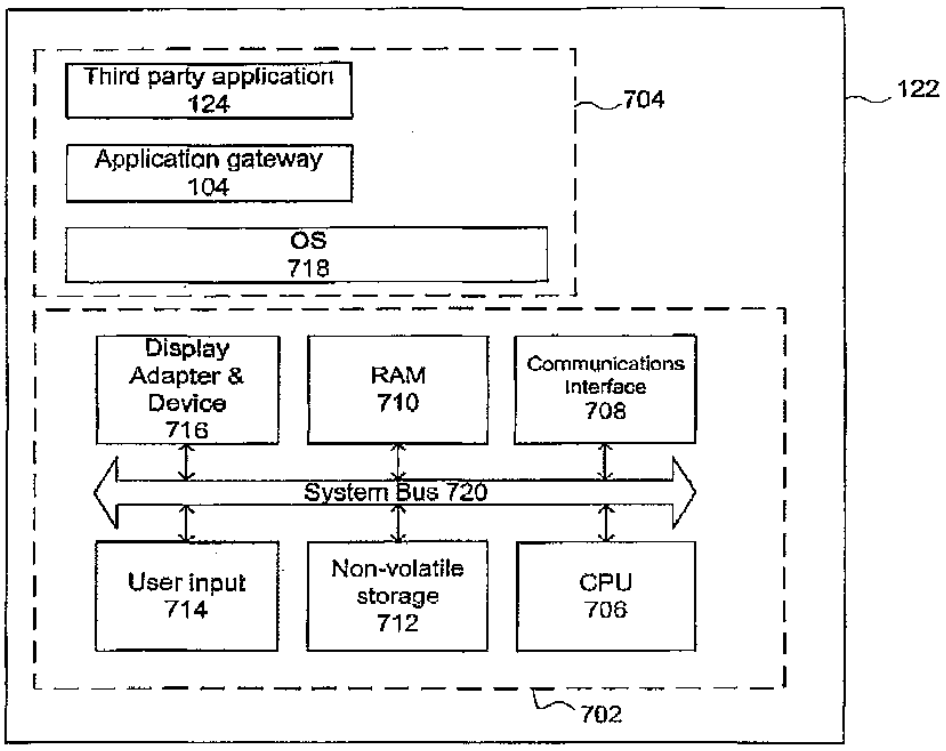

Third party application
124
Application gateway
104
OS
718
704
122
Display
Adapter &
Device
716
RAM
710
Communications
Interface
708
System Bus 720
User input
714
Non-volatile
storage
712
CPU
706
702

FIGURE 7

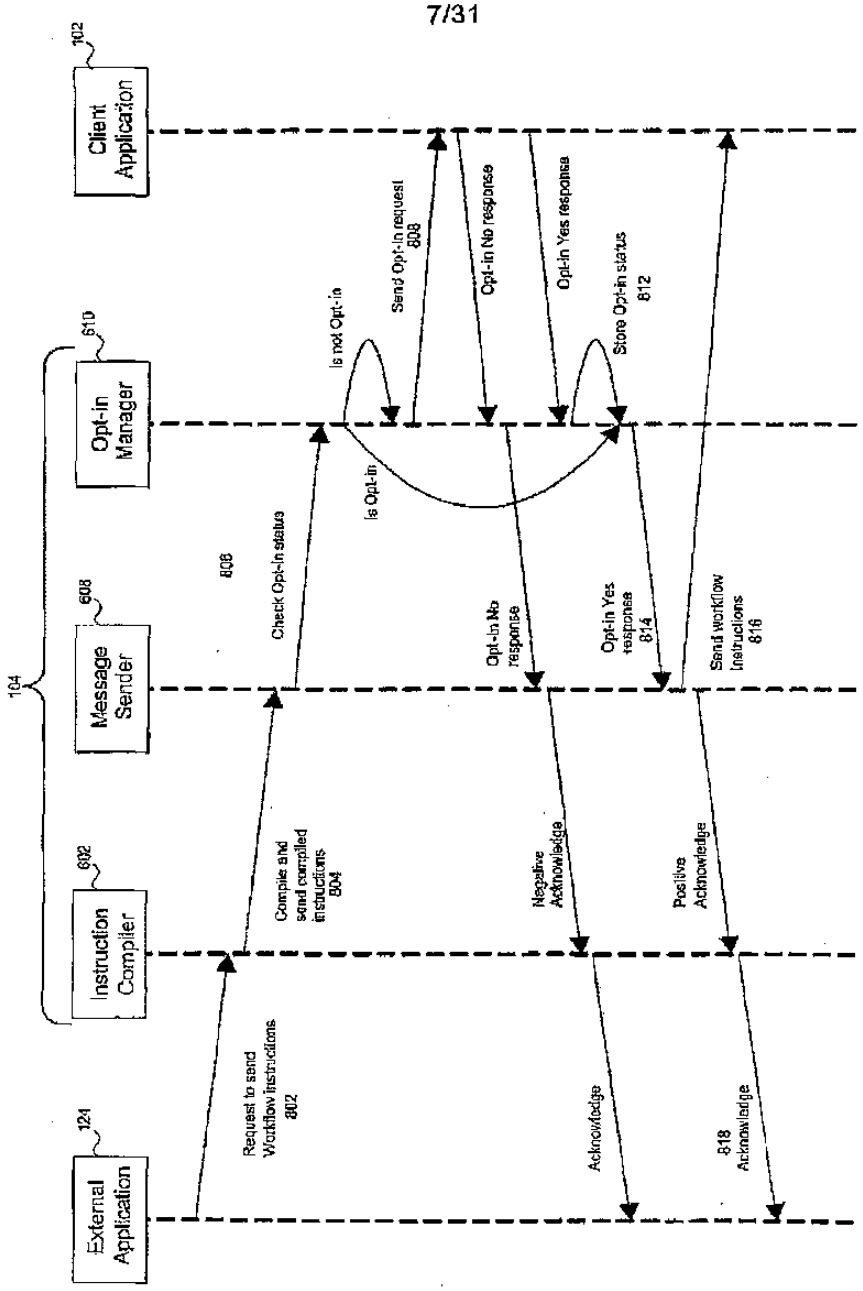


Figure 8

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 837 of 1360

8/31

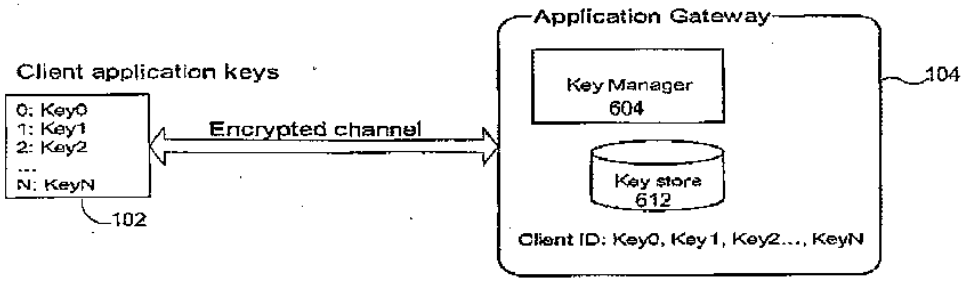

Application Gateway
Client application keys
0: Key0
1: Key1
2: Key2
...
N: KeyN
Encrypted channel
Key Manager
604
Key store
612
Client ID: Key0, Key1, Key2..., KeyN
102
104

FIGURE 9

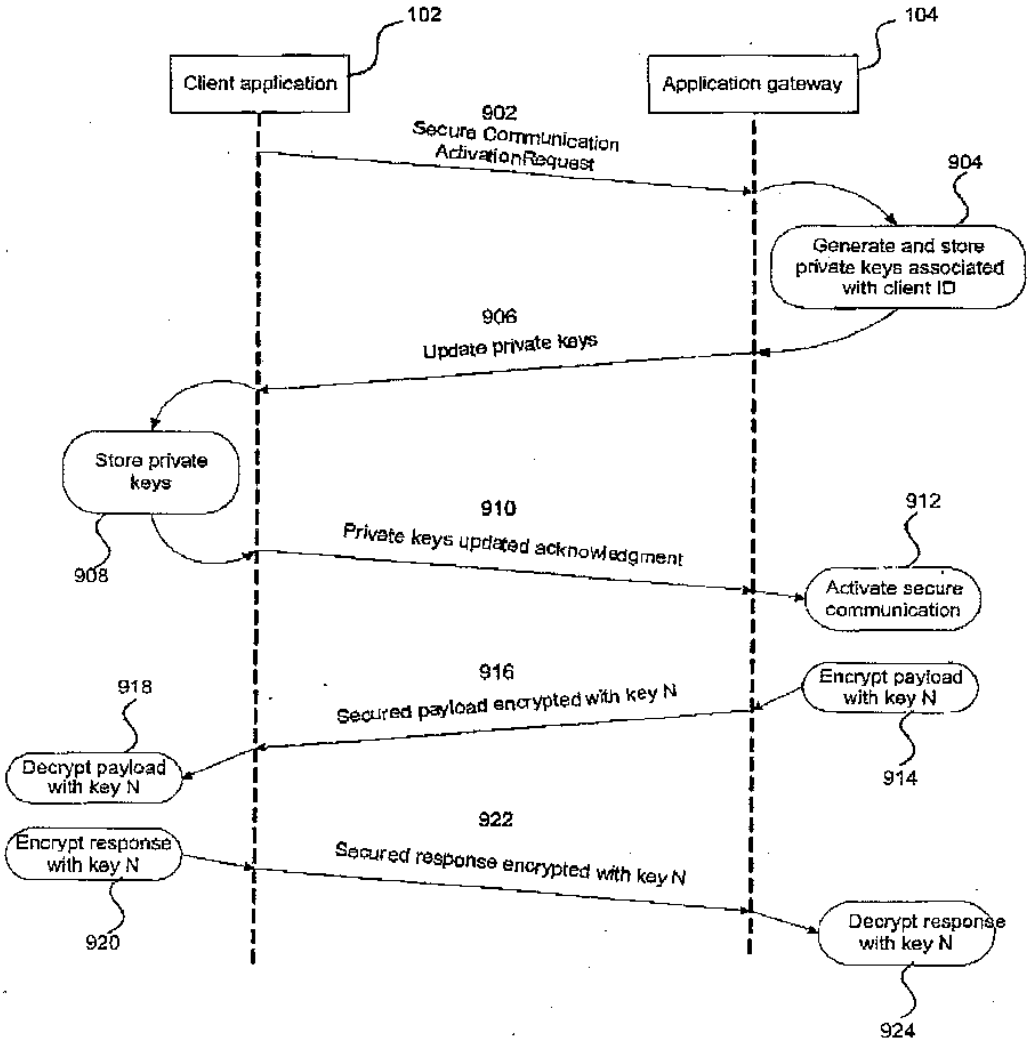

102
Client application
104
Application gateway
902
Secure Communication ActivationRequest
904
Generate and store private keys associated with client ID
906
Update private keys
Store private keys
908
910
Private keys updated acknowledgment
912
Activate secure communication
916
Secured payload encrypted with key N
Encrypt payload with key N
914
918
Decrypt payload with key N
922
Encrypt response with key N
Secured response encrypted with key N
920
Decrypt response with key N
924

FIGURE 10

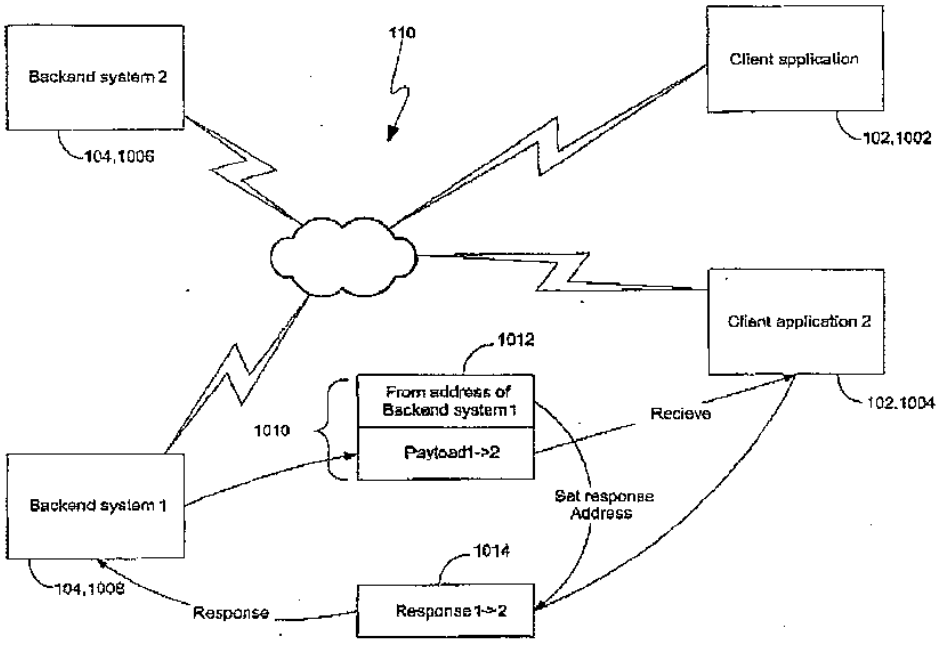

110
Backend system 2
104,1006
Client application
102,1002
Client application 2
102,1004
1012
From address of Backend system 1
Payload1->2
1010
Recieve
Set response Address
Backend system 1
104,1008
Response
1014
Response1->2

FIGURE 11

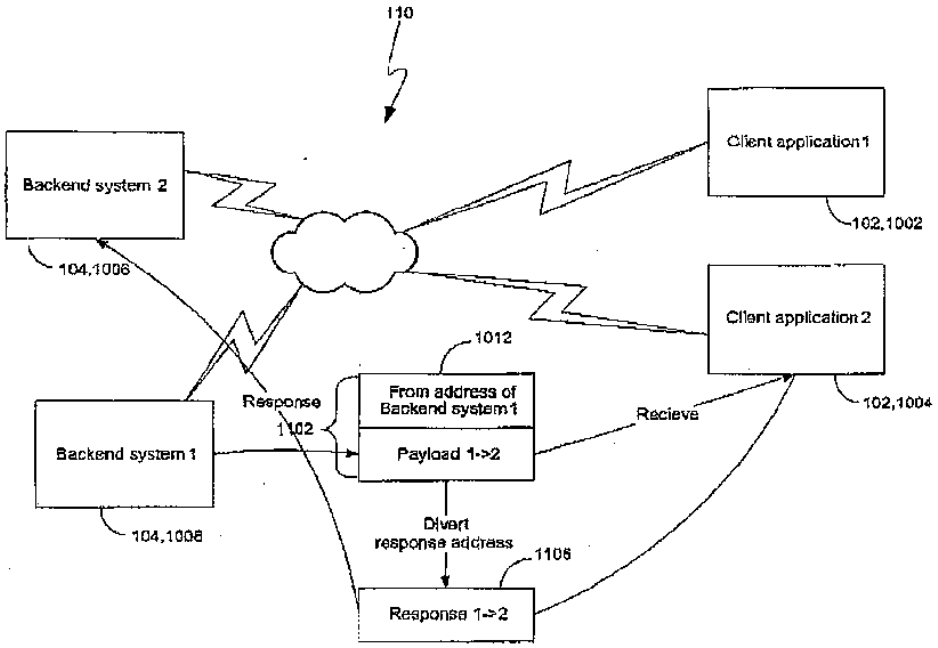

110
Backend system 2
Client application1
102,1002
104,1006
Client application 2
1012
From address of Backend system1
Response 1102
Backend system 1
Payload 1->2
Recieve
102,1004
Divert response address
1106
104,1008
Response 1->2

FIGURE 12

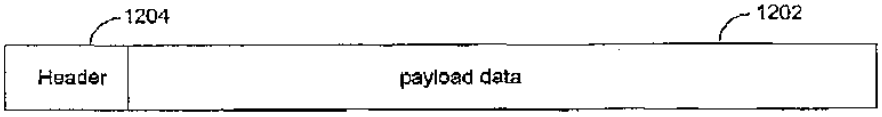


FIGURE 13

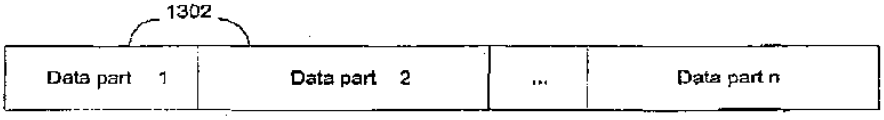


FIGURE 14

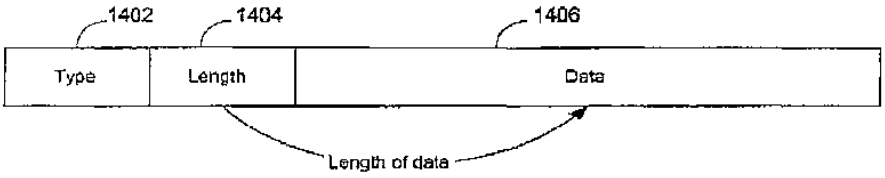


FIGURE 15

Workflow instruction data structure

	Type	Data
Menu Single/Multiple Select	S,M	[PARAMETER] [TITLE] [ITEM1] [ITEM2].....[ITEMn]
Information Message	I	[TITLE] [MESSAGE]
Header Response	H	[HEADER]
Redirect Address	R	[PHONE NUMBER]
User Input	T	[PARAMETER] [LABEL] [TYPE]
Execute URL	E	[URL]
Jump to index	J	[CMD Index]
Go to previous Cmd	P	
Branch menu	B	[PARAMETER] [TITLE] [Label1,index1] [Label2,index2] .....[ITEMn]
No-op	N	
Store Permanent	K	[Title]
Clear Permanent Storage	Q	
Read System Property	P	[Property name]
Configuration Settings	C	[Configurations]

Type enumeration:
TYPE_ANY = 0;
TYPE_EMAILADDR=1;
TYPE_NUMERIC = 2;
TYPE_PHONENUMBER = 3;
TYPE_URL = 4;
TYPE_DECIMAL = 5;

FIGURE 16

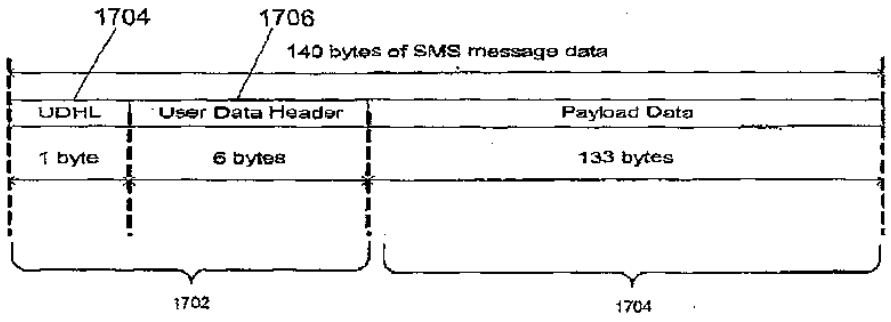

1704
1706
140 bytes of SMS message data
UDHL
User Data Header
Payload Data
1 byte
6 bytes
133 bytes
1702
1704

FIGURE 17

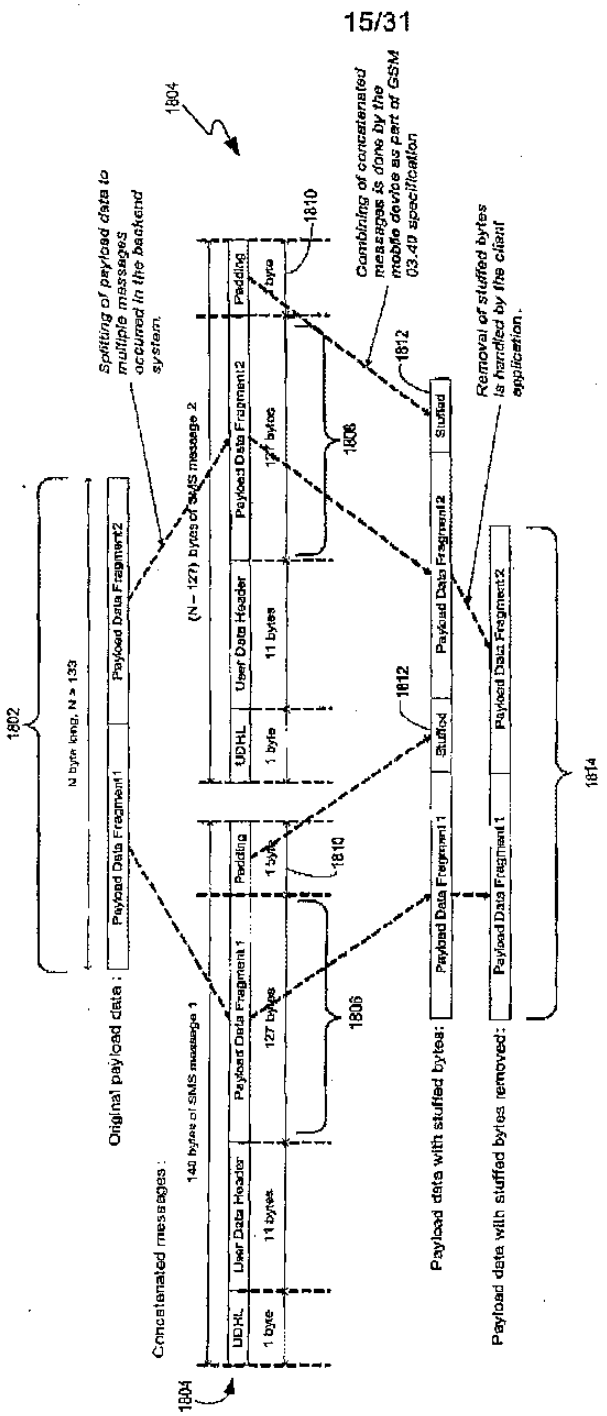


FIGURE 18

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 845 of 1360

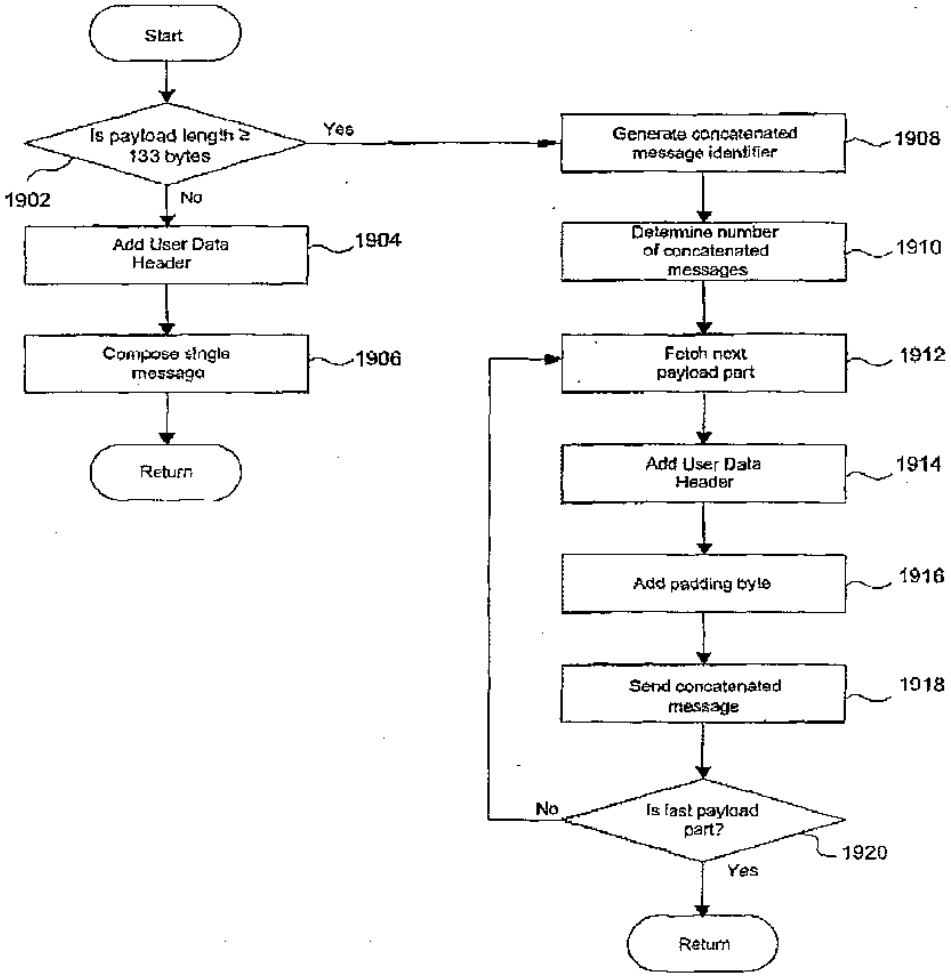

Start
Is payload length ≥ 133 bytes
Yes
No
1902
Add User Data Header
1904
Compose single message
1906
Return
Generate concatenated message identifier
1908
Determine number of concatenated messages
1910
Fetch next payload part
1912
Add User Data Header
1914
Add padding byte
1916
Send concatenated message
1918
Is last payload part?
1920
No
Yes
Return

FIGURE 19

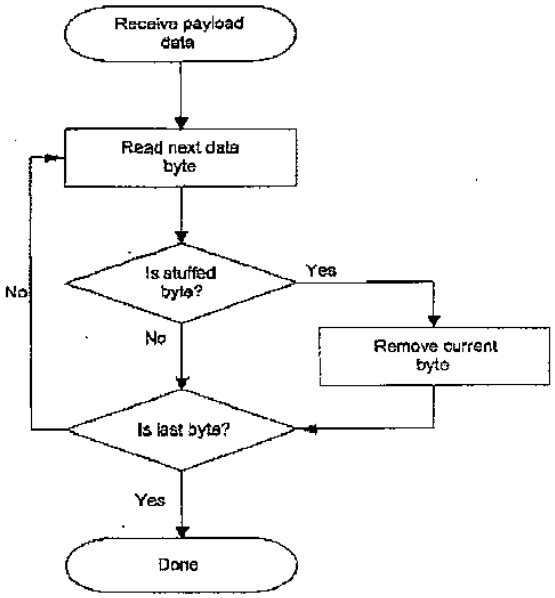

Receive payload data
Read next data byte
Is stuffed byte?
Yes
No
Remove current byte
Is last byte?
No
Yes
Done

FIGURE 20

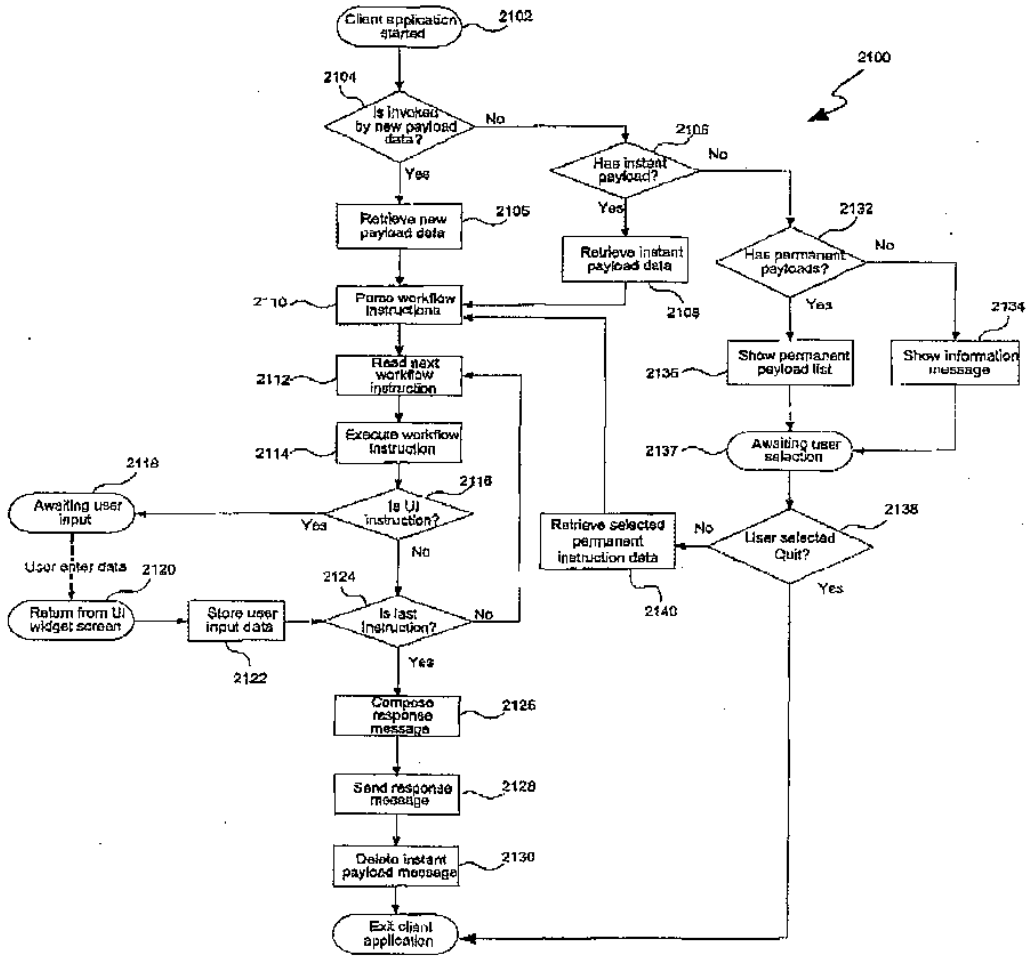

Client application started
2102
2100
2104
Is invoked by new payload data?
No
Yes
2106
Has instant payload?
No
Yes
Retrieve new payload data
2105
Retrieve instant payload data
2108
2132
Has permanent payloads?
No
Yes
2134
Show information message
Parse workflow instructions
2110
Read next workflow instruction
2112
Show permanent payload list
2136
Execute workflow instruction
2114
2137
Awaiting user selection
2118
Awaiting user input
Yes
Is UI instruction?
2116
No
Retrieve selected permanent instruction data
2140
2138
No
User selected Quit?
Yes
User enter data
2120
Return from UI widget screen
Store user input data
2122
2124
Is last instruction?
No
Yes
Compose response message
2126
Send response message
2128
Delete instant payload message
2130
Exit client application

FIGURE 21

0	Instruction 1 response
1	Instruction 2 response
n	Instruction n response

FIGURE 22

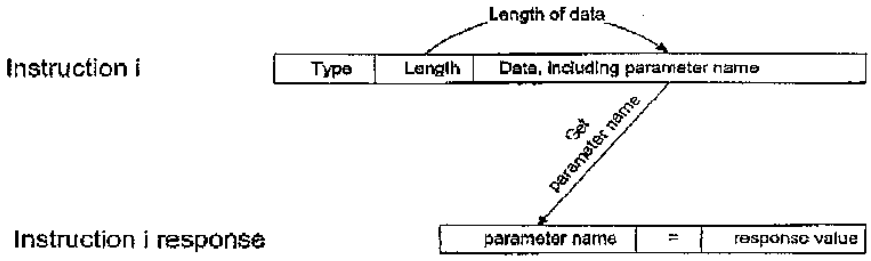


FIGURE 23

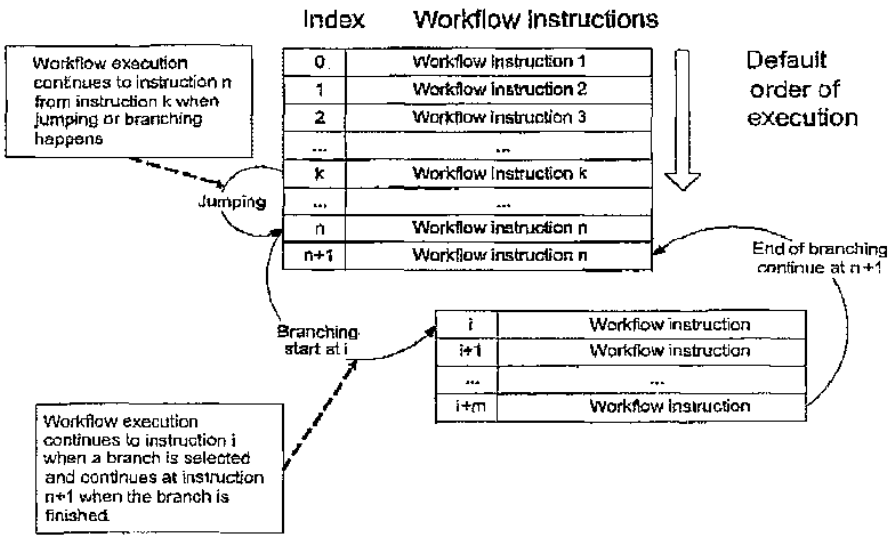

Index
Workflow Instructions
Workflow execution continues to instruction n from instruction k when jumping or branching happens
0
Workflow Instruction 1
1
Workflow Instruction 2
2
Workflow Instruction 3
...
...
k
Workflow Instruction k
...
...
n
Workflow Instruction n
n+1
Workflow Instruction n
Default order of execution
Jumping
End of branching continue at n+1
Branching start at i
i
Workflow instruction
i+1
Workflow instruction
...
...
i+m
Workflow instruction
Workflow execution continues to instruction i when a branch is selected and continues at instruction n+1 when the branch is finished.

FIGURE 24

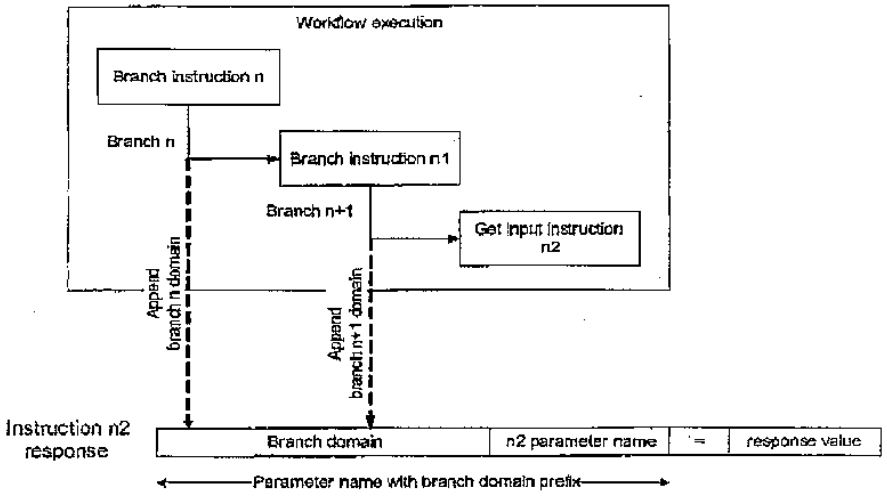

Workflow execution
Branch instruction n
Branch n
Branch instruction n1
Branch n+1
Get input instruction n2
Append branch n domain
Append branch n+1 domain
Instruction n2 response
Branch domain
n2 parameter name
=
response value
Parameter name with branch domain prefix

FIGURE 25

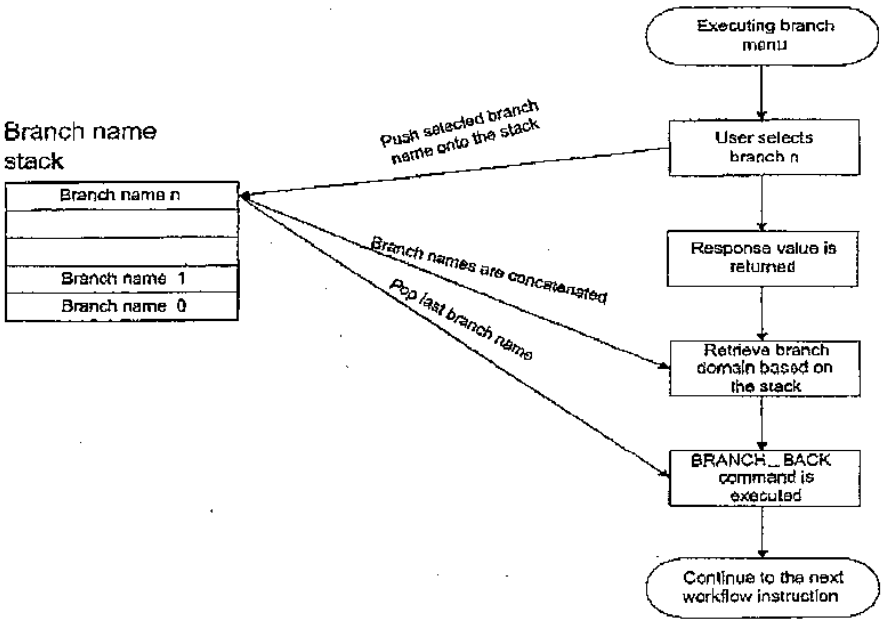

Executing branch menu
User selects branch n
Response value is returned
Retrieve branch domain based on the stack
BRANCH_BACK command is executed
Continue to the next workflow instruction
Branch name stack
Branch name n
Branch name 1
Branch name 0
Push selected branch name onto the stack
Branch names are concatenated
Pop last branch name

FIGURE 26

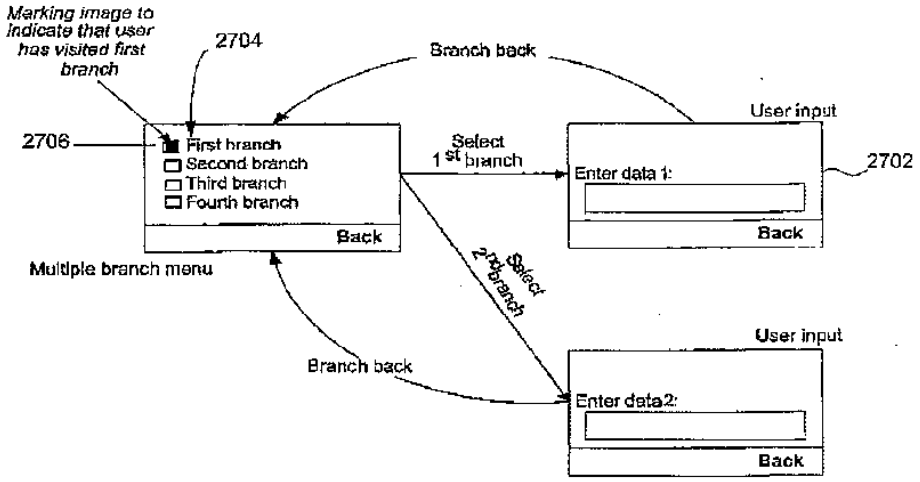


FIGURE 27

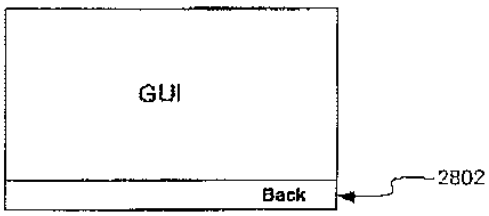


FIGURE 28

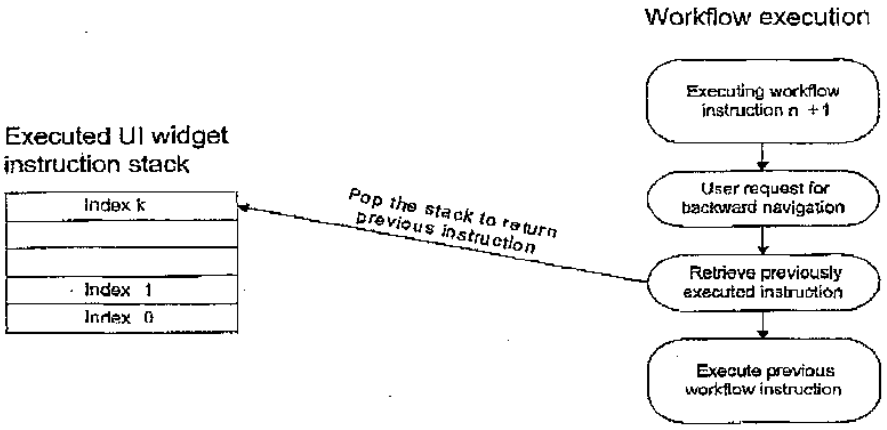

Workflow execution
Executing workflow instruction n +1
User request for backward navigation
Retrieve previously executed instruction
Execute previous workflow instruction
Pop the stack to return previous instruction
Executed UI widget instruction stack
Index k
Index 1
Index 0

FIGURE 29

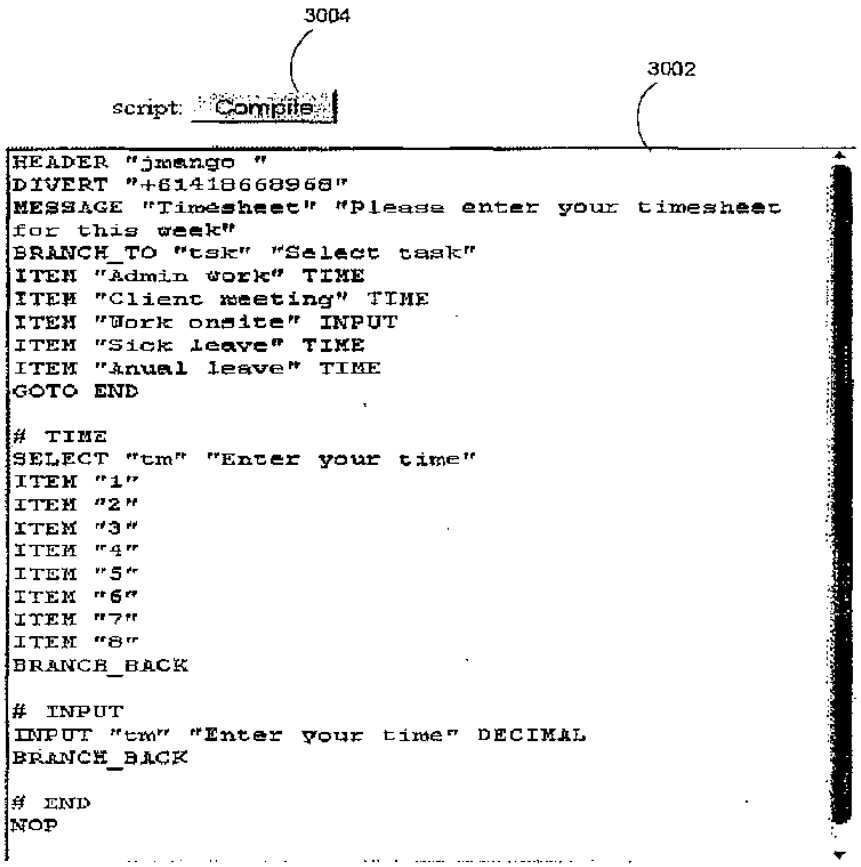

3004
3002
script:
Compile
HEADER "jmango "
DIVERT "+61418668968"
MESSAGE "Timesheet" "Please enter your timesheet for this week"
BRANCH_TO "tsk" "Select task"
ITEM "Admin work" TIME
ITEM "Client meeting" TIME
ITEM "Work onsite" INPUT
ITEM "Sick leave" TIME
ITEM "Anual leave" TIME
GOTO END
TIME
SELECT "tm" "Enter your time"
ITEM "1"
ITEM "2"
ITEM "3"
ITEM "4"
ITEM "5"
ITEM "6"
ITEM "7"
ITEM "8"
BRANCH_BACK
INPUT
INPUT "tm" "Enter your time" DECIMAL
BRANCH_BACK
END
NOP

FIGURE 30

```
private string SendWorkflowRequest(string sourceNumber,
    string destinationNumber, string bookingHeader,
    string bookingTitle, string bookingDetails)
{
3102 ──→ J2MECommand workflowCommand = new J2MECommand();
3104 ──→ if(bookingHeader != null)
             workflowCommand.AddCmdHeader(bookingHeader);

    // Add information message
3106 ──→ workflowCommand.AddInfoMessage(bookingTitle, bookingDetails);
    // Add selection menu
3108 ──→ workflowCommand.AddSingleMenu("action", "Select", new String[]{"Accept", "Reject"});
    // Add input text box to enter name
3110 ──→ workflowCommand.AddUserInputCmd("name", "Enter your name", J2MECommand.InputType.ANY);
    // Add input text box to enter contact number
3112 ──→ workflowCommand.AddUserInputCmd("contact", "Contact number", J2MECommand.InputType.PHONENUMBER);
    // Add redirection address where the response message is sent to
3114 ──→ workflowCommand.AddRedirectHeader("sms://1991616");

    // Now send the command, in multiple messages if it is neede
3116 ──→ IList messages = workflowCommand.BuildCommandMessages(1000);
    string sentIds = "";
    foreach(BinaryMessage binMessage in messages)
    {
3118    sentIds += _messageSender.SendBinaryMessage(sourceNumber, destinationNumber,
                                                    binMessage.UserData, binMessage.DataHeader);
        sentIds += ",";
    }
    return sentIds;
}
```

FIGURE 31

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 856 of 1360

27/31

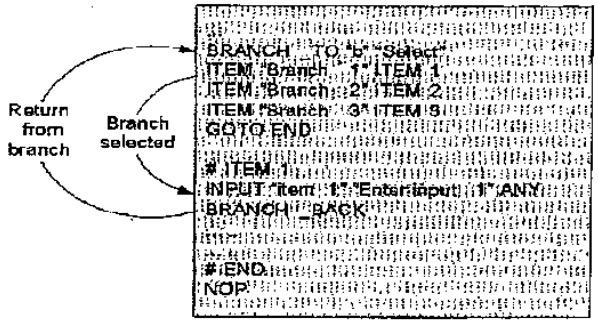


FIGURE 32

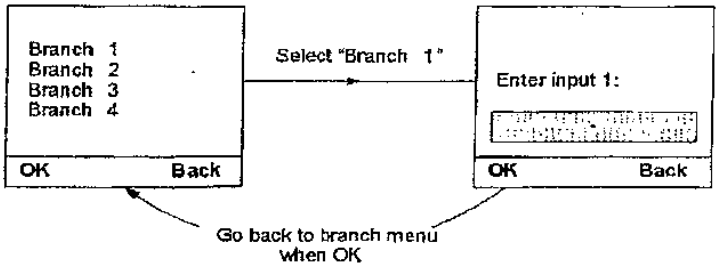


FIGURE 33

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 857 of 1360

28/31

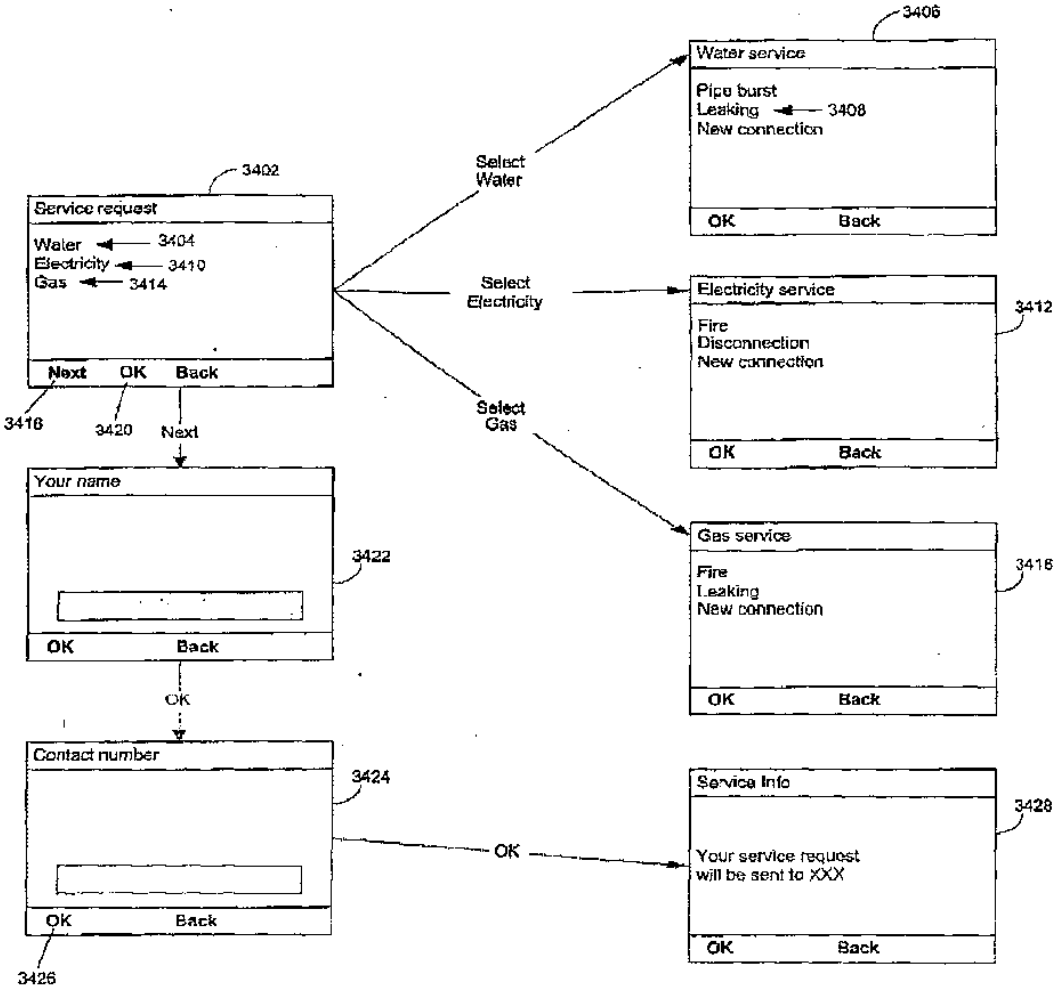


FIGURE 34

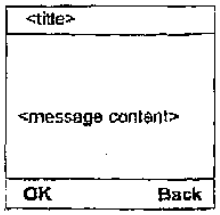


FIGURE 35

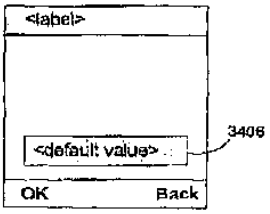


FIGURE 36

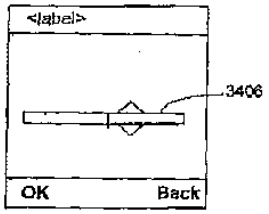


FIGURE 37

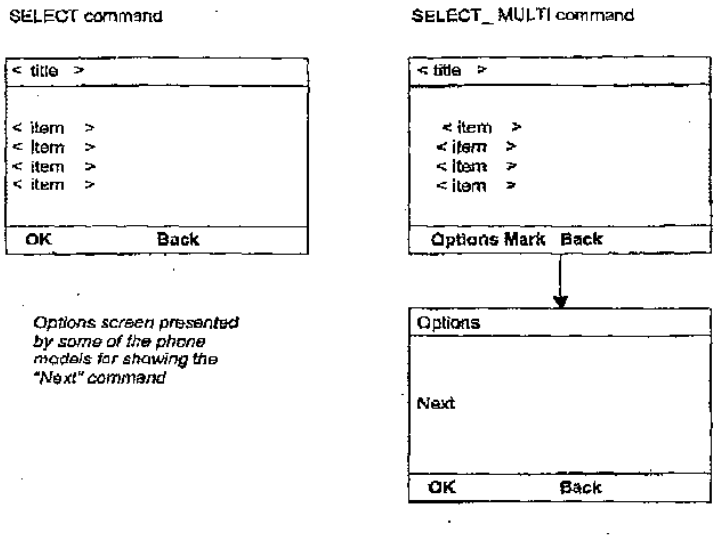

SELECT command
< title >
< item >
< item >
< item >
< item >
OK
Back
Options screen presented by some of the phone models for showing the "Next" command
SELECT_ MULTI command
< title >
< item >
< item >
< item >
< item >
Options Mark Back
Options
Next
OK
Back

FIGURE 38

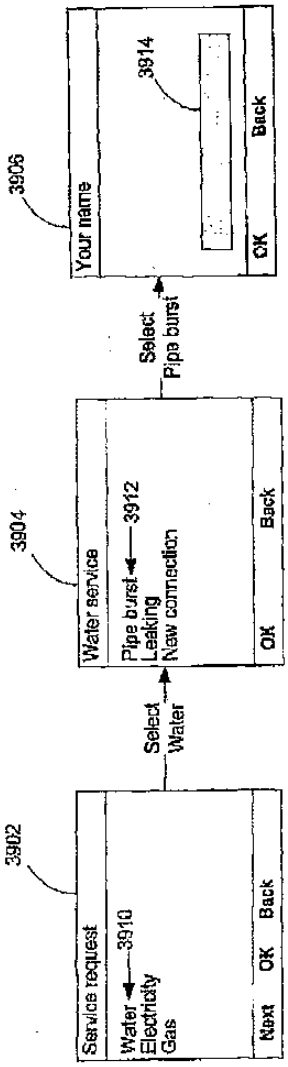
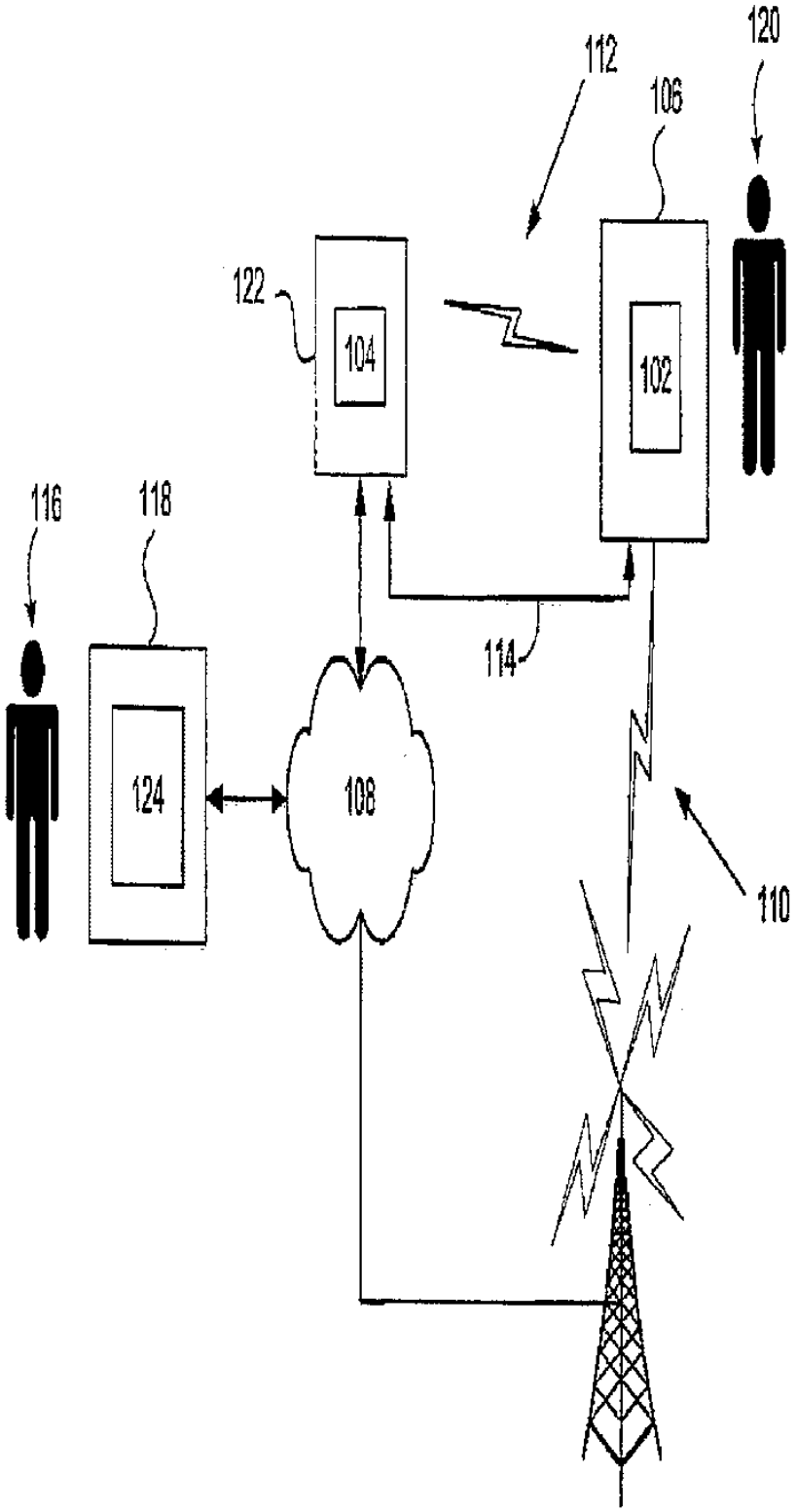


FIGURE 39

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 861 of 1360


112
120
106
122
104
102
116
118
114
124
108
110

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－297198
（P2001－297198A）
(43)公開日　平成13年10月26日(2001.10.26)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	２５０	Ｇ０６Ｆ　17/60	２５０	３Ｅ０４０
	２３４		２３４Ｚ	５Ｂ０４９
	２３６		２３６Ａ	５Ｂ０５５
	２３８		２３８	５Ｋ０２７
	５０６		５０６	５Ｋ１０１

審査請求　有　請求項の数８　ＯＬ　（全　６　頁）　最終頁に続く

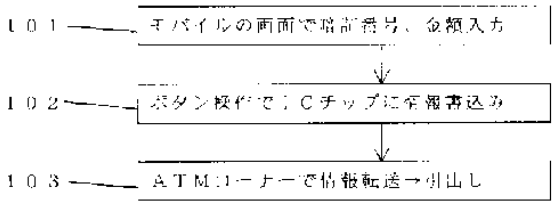
(21)出願番号　特願2000－113414(P2000－113414)
(22)出願日　平成12年４月14日(2000.4.14)

(71)出願人　599175026
株式会社三和銀行
大阪府大阪市中央区伏見町三丁目５番６号
(72)発明者　芦崎　武志
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内
(72)発明者　三砂　仁
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内
(74)代理人　100095267
弁理士　小島　高城郎　（外１名）

最終頁に続く

(54)【発明の名称】　携帯電話に組み込まれる金融処理システム

(57)【要約】
【課題】　携帯電話に種々の金融コンテンツを組込むことにより、携帯電話を利用してＡＴＭからの迅速な現金引出し、各種入出金処理の実行等を容易に行う。
【解決手段】　携帯電話に組み込まれる金融処理システムにおいて、携帯電話がＩＣチップを内蔵すると共に、ＩＣチップからＡＴＭへ非接触にてデータ転送するためのデータ転送手段を設け、暗証番号及びＡＴＭにおける金融処理情報を前記携帯電話に入力した後ＩＣチップに書込み、データ転送手段を介してＩＣチップからＡＴＭへ転送し、ＡＴＭは転送された入力情報に基づいて金融処理を実行する。



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 863 of 1360

1

【特許請求の範囲】

【請求項１】　ＡＴＭにおける金融処理を実行するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、

前記携帯電話がＩＣチップを内蔵すると共に、該ＩＣチップから前記ＡＴＭへ非接触にてデータ転送するためのデータ転送手段を設け、

前記入力手段を用いて銀行口座に係る暗証番号及び前記ＡＴＭにおける金融処理に係る情報を前記携帯電話に入力した後、該入力した情報を前記ＩＣチップに書込み、

前記データ転送手段を介して前記携帯電話の前記ＩＣチップから前記入力情報を前記ＡＴＭへ転送し、

前記ＡＴＭは転送された前記入力情報に基づいて前記銀行口座に係る前記金融処理を実行することを特徴とする携帯電話に組み込まれる金融処理システム。

【請求項２】　前記金融処理が、残高照会、引出し、入出金明細照会、振込み及び振替を含む群の中から選択されることを特徴とする請求項１に記載の携帯電話に組み込まれる金融処理システム。

【請求項３】　銀行口座の入出金状況を確認するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、

前記携帯電話により前記銀行口座の入出金状況に係る情報を格納したデータベースへ電話回線によりアクセスしデータを取得し、

前記取得したデータを前記表示手段に表示することを特徴とする携帯電話に組み込まれる金融処理システム。

【請求項４】　前記銀行口座の入出金状況に係る情報が、該銀行口座からの引落しに関する情報であって、引落日、引落内容及び引落金額を含むことを特徴とする請求項３に記載の携帯電話に組み込まれる金融処理システム。

【請求項５】　家計の収入支出状況を入力するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、

家計の収入支出状況に係る情報を前記入力手段により入力し、

前記家計の収入支出状況に係る情報を格納したデータベースへ電話回線によりアクセスすることにより前記入力されたデータを格納することを特徴とする携帯電話に組み込まれる金融処理システム。

【請求項６】　現在地及び最寄りのＡＴＭ設置場所に関する情報を取得するべく表示手段を具備する携帯電話に組み込まれるシステムにおいて、

電話回線により携帯基地局へアクセスし、携帯基地局がＧＰＳを実施することにより前記現在地及び前記最寄りのＡＴＭ設置場所に関する情報を取得し、

前記取得した情報を前記携帯電話へ返送し、

前記返送された情報を前記表示手段により表示することを特徴とする携帯電話に組み込まれるシステム。

2

【請求項７】　前記表示手段による表示に地図が含まれることを特徴とする請求項６に記載の携帯電話に組み込まれるシステム。

【請求項８】　請求項１乃至請求項７のいずれかに記載のシステムを組み込まれたことを特徴とする携帯電話

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯電話に組み込まれるアプリケーションシステム、特に、金融処理機能及び金融処理に関連する機能を具備するアプリケーションシステムに関する。

【０００２】

【従来の技術】昨今、携帯電話の機能は目覚しく発展しつつあり、インターネットのウェブページの閲覧や電子メールの送受信等、様々な機能が提供されている。その中には、個人の銀行口座の入出金処理いわゆるテレフォンバンキング機能も含まれる。テレフォンバンキングでは、利用者が電話機のプッシュボタンにより暗証番号等を入力した後、入出金処理の種類（振込み、振替等）や金額の入力操作を行うことにより所望する処理が行われる。入力操作に当たっては、自動音声案内または携帯電話の表示画面に表示される指示に従ってプッシュボタンにより適宜の項目を選択する。

【０００３】

【発明が解決しようとする課題】このように、携帯電話における金融処理機能いわゆる金融コンテンツを提供するアプリケーションが種々提供されているが、未だ、口座からの現金の引出し及び口座からの出金による商品代金の決済並びに当該口座の入出金データの整理・保存による家計簿機能等の総合的な個人バンキング処理を実行するアプリケーションは提示されていない。

【０００４】　一方、口座からの現金の引出しは、専らＡＴＭを利用して行われることが多いが、キャッシュカードをＡＴＭに挿入してから、暗証番号や引出し金額等の必要な情報をＡＴＭの入力装置に入力しなければならない。現状では、接触型のキャッシュカードが一般的に用いられており、カード挿入及びその後の入力操作に所定の時間が掛かるため、ＡＴＭの混雑時にはいっそうその混雑を増長させることとなる。

【０００５】以上の現状に鑑み、本発明は、携帯電話のアプリケーションとして個人バンキング処理を含めた総合的な機能を具備する金融コンテンツを組込むことにより、携帯電話を利用してＡＴＭからの迅速な現金引出し、各種入出金処理の実行、商品代金の決済、商品受渡し、入出金データの管理を容易に行うことを目的とする

【０００６】

【課題を解決するための手段】上記の目的を達成するべく、本発明は以下の構成を提供する。

【０００７】（１）ＡＴＭにおける金融処理を実行する

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 864 of 1360

べく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、前記携帯電話がＩＣチップを内蔵すると共に、該ＩＣチップから前記ＡＴＭへ非接触にてデータ転送するためのデータ転送手段を設け、前記入力手段を用いて銀行口座に係る暗証番号及び前記ＡＴＭにおける金融処理に係る情報を前記携帯電話に入力した後、該入力した情報を前記ＩＣチップに書込み、前記データ転送手段を介して前記携帯電話の前記ＩＣチップから前記入力情報を前記ＡＴＭへ転送し、前記ＡＴＭは転送された前記入力情報に基づいて前記銀行口座に係る前記金融処理を実行する。

【０００８】（２）上記（１）の構成において、前記金融処理が、残高照会、引出し、入出金明細照会、振込み及び振替を含む群の中から選択される。

【０００９】（３）銀行口座の入出金状況を確認するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、前記携帯電話により前記銀行口座の入出金状況に係る情報を格納したデータベースへ電話回線によりアクセスしデータを取得し、前記取得したデータを前記表示手段に表示する。

【００１０】（４）上記（３）の構成において、前記銀行口座の入出金状況に係る情報が、該銀行口座からの引落しに関する情報であって、引落日、引落内容及び引落金額を含む

【００１１】（５）家計の収入支出状況を入力するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、家計の収入支出状況に係る情報を前記入力手段により入力し、前記家計の収入支出状況に係る情報を格納したデータベースへ電話回線によりアクセスすることにより前記入力されたデータを格納する。

【００１２】（６）現在地及び最寄りのＡＴＭ設置場所に関する情報を取得するべく表示手段を具備する携帯電話に組み込まれるシステムにおいて、電話回線により携帯基地局へアクセスし、携帯基地局がＧＰＳを実施することにより前記現在地及び前記最寄りのＡＴＭ設置場所に関する情報を取得し、前記取得した情報を前記携帯電話へ返送し、前記返送された情報を前記表示手段により表示する。

【００１３】（７）上記（６）の構成において、前記表示手段による表示に地図が含まれる。

【００１４】（８）上記（１）乃至上記（７）のいずれかに記載のシステムを組み込まれた携帯電話である

【００１５】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。本発明における携帯電話（図中では、「モバイル」と称する）は、ＩＣカードに内蔵されると同様のＩＣチップを内蔵し、非接触にてＩＣチップへデータを入出力するために手段を具備する。ＩＣチップは、磁気記録媒体と比べてセキュリティ性が高くかつ大量の情報を記憶できることで知られている。さらに、この携帯電話は、データを入力するためのプッシュボタンまたは類似の入力手段並びにデータを表示するためのディスプレイを具備する

【００１６】一方、自動取引装置すなわちＡＴＭは、通常、タッチパネルまたはプッシュボタン等のデータの入力手段と表示手段を具備するが、本発明においては特に、非接触にて携帯電話のＩＣチップへデータを書込みまたデータを読取るための手段もまた具備する。

【００１７】斯かる携帯電話の所有者は、ＡＴＭを設置している銀行またはその銀行と提携する銀行に、口座を保有するものとする。当該口座に関連して、口座保有者のみが認知する暗証番号が設定されている。通常、口座保有者はキャッシュカードを所有しており、キャッシュカードをＡＴＭに適用することにより現金の引出しを行うことができる

【００１８】図１は、本発明による携帯電話における金融処理システムの１つである現金引出し機能を利用する場合の操作フローを示す概略的な流れ図である。ステップ１０１において、口座保有者は、携帯電話の入力手段を用いて暗証番号を入力する。暗証番号は高度の機密事項であるので、入力の際に画面上には暗証番号は明示されず、代わりに＊等の記号により入力字数のみが表示される。暗証番号の入力後、口座保有者は、引出し金額を入力する。

【００１９】入力後、ステップ１０２において携帯電話上に設けられた所定のボタンを押すことにより、あるいは他の適宜の操作により、携帯電話に内蔵されたＩＣチップに入力された情報を書込む。

【００２０】ステップ１０１及び１０２は、ＡＴＭ設置場所へ赴く前に予め行っておくことが好ましい。本発明の利点の１つは、ＡＴＭ設置場所以外の任意の場所で、予め現金引出しのための必要な操作を行うことができることである。

【００２１】ステップ１０３において、口座保有者はＡＴＭに赴き、携帯電話のＩＣチップ内の情報をＡＴＭの読取り手段に読取らせることにより、ＩＣチップ内の情報を転送する。これは、非接触にて行われる。ＡＴＭからオンラインにてホストコンピュータへの照会が実行され、暗証番号により本人確認できたならば、ＡＴＭから入力情報で指定された金額の現金が出金される。

【００２２】図２は、携帯電話での現金引出し操作における携帯電話のディスプレイ上の表示例を示した図である。先ず、初期画面においては、携帯電話に組み込まれる金融コンテンツの一覧が示される。例えば、残高照会、引出し、入出金明細照会、振込み、振替、マネーカレンダーである。マネーカレンダーについては後述する。ここでは「２．引出し」を選択するとする、すると、次画面で、暗証番号と引出し金額の入力が促される。

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 865 of 1360

【0023】図3は、図2の初期画面において「4．振込み」を選択する場合の表示例を示した図である。次画面において、本人確認のための暗証番号、振込み金額及び振込先を入力する。さらに、振込み操作においては、振込み相手に対するメッセージを添付することができる。メッセージを添付したい場合は、メッセージ内容及び相手のメールアドレスを入力する。これらの入力を終えたならば、入力情報をICチップに書込む。その後、ATMにおいて入力情報をATMに読取らせると、直ちに振込みが実行される。メッセージがある場合は、相手にメッセージが送られる。この振込み機能により、ショッピングが可能となる。例えば、商品販売する店舗の口座へ振込みを行うと共に、所望する商品内容をメッセージにて店舗に伝えることにより、商品代金の決済が完了し、後日商品が届けられることとなる。

【0024】図4は、図2の初期画面において「6．マネーカレンダー」を選択する場合の表示例を示した図である。「マネーカレンダー」においては、銀行口座の入出金状況の確認及び家計の収入支出に関する情報の入出力を行う。図4では、マネーカレンダーの項目として、引落日情報及び家計簿入力が挙げられている。「1．引落日情報」を選択した場合、電話回線を通して銀行のホストコンピュータの管理するデータベースへアクセスすることにより、近日中に口座引落しされる項目の情報を取得し、それが表示される。情報には、引落しの日付、内容及び金額が示されている。これにより口座保有者は、必要な口座残高を確保するよう注意することができる。

【0025】マネーカレンダーの「2．家計簿入力」を選択した場合は、家計簿へ記録すべき内容すなわち家計における収入支出状況を入力することができる。図5は、家計簿入力を選択した場合の表示例を示した図である。入力は、画面に表示された指示に沿って行えば容易に行える。先ず、利用金額を入力し、次に利用用途を複数の項目から選択することにより入力すると、確認画面が表示される。確認画面では、入力内容がまとめて示され、間違いなければ、「2．追加入力」を選択することにより、電話回線を通して銀行のホストコンピュータの管理するデータベースへアクセスし、入力データが送られ、データベースに入力データが格納される。家計簿情報は、入力を修正する場合は、「PDAで編集」を選択することにより編集する。尚、ショッピング内容を家計簿入力する場合、店舗のPOSと携帯電話が互いに通信し、店舗のPOSから入力データが転送されることにより、自動入力してもよい。

【0026】本発明に係る携帯電話は、好適にはJAVA言語を搭載しており、入力操作及びメモ・編集操作を効率的に行うことができる。

【0027】種々の金融コンテンツからなる金融処理システムを組み込んだ本発明の携帯電話は、近年、コンビニエンスストアに設置されるようになったATMや24時間営業ATMにおいて利用する場合に特に有用である。場所や時間を限定されること無く、いつでも容易にバンキング処理が可能となるからである。

【0028】従って、図6に示すATM設置場所情報提供機能を付加することにより、本発明に係る携帯電話は、さらに効果的に利用されることとなる。図6は、ATMの設置場所情報を提供する機能を具備する携帯電話のディスプレイ表示例を示す。ディスプレイ上には、現在地の周辺地図が表示されると共に、最も近い24時間営業の銀行ATM、及び、ATM設置コンビニエンスストアが表示されている。具体的な実施方法としては、携帯電話の基地局を活用してGPS（広域位置情報機能）サービスを実施する。携帯電話はJAVA言語を搭載しており、先ず、利用者が携帯電話を用いて基地局のホストへアクセスする。基地局のホストは、GPSを実施することにより携帯電話の現在位置情報を取得し、最寄りのキャッシュポイントすなわちATM設置場所の情報を地図及びテキストデータで携帯電話へ返送する。利用者はディスプレイに表示された地図を見て最寄りのATMを知ることができる。

【0029】

【発明の効果】本発明においては、携帯電話自体がICチップを搭載し、ICチップに書込んだ情報を非接触にてATMに読取らせることができる。従って、携帯電話をキャッシュカードの代わり用いてATM操作することができる。携帯電話のICチップには、予め必要な入力情報を書込んでおくことができるため、ATM設置場所においては、現金引出しや振込み等の処理を容易にかつ速やかに行うことができる。よってATMの混雑緩和に多大に寄与することとなる。

【0030】振込み機能にはメッセージ添付機能があり、オンラインショッピングの代金決済が可能であると同時に、商品の受渡しに関する情報をメッセージで伝えることができる。

【0031】また、携帯電話により、銀行口座の入出金及び家計の収入支出に関する情報の入力及び出力を行うことができるため、いつでも、どこでも簡単に日々のお金の利用状況を確認したり編集したりすることが可能となる。家計簿を継続的につけることは面倒であり長続きしないことが多いが、本発明のシステムを用いれば、クレジットカード等の引落日を確認しながら、無駄なく上手にお金を消費することができる。

【0032】さらに、携帯電話を通して24時間営業のATMや、ATMを設置したコンビニエンスストアの位置情報を得られるため、携帯電話に組み込まれた金融コンテンツを利用できる場所へ利用者を用意に導くことができ、極めて利便性の高いしシステムが実現される。

【図面の簡単な説明】

【図1】本発明による携帯電話における金融処理システ

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 866 of 1360

ムの１つである現金引出し機能を利用する場合の操作フローを示す概略的な流れ図である。

【図２】携帯電話での現金引出し操作における携帯電話のディスプレイ上の表示例を示した図である

【図３】図２の初期画面において「４．振込み」を選択する場合の表示例を示した図である。

【図４】図２の初期画面において「６．マネーカレンダー」を選択する場合の表示例を示した図である。

【図５】図４の次画面において「２．家計簿入力」を選択した場合の表示例を示した図である。

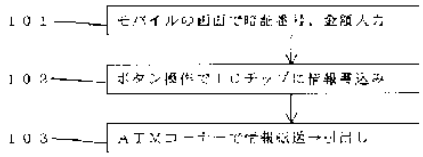
【図６】ＡＴＭの設置場所情報を提供する機能を具備する携帯電話のディスプレイ表示例を示す図である。

【符号の説明】

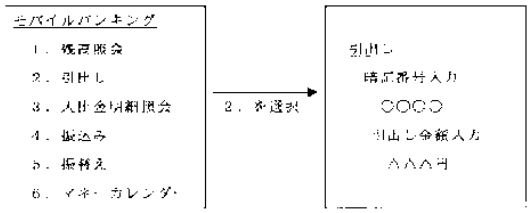
１０　携帯電話

１２　ディスプレイ

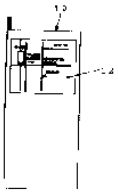
【図１】



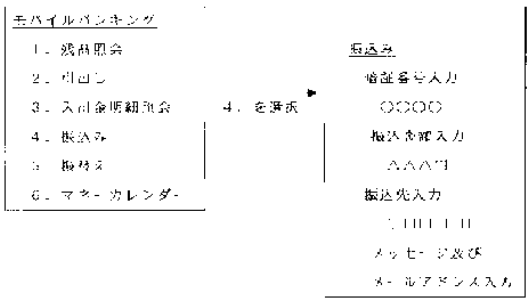
【図２】



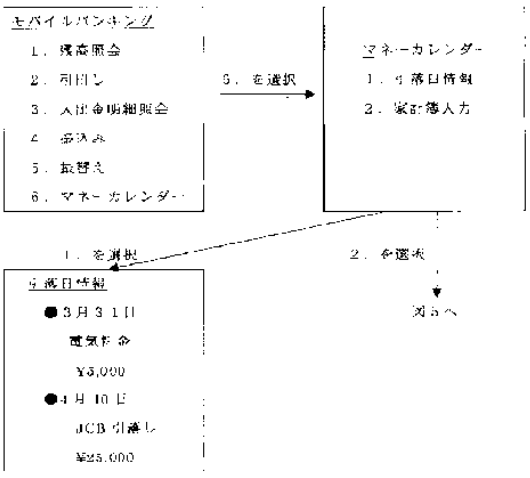
【図６】



【図３】

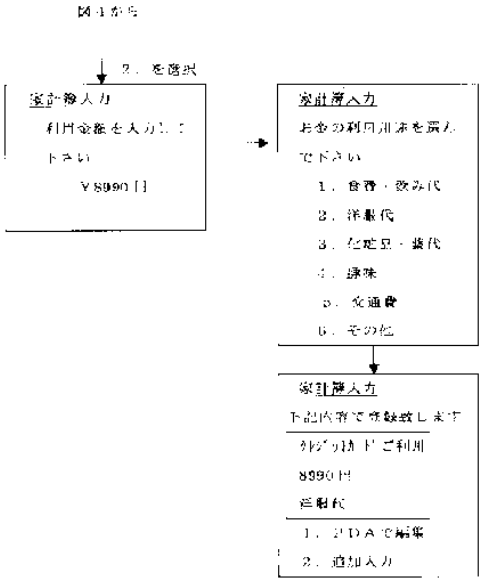


【図４】



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 867 of 1360

【図５】



フロントページの続き

(51)Int.Cl.⁷		識別記号	F I		テーマコード（参考）
G07D	9/00	451	G07D	9/00	451C　9A001
G07F	19/00		H04M	1/00	H
H04M	1/00			1/725	
	1/725			11/00	303
	11/00	303	G07D	9/00	476

(72)発明者　中村　喜治
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内
(72)発明者　山本　泰仁
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内
(72)発明者　森田　直樹
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内

Ｆターム(参考)　3E040 BA07 BA18 CA14 EA01 EA02 FH05
5B049 AA02 BB46 CC36 GG06
5B055 BB03 CB01 CB08 CB09 PA05 PA11
5K027 AA11 FF01 FF22
5K101 KK11 KK15 LL12 NN01 NN18
9A001 JJ64 KK56 KK58

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 868 of 1360

DERWENT-ACC-NO: 2002-023233

DERWENT-WEEK: 200203

COPYRIGHT 2012 DERWENT INFORMATION LTD

TITLE: Financial processing system in mobile telephones, has integrated circuit chip built in telephone, which stores input financial process information including bank account number which is then transmitted to ATM

INVENTOR: ASHIZAKI T; MISAGO H ; MORITA N ; NAKAMURA Y ; YAMAMOTO T

PATENT-ASSIGNEE: MIWA GINKO KK[MIWAN]

PRIORITY-DATA: 2000JP-113414 (April 14, 2000)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE
JP 2001297198 A	October 26, 2001	JA

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
JP2001297198A	N/A	2000JP-113414	April 14, 2000

INT-CL-CURRENT:

TYPE	IPC DATE
CIPP	G07D9/00 20060101
CIPS	G06Q10/00 20060101
CIPS	G06Q40/00 20060101
CIPS	G07F19/00 20060101
CIPS	H04M1/00 20060101
CIPS	H04M1/725 20060101
CIPS	H04M11/00 20060101

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 869 of 1360

ABSTRACTED-PUB-NO: JP 2001297198 A

BASIC-ABSTRACT:

NOVELTY - The financial process information input as a code number along with the bank account number is written in an integrated circuit (IC) chip built in a telephone. A data transmitter transmits the data from the IC chip to an automatic teller machine (ATM) which executes the financial process based on the transferred information.

USE - Is built in the mobile telephone for financial processing in banks.

ADVANTAGE - Performs quick and easy execution of various deposit and withdrawal processes, etc.

DESCRIPTION OF DRAWING(S) - The figure shows the flow diagram of operation of financial processing system. (Drawing includes non-English language text).

CHOSEN-DRAWING: Dwg.1/6

TITLE-TERMS: FINANCIAL PROCESS SYSTEM MOBILE TELEPHONE INTEGRATE CIRCUIT CHIP BUILD STORAGE INPUT INFORMATION BANK ACCOUNT NUMBER TRANSMIT ATM

DERWENT-CLASS: T01 T05 W01

EPI-CODES: T01-J05A; T05-L; T05-L03; W01-C01; W01-C01D1; W01-C05;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: 2002-018604

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 280 115 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.01.2003 Bulletin 2003/05

(51) Int Cl.7: **G07F 19/00**, G07F 7/08

(21) Application number: **02015629.5**

(22) Date of filing: **16.07.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.07.2001 JP 2001222163**
29.01.2002 JP 2002020410

(71) Applicant: **NTT DoCoMo, Inc.**
Tokyo 100-6150 (JP)

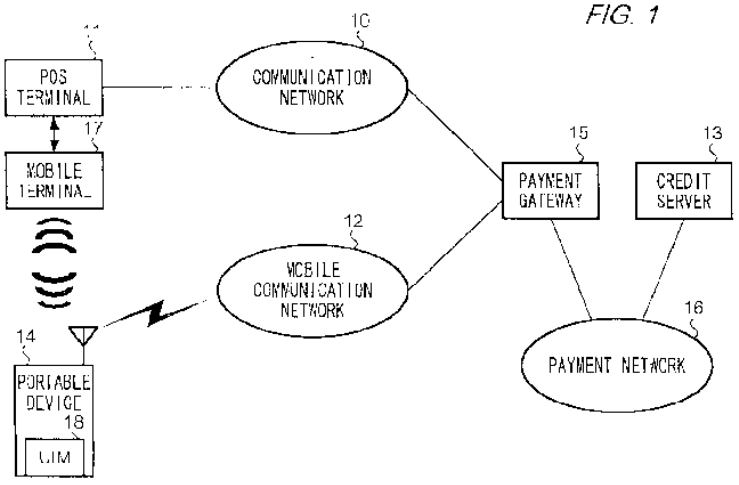
(72) Inventors:
- **Kinoshita, Masaki, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Yoshida, Junichi, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Nakajima, Atsushi, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Tanaka, Manabu, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Hanada, Kazutoyo, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Yasuda, Jun, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Tomita, Syuichi, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Nakamura, Taijiro, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Ishibashi, Hideaki, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**

(74) Representative: **HOFFMANN - EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) Electronic payment method, system, and devices

(57) A portable device authenticates a user of the portable device. If authenticity of the user is confirmed, a user ID is transmitted to a POS terminal. Upon receipt of the user ID, the POS terminal sends a request for payment including the user ID and transaction information to a payment gateway. Upon receipt of the request, the payment gateway sends an e-mail to the portable device to execute an application for payment stored in the portable device.

FIG. 1



EP 1 280 115 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 871 of 1360

Description

Background of the Invention

Field of the Invention

[0001] The present invention relates generally to a method, system and devices used for electronic financial transactions between financial institutions connected by a network.

Description of the Related Art

[0002] Electronic payment using a credit card is known in the art. As an example, a prior system for electronic payment is shown in fig. 21.

[0003] When a people (purchaser) buys goods at a shop, firstly, a clerk inputs transaction data including the name of goods, quantity, price, and tax into a Point of Sales (POS) terminal 1 provided at the shop. Secondly, he/she hand his/her credit card to the clerk. Thirdly, the clerk sets the card to a Card reader 2. Card reader reads out information such as a card number and expiration date stored in the card. Next, this card information is supplied to POS terminal 1. Upon receipt the information, POS terminal 1 makes a request for credit by adding information on the shop (merchant) to the card information and transaction data and sends it to a Credit server 4 manages by a credit card company via a Network 3 such as Credit Finance Information Switching Systems (CAFIS). Credit server 4 checks the card information includec in the request sent by POS terminal 11. Finally if Credit server 4 accepts authenticity of the card, it sends a completion message to POS terminal 1. In such a system, a consumer buys goods without carrying cash.

[0004] However it is known that there is a security concern in such a system. Since a purchaser has to hand his/her credit card to a clerk in paying by a credit card, there is a danger that unauthorized persons improperly use the card. Furthermore, there is always possibility of dropping off a credit card. In other words, a consumer necessarily takes risks that a stranger uses his/her credit card illegally.

[0005] The present invention has been made with a view to overcome the above problem and it is an object of the present invention to provide a method, system, server, terminal, computer program, and storage medium to conduct electronic financial transactions.

Summary of the Invention

[0006] To achieve the above aim, an electronic payment method of the present invention comprises the steps of:

authenticating a user of a user terminal on the basis of user identification information inputted to the user terminal by the user, by the user terminal;

storing an authentication result of the user, by the user terminal when the user terminal confirms authenticity of the user;

transmitting a user identification information stored beforehand in the user terminal to a merchant terminal when the user terminal confirms authenticity of the user, by the user terminal;

transmitting to payment device via a first communication network the user identification information and transaction information transmitted from the user terminal, by the merchant terminal;

receiving the user identification information and the transaction information transmitted from the merchant terminal, by the payment device;

identifying the user terminal on the basis of the user identification information and transmitting commands for instructing transmission of the authentication result to the user terminal via a second communication network;

transmitting authenticity of the user to the payment device via the second communication network if the user terminal stores authenticity of the user, by the user terminal; and

performing payment processing on the basis of the transaction information upon receipt of the authenticity from the user terminal, by the payment device.

[0007] In an electronic payment system in which the above method is applied, a user is able to pay by credit card using a terminal without handing a credit card to a clerk, thereby preventing a third-party including a clerk from using the card improperly. Furthermore, since the user terminal authenticates a user, if a third-party obtains a user terminal improperly, the terminal cannot be used for payment in the electronic payment system by the third-party. Furthermore, the payment device identifies a user to which authentication result is transmitted. In other words, the only user terminal that the payment device specifies can proceed payment processes. Thus, the danger of an improper use by a third-party of the user terminal is reduced. Furthermore, the user terminal transmits an authentication result according to the commands send from the payment device, in other words, a user does not have to operate the user terminal for the transmission. Therefore, the danger of stop of payment processing due to misoperation by a user is prevented.

[0008] In a preferred embodiment, an electronic payment method of the present invention comprises the steps of:

authenticating a user of a user terminal on the basis of user identification information inputted to the user terminal by the user, by the user terminal;

transmitting user identification information for identifying a user to a merchant terminal, by the user terminal, when the user terminal confirms authen-

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 872 of 1360

ficity of the user;
transmitting to a payment device via a first communication network the user identification information transmitted from the user terminal, by the merchant terminal;
receiving the user identification information from the merchant terminal, by the payment device;
identifying the user terminal referring to received user identification information and transmitting commands for executing an application for payment stored in the user terminal to identified user terminal via a second communication network, by the payment device;
upon receipt of the commands, executing the application to transmit a request for proceeding payment processing to the payment device via the second communication network, by the user; and
upon receipt of the request from the user terminal, performing a payment processing.

[0009] In this embodiment the payment device identifies a user terminal on the basis of user identification information and sends commands so that the user terminal can execute application for payment stored in the user terminal. In other words, both a user and a user terminal are authenticated, thereby ensuring security against authorized person greatly. In addition, a user's convenience is improved because a user does not have to carry out troublesome operation necessary for payment.

[0010] In another embodiment an electronic payment method comprises the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal, by a receiving unit
retrieving from a storage unit a card number corresponding to the
identified user, by a retrieving unit
encrypting the retrieved card number, by an encryting unit;
generating a key for decryption of the encrypted card number, by a generating unit;
transmitting to the merchant terminal the encrypted card number, by a first transmitting unit; and
transmitting the key to a credit server managed by an issuer of the credit card, by a second transmitting unit.

[0011] In an electronic payment system in which a method of this embodiment of the present invention is used, a user is able to pay by credit card to a merchant in a way that the merchant does not know a card number because a credit card number is encrypted for transmission to the merchant. Specifically, a payment device determines a card to be encrypted on the basis of the user identification information. On the other hand, the credit server obtains a card number by decrypting an encrypted card number using the key for decryption received from the payment device. Thus the credit server is able to carry out payment processing. Further, since the encrypted card number is generated each time a transaction is conducted, the merchant can manage sales at the shop using the encrypted card number although the merchant does not know card numbers.

[0012] An electronic payment system of the present invention has a payment device, a merchant terminal connected with the payment device via a first communication network and a user terminal connected with the payment device via a second communication network and is characterized in that:

the user terminal authenticates a user of the user terminal on the basis of user identification information inputted to the user terminal by the user;
if authenticity of the user is confirmed, stores authentication result; and
transmits to the merchant terminal user identification information stored in the user terminal;
the merchant terminal transmits to the payment device via the first communication network the user identification information transmitted from the user terminal and transaction information;
the payment device identifies the user terminal on the basis of the user identification information transmitted from the merchant terminal and
transmits to the identified user terminal via the second communication network commands for instructing transmission of the authentication result;
the user terminal transmits to the payment device via the second communication network according to the commands transmitted from the payment device when the user terminal stores the authentication result; and
upon receipt of the authentication result from the user terminal, the payment device performs payment processing on the basis of the transaction information.

[0013] In a preferred embodiment, an electronic payment system of the present invention is characterized in that:

the user terminal authenticates a user on the basis of the user identification information inputted to the user terminal by the user;
if authenticity of the user is confirmed, transmits to the merchant terminal a user identification information for identifying the user;
the merchant terminal transfers the user identification information to the payment device via the first communication network;
the payment device identifies the user terminal on the basis of the user identification information and transmits to the identified user terminal via the second communication network commands for execut-

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 873 of 1360

ing an application for payment stored in the user terminal;
the user terminal executes the application according to the commands and
transmits a request for proceeding payment processing to the payment device via the second communication network; and
the payment device performs the payment processing according to the request.

[0014] A communication terminal used for an electronic payment system of the present invention has a payment device connected with a first and a second communication network and a merchant terminal connected with the payment device via a first communication network and comprises

an authenticating means for authenticating a user of the communication terminal on the basis of a user identification information inputted to the user terminal by the user;
a storing means for storing an authentication result when authenticity of the user is confirmed by the authenticating means;
a storage medium for storing the user identification information;
a first transmitting means for transmitting, when authenticity of the user is confirmed, the user identification information stored in the storage means to the merchant terminal so that the merchant terminal transmits to the payment device a request for payment processing including the user identification information;
a receiving means for receiving commands for instructing transmission of the authentication result which is transmitted, in response to the request for payment, from the payment device via the second communication network; and
a second transmitting means for transmitting, upon receipt of the commands, a request for proceeding the payment processing including the authentication result to the payment device via the second communication network.

[0015] In a preferred embodiment, a communication terminal used for the electronic payment system comprises:

an authenticating means for authenticating a user of the communication terminal on the basis of a user identification information inputted to the user terminal by the user;
a first transmitting means for transmitting, when authenticity of the user is confirmed, the user identification information stored in the storage means to the merchant terminal so that the merchant terminal transmits to the payment device a request for payment processing including the user identification information
a receiving means for receiving commands for executing an application for payment which is transmitted from the payment device via the second communication network; and
a second transmitting means for executing the application for payment stored in the user terminal and transmitting, according to the application, a request for proceeding payment processing to the payment device via the second communication network.

[0016] A payment device of the present invention comprises:

a receiver for receiving a request for payment including a user identification information for identifying a user of a user terminal from a merchant terminal via a first communication network;
an identifying means for identifying the user terminal among registered user terminal on the basis of the received user identification information a transmitter for transmitting to the identified user terminal via a second communication network commands for executing an application for payment stored in the user terminal; and
a processing means for performing a payment processing on the basis of a request sent from the user terminal via the second communication network after transmission of the commands.

[0017] In another embodiment a payment device comprises:

a storage unit for storing a user identification information for identifying a user of a user terminal and a card number of a credit card correspondingly; a receiving unit for receiving from a merchant terminal a user identification information
a retrieving unit for retrieving from the storage unit a card number corresponding to the identified user;
an encrypting unit for encrypting the retrieved card number;
a generating unit for generating a key for decryption of the encrypted card number
a first transmitting unit for transmitting to the merchant terminal the encrypted card number and
a second transmitting unit for transmitting the key to a credit server managed by an issuer of the credit card.

[0018] A computer program product of the present invention makes a computer incorporated into a communication terminal used for the electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with the payment device via a first communication network to execute the steps of:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 874 of 1360

authenticating a user of the communication terminal on the basis of a user identification information inputted to the user terminal by the user;
storing an authentication result into a storage means when authenticity of the user is confirmed by the authenticating means;
transmitting, when authenticity of the user is confirmed, the user identification information stored in the storage means to the merchant terminal so that the merchant terminal transmits to the payment device a request for payment processing including the user identification information;
receiving commands for instructing transmission of the authentication result which is transmitted, in response to the request for payment, from the payment device via the second communication network and
transmitting, upon receipt of the commands, a request for proceeding the payment processing including the authentication result to the payment device via the second communication network.

[0019] In another embodiment, a computer program product makes a computer to execute the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal;
retrieving from a storage unit a card number corresponding to the identified user;
encrypting the retrieved card number;
generating a key for decryption of the encrypted card number transmitting to the merchant terminal the encrypted card number; and
transmitting the key to a credit server managed by an issuer of the credit card.

[0020] A storage medium of the present invention stores the above computer program products.

Brief description of the drawings

[0021]

Fig.1 is a conceptual block diagram to illustrate an electronic payment system based on the first embodiment of the present invention.
Fig.2 is a block diagram to illustrate a portable device used in the system.
Fig.3 illustrates a UIM mounted detachably to the portable device.
Fig.4 shows a storage area of EEPROM in the UIM.
Fig.5 is a block diagram to illustrate a POS terminal and a mobile terminal used in the system.
Fig.6 is a block diagram illustrating a payment gateway used in the system.
Fig.7 illustrates data items stored in a user table in a hard drive of the gateway.
Fig.8 illustrates data items stored in a transaction table in a hard drive of the gateway.
Fig.9 illustrates data items stored in an issuer table in a hard drive of the gateway.
Fig.10 illustrates data items stored in a merchant table in a hard drive of the gateway.
Fig.11 is a sequence flowchart illustrating payment processing in the system.
Fig.12 is a flowchart illustrating a processing performed by the portable device.
Fig.13 illustrates a screen displayed on a display of the portable device.
Fig.14 is a flowchart illustrating a processing performed by the portable device.
Fig.15 is a flowchart illustrating a processing performed by the portable device.
Fig.16 illustrates a screen displayed on a display of the portable device.
Fig.17 illustrates a screen displayed on a display of the portable device.
Fig.18 is a flowchart illustrating a processing performed by the POS terminal.
Fig.19 is a flowchart illustrating a processing performed by the payment gateway.
Fig.20 is a conceptual block diagram illustrating an electronic payment system based on a modification of the first embodiment.
Fig.21 illustrates an electronic payment system of the prior art.
Fig.22 illustrates an electronic payment system based on the second embodiment.
Fig.23 illustrates an example of date items stored in a POS terminal.
Fig.24 illustrates an example of date items stored in a credit server.
Fig.25 illustrates an example of date items stored in a storage unit of a payment gateway.
Fig.26 is a flowchart illustrating a method for payment used in the system.
Fig.27 is a flowchart illustrating a method for payment used in the system.
Fig.28 is a conceptual block diagram to illustrate a computer program for payment based on the second embodiment.

Detailed Description

(First embodiment)

[0022] The first embodiment of the present invention will now be described referring to the drawings.

A. Configuration of the system

A-1. Overall configuration

[0023] Fig. 1 shows that a system to which a method for electronic payment of the present invention based

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 875 of 1360

or the first embodiment is applied. As shown therein, the system comprises (a) a POS terminal 11 connected to a communication network 10, (b) a payment gateway 15 connected to Communication network 10, a mobile communication network 12, and a payment network 16, (c) a portable device 14 by which a user obtains communication services via Mobile communication network 12, (d) a credit server 13 connected to Payment network 16, and (e) a mobile terminal 17. For the sake of simplicity, only one POS terminal 11 and one Portable device 14 is shown in the figure. In actuality, a plurality of POS terminals are connected to Communication network 10 and many portable devices are connected to Mobile communication network 12.

[0024] A mobile communication network 12 includes mobile telephone networks in which Personal digital Cellular (PDC) scheme, Code Division Multiple Access (CDMA) scheme, or other schemes is used and data communication networks in which PDC-Packet (PDC-P) scheme is used. Each network has base stations which are not shown. Each base station covers an area and carries out radio communications with portable devices 14 within the area. Therefore, Portable device 14 is able to carry out voice and data communications by radio via Mobile communication network 12. A payment gateway 15 is connected to Mobile communication system 12, thus Portable device 14 is able to carry out data communications with Payment gateway 15.

[0025] A POS terminal 11 and Payment gateway 15 are connected via Communication network 10. Specifically, Communication network 10 is a dedicated line to which many POS terminals 11 and Gateway system 15 are connected. Needless to say, Communication network 10 can be a fixed telephone network, a public network such as Internet, or a mobile communication network (possibly Mobile communication network 12).

[0026] A credit server 13 managed by a credit company and Gateway system 15 are connected via a payment network 16. Specifically, Payment network 16 is designed especially for credit payment such as Credit and Finance Information Switching Systems (CAFIS). Credit server 13 is a conventional server for credit payment. Specifically, upon receipt of a request for credit transmitted by a POS terminal via Payment network 16, Credit server 13 checks authenticity of a credit card. If the authenticity is confirmed, Server 13 carries out a payment processing before sending a completion message to the POS terminal.

[0027] An essence of the electronic transaction service using a method for paying electronic transactions based on this embodiment is as follows. When a user of Portable device 14 buys goods at a shop, the user uses Portable device 14 to make request for payment to Credit server 13 via POS terminal 11 and Payment gateway 15. As such, a user is able to pay without handing a credit card to others including a clerk. Components of this system will be described in detail below.

A-2. Portable device

[0028] Portable device 14 has a function of carrying out wireless voice and data communications via Mobile communication network 12. Further, it has a function of carrying out short-range radio communication using Bluetooth, for example, to carry out data communications with POS terminal. In addition, the device 14 is able to mount a User Identity Module (UIM) detachably.

[0029] As shown in fig.2, Portable device 14 has a control unit 310, memory 320, control unit 330, communication unit 340, mic/speaker 350, UIM interface 360, and radio interface 370.

[0030] Control unit 310 has a Central processing unit (CPU) and other microprocessors to execute programs stored in Memory 320 to control each unit of the device 14 including reading/writing data from/to UIM 18.

[0031] Memory 320 includes a Read Only Memory (ROM), a Random Access Memory (RAM), and an Electrically Erasable and Programmable ROM (EEPROM) and has several storage areas, one of which is assigned for storing programs including programs for starting and proceeding payment described later, and another one of which is for storing data. Another program stored in Memory 320 is used for browsing, in other words, accessing a Web server on the Internet, downloading Hyper Text Markup Language (HTML) data or Compact-HTML (C-HTML) data, and displaying the data. Another one is used for sending and receiving e-mail. Control unit 310 executes these programs so that the user can browse and use e-mail.

[0032] Input device 330 has operation buttons such as a ten-key pad, which is not shown in the figure, to input information such as a telephone number and to select buttons or icons displayed on a liquid crystal display not shown in the figure. Communication unit 340 transmits data such as information on ordering via an antenna 341 under control of Control unit 34 and receives data send via Antenna 341. Mic/speaker 350 includes a microphone to input a sound and a speaker to output a sound.

[0033] UIM interface 360 supplies information outputted from Control unit 310 to UIM 18 and information outputted from UIM 18 to Control unit 310. Information stored in UIM 18 is used each time a user carries out voice and data communications by radio via Communication network 12. Radio interface 370 is used to carry out short-rage communication with POS terminal 11 by Bluetooth, for example.

A-3. UIM

[0034] As shown in fig.3, UIM 18 is an Integrated Circuit (IC) card which is detachable/attachable and includes a CPU 210, interface 215, ROM 220, RAM225, and EEPROM 230. UIM 18 stores information unique to the user including a subscriber number and telephone book used for carrying out communication via Mobile

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 876 of 1360

communication network 12.

[0035] CPU210 executes a control program stored in ROM 220 to control each unit with n UIM 18. Interface 215 connects UIM 18 with Portable device 14. ROM 220 is a nonvolatile memory and stores programs for analyzing and executing commands supplied from Portable device 14 and for managing data, for example, as well as the control program. RAM 225 is a rewritable memory for temporarily storing data supplied from Portable device 14. EEPROM 230 is a versatile and is rewritable. EEPROM 230 stores information necessary for communication with Portable device 14.

[0036] Fig.4 shows storage areas in EEPROM. As shown, EEPROM 230 has storage areas 231 and 233.

[0037] Storage area 231 stores subscriber numbers, outgoing history, incoming history, talk time, telephone book data, and other information specific to user(s) of UIM 18. Storage area 233 stores information used when Portable device 14 starts a payment operation. Specifically, a device ID for identifying Portable device 14 uniquely is stored. For example, a user registers in advance, Portable device 14 at a provider of this electronic financial transaction service to obtain the service using the device 14. After the registration, the provider gives the user the device ID.

[0038] In addition, Storage area 233 stores an address such as Uniform Resource Locator (URL), to connect with Payment gateway 15. Further, Storage area 233 stores pairs of a user ID and a password, each of which is used for an application for payment executed at the Portable device 14 when the user uses the electronic payment service. If the user possesses two or more credit cards, it is possible that each pair of a user ID and a password corresponds to each credit card. Furthermore, Storage area 233 has an area for authentication results which is used for the payment application.

[0039] When UIM 18 is attached to Portable device 14, information stored in UIM 18 can be supplied to Portable device via UIM interface 360, thereby allowing for Portable device 14 to carry out various functions including radio communication.

A-4. POS terminal

[0040] POS terminal 11 is installed at a shop of a merchant participating in the electronic payment service. POS terminal 11 stores data necessary for managing information on financial transactions, sales, and customers, for example.

[0041] As shown in fig.5, POS terminal 11 has a control unit 710, a display 720, communication interface 730, and an interface 740.

[0042] Control unit 710 includes a CPU, a ROM, and a RAM and controls all units of POS terminal 11. Control unit 710 has the same function as a general POS terminal for managing information on financial transactions, sales, and customers. In addition, Control unit 710 has functions of controlling each unit to perform processing necessary for the electronic payment service. Display 720 includes a liquid crystal panel, for example, on which information on merchandise such as a name, price, quantity, tax, and total amount is displayed. Communication interface 730 carries out communication with Gateway system 15 via Communication network 10. Interface 740 is, for example, a general interface such as RS-232C or Universal Serial Bus (USB). POS terminal 11 is connected to Mobile terminal 17 through a cable to carry out data communication.

[0043] Mobile terminal 17 is, for example, a Personal Digital Assistants (PDA) or a laptop computer, which includes a control unit 810, interface 820, display 840, and radio interface 830.

[0044] Control unit 810 includes a CPU, ROM, RAM, and other modules and controls all units of POS terminal. Control unit 810 has the same functions as a general mobile terminal such as PDA. In addition, Control unit 810 has a function of controlling each unit to carry out processing necessary for the electronic transaction service.

[0045] Display 840 includes a liquid crystal panel to display information, for example. Interface 820 is, for example, a general interface such as RS-232C or Universal Serial Bus (USB). POS terminal 11 is connected to Mobile terminal 17 through a cable to carry out data communication. Radio interface 830 features short-range wireless communication with Portable device 14 via Bluetooth, for example.

A-5. Payment gateway

[0046] Payment gateway 15 for providing the electronic payment service using a method for electronic payment based on this embodiment is installed by a provider of the service. As shown in fig.6, Payment gateway 15 includes a payment server 150 connected to a Local Area Network (LAN), direction server 160, and a network interface (I/F) 170.

[0047] Network interface 170 is, for example, a router. Payment server 150 and direction server 160 exchanges data with POS terminal 10, Portable device 14, and Credit server 13 via Communication network, Mobile communication network, and Payment network 16, respectively.

[0048] Payment server 150 may be a personal computer or a workstation, including a CPU 151, ROM 152, RAM 153, hard drive 154, and LAN interface 155. Further, Payment server 150 includes an input device such as a keyboard and Cathode-ray Tube (CRT) or Liquid Crystal Display (LCD) allowing an administrator of Gateway system 15 to make reconfigurations including registration of users.

[0049] LAN interface 155 is used for exchange of data between Network interface 170 and Direction server 160 connected to the LAN.

[0050] CPU 151 performs arrhythmic computation as well controls each unit of Payment server 150. ROM 152

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 877 of 1360

stores programs to be read out and executed by CPU 151. CPU uses RAM 153 as a work area.

[0051] Hard drive 154 stores application programs and data to be read out and executed by CPU 151 to control each unit for provision of the electronic transaction service. Hard drive 154 includes a user table 154a, transaction table 154b, issuer table 154c and merchant table 154d.

[0052] As shown in fig.7, user table 154a has four areas for user ID 154aa, password 154ab, terminal ID 154ac, and credit card number 154ad. A staffer of the provider of this service inputs the above information into User table 154a when a user subscribes to the service. It is possible that, if a subscriber has more than two credit cards and wants to obtain the service using these credit cards, the subscriber (user) has a plurality of user IDs each of which is corresponding to each credit card.

[0053] Area 154aa stores user IDs each of which identifies a subscriber uniquely. Area 154ab stores passwords each of which is used for authentication of a user. Area 154ac stores identification information on each to identify Portable device 14 used for the electronic transaction service. The user IDs, passwords, and identification information stored in Hard drive 154 are the same stored in Storage area 233 in EEPROM 230 of UIM 18 shown in fig. 4. Area 154ad stores credit card numbers of users. If a user has two or more credit cards, the user can specify one or more credit cards to be used for this service and thus stored in Area 154ad when the user subscribes to the service. In addition, Area 154ad stores expiration dates of the cards, which are not shown in the figures.

[0054] Referring back to fig. 6, Transaction table 154ab has areas for storing details of transactions conducted by users. Specifically, as shown in fig. 8, Transaction table 154ab corresponding to a subscriber having a user ID "00001" has four areas for transaction 154ba, for date 154bb, for merchant number 154bc, and for transaction details 154bd. Area 154ba stores IDs each of which identifies a transaction conducted by a user. It is noted that CPU 151 gives a transaction ID every time a transaction is conducted. Area 154ab stores dates and times of transactions each corresponding to each transaction ID. Area 154bc stores merchant numbers each identifying a shop where the transaction was conducted. A unique merchant number is assigned to all merchants in advance. Area 154bd stores details of transactions each corresponding to each transaction ID. Specifically, merchandise name, quantity, price, tax, payment method (lump-sum, installment, payment with bonus, payment partially with bonus, and, revolving, for example), and other related information on the transaction.

[0055] Referring again to fig. 6, Issuer table 154c stores information on credit companies and credit cards available for the service. Specifically, as shown in fig. 9, Issuer table 154c has three areas. Area 154ca stores ranges of card numbers. Area 154cb stores company codes each of which identifies corresponding credit company. Area 154cc stores names of credit companies. For example, fig. 9 shows that a credit card whose number lies within a range between "1525000000" and "1525059999" is issued by credit company "A".

[0056] Referring again to fig. 6, Merchant table 154c stores information on which cards and which methods of payment are available at a shop. Specifically, as shown in fig. 10, Merchant table 154d has four areas of 154da, 154db, 154dc, and 154dd. Area 154da stores codes each of which identifies each merchant. Area 154db stores merchants names. Area 154dc stores codes each of which identifies a credit company, namely, issuer of a credit card available for the merchant, which is the same stored in Area 154cb shown in fig. 9. Area 154dd stores credit company's names. Area 154de stores payment methods in which a user can pay by a card. As an example, fig. 10 shows that a user is able to arrange payment in a lump-sum, installments or revolving system but neither payment with bonus nor payment partially with bonus is accepted. "_", "I", "B", "pB", and "R" represents lump sum, installments, bonus, bonus (partially), and revolving, respectively. Furthermore, detailed information such as the number of payment in installments and an available period in payment with bonus may be stored.

[0057] Direction server 160 will now be described referring to fig. 6. Direction server 160 may be a personal computer or a workstation, including a CPU 161, ROM 162, RAM 163, hard drive 164, and LAN interface 165. Further, Payment server 150 includes an input device such as a keyboard and Cathode-ray Tube (CRT) or Liquid Crystal Display (LCD). Detailed description of these devices is omitted.

[0058] LAN interface 165 is used for exchange of data between Network interface 170 and Payment server 150 connected to the LAN. CPU 161 performs arithmetic computation as well controls each unit of Direction server 160. ROM 162 stores programs to be read out and executed by CPU 161. CPU uses RAM 163 as a work area. Hard drive 164 stores application programs and data to be read out and executed by CPU 161, to control each unit for provision of the electronic payment service. In addition, Hard drive 164 stores a mail box 164a used for the electronic transaction service. To be more specific, Mail box 164a includes mailboxes each corresponding to an e-mail account of Portable device 14.

[0059] Upon receipt of a request from Payment server 150, CPU 161 generates and stores e-mail into a mail box assigned to each Portable device 14 in Mail box 164a and sends a reception message to the Portable terminal 14 having an address indicated by the request. Upon receipt of the reception message, Portable device 14 accesses Mailbox 164a via Mobile communication network to obtain e-mails for Portable device 14. Namely, Direction server 160 a function as a mail server with features including sending a reception message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 878 of 1360

B. Operations of the system

B-1. Overall sequence of the operations

[0060] An outline of sequence of operations carried out in this electronic payment system will now be described.

[0061] Fig. 11 is a sequence flowchart showing an outline of sequence of operations in which a user of Portable device 14 conducts a transaction (purchases goods) at a shop at which POS terminal 11 and Mobile terminal 17 are installed and obtains this electronic payment service for payment using Portable device 14.

[0062] As shown in fig. 11, firstly, a clerk inputs information on a transaction including a merchandise name, quantity, price, tax into POS terminal 11 at a shop. If a purchaser wants to pay using this electronic payment service, the purchaser operates his/her Portable device 14 to execute an application program for the electronic payment. And an input screen for a user ID and a password to be used for authentication is displayed on a display of Portable device 14.

[0063] The purchaser (the user of Portable device 14) operates ten-key pad or the like, to input a user ID and a password. Portable device 14 checks the user ID and password against those stored in UIM 18, to authenticate the user (step S1).

[0064] If the authentication failed, Portable device 14 notifies the user that the user is not a right person and thus rejected before carrying out error processing, for example, terminating the processing. If the authentication is completed, Portable device 14 sends the user ID stored in UIM 18 to Mobile terminal 17 by short-range wireless communication. The user ID is transferred from Mobile terminal 17 to POS terminal 11 (step S2). In addition, Portable device 14 stores the authentication result representing authenticity of the user into Storage area 233 of UIM18. It is noted that Mobile terminal 17 is omitted in fig. 1 for sake of simplicity. But in reality data is exchanged via Mobile terminal 17 between POS terminal 11 and Portable device 14.

[0065] Upon receipt of a user ID sent from portable device 14 via Mobile terminal 17, POS terminal 11 sends to Payment gateway 15 via Communication network 10 transaction information, the user ID, and a request for transaction number including information to identify the shop (merchant), which is inputted buy a clerk (step S3). Upon receipt of the request sent from POS terminal, Payment gateway 15 stores the transaction information included in the request into Transaction table 154b and adds a transaction number to the transaction information to send back to POS terminal 11 via Communication network 10 (step S4).

[0066] Further, Payment gateway 15 sends an e-mail including commands for direction of payment to Portable device 14 indicated by the user ID included in the request (step S5). Upon receipt of the e-mail sent from Payment gateway 15 via Mobile communication system 12, Portable device 14 executes an application for payment according to the commands included in the e-mail.

[0067] Specifically, the authentication result and the device ID both stored in UIM 18 are transmitted to Payment gateway 15 via Mobile communication network 12, to make a request for proceeding payment processing (step S6). Therefore, the user need not do complicated procedures for payment, for example inputting information on the transaction which is often bothersome for a user. In this system a request for proceeding payment processing is sent to Payment gateway 15 automatically after completion of the authenticity.

[0068] Upon receipt of the authentication result and the request including the device ID both sent from Portable device 14 via Mobile communication network 12, Payment gateway 15 confirms authenticity of the user through the result. Next, Payment gateway 15 authenticates the Portable device 14 by checking the device ID (step S7). Specifically, Payment gateway 15 checks the device ID sent from Portable device 14 against a device ID stored correspondingly to the user ID in User table 154a. If the two IDs coincide, authenticity of Portable device 14 is established. Otherwise Payment Gateway 15 stops payment processing.

[0069] If the authenticity of Portable device 14 is established, Payment gateway 15 sends to Portable device 14 via Mobile communication network 12 transaction details including name of goods, quantity and price and information on possible payment methods (step S8). Upon receipt of a payment method and a confirmation from Portable device 14 (step S9), Payment gateway 15 retrieves transaction information from Transaction table 154b and a credit card number and its expiration date from User table 154a. Next, Payment gateway 15 sends to Credit server 13 via Payment network 16 a request for credit including information on the merchant and the payment method along with the retrieved transaction information (step S10).

[0070] Upon receipt of the request Credit server 13checks the credit card number and its expiration date, to determine whether to conduct the payment processing. If the credit card number and the expiration date are proper, Credit server 13 carries out payment processing (step S11) and sends a completion report to Payment gateway 15 via Payment network 15 (step S12). This report is transferred from Payment gateway 15 to POS terminal 11 via Communication network 10 and to Portable device 14 via Mobile communication network 12 (step S13 and step S14, respectively). B-2. Operations of portable device

[0071] It will now be described that processing carried out by Portable device 14 when a user obtains the electronic payment service. As shown in fig. 12, if a user wants to use the service using his/her Portable device 14 when purchasing goods at a shop, the user inputs with input device 330 a direction for Portable device to execute an application for payment. Control unit 310 of Portable device 14 displays credit cards available for the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 879 of 1360

user on a display

[0072] An example of a screen for selection of a credit card displayed on a display of Portable device 14 is shown in fig.13. This screen shows a list of credit cards registered in advance by the user at a provider of the service. When the user operates Input device 350 to select a check box and clicks an "OK" button, a credit card for use in the payment is determined.

[0073] After selection of a credit card, Control unit 310 displays an input screen for a user ID and a password on the display. When the user inputs a user ID and a password, Control unit 310 authenticates the user by the inputted user ID and password (step Sa3). Specifically, Control unit 310 compares a user ID and a password each corresponding to the selected credit card stored in Storage area 233 in EEPROM of UIM 18 with the inputted user ID and password. If the two user IDs and two passwords coincide, Control unit 310 confirms authenticity of the user. If not, it confirms inauthenticity. If the authenticity is confirmed (step Sa3 "NO"), Control unit 310 carries out error processing (step Sa4) for example, displays an error message on the display. If the authenticity is confirmed (step S3 "YES"), Control unit 310 stores the authentication result (authenticity) into Storage area 233 (step Sa5) and outputs the user ID stored in Storage area 233 to Radio interface 370 to transmit to Mobile terminal 17 (step Sa6). Then Control unit 310 terminates processing.

[0074] It is noted that when storing the authentication result into Storage area 233, Control unit 310 may write an expiration time of the authentication result, which is an hour, for example. After the expiration, Control unit 310 deletes the authentication result.

[0075] As a result, a user ID is sent from Portable device 14 to Mobile terminal 17 and subsequently a request for payment is sent from POS terminal to Payment gateway 15 (step S3 in fig.11). Next, an e-mail including commands to execute an application for payment (step S5 in fig.11) is transmitted from Payment gateway 15 to Portable device 14.

[0076] It will now be described that operations of Portable device 14 after reception of the e-mail sent from Payment gateway 15 referring to fig.14. Firstly, Control unit 310 checks whether an e-mail is received (step Sb1).

[0077] If Portable device 14 receives any e-mails, Control unit 310 terminates processing. If Portable device receives e-mail, Control unit 310 determines whether the e-mail is sent from Payment gateway 15 and checks whether the e-mail contains predetermined commands referring to the content of the e-mail (step Sb2).

[0078] If a sender of the e-mail is not Payment gateway 15 or the e-mail does not contain predetermined commands, Control unit 310 terminates the processing. If the sender is Payment gateway 15 and the e-mail contains predetermined commands, Control unit 310 executes an application for payment (step Sb3) before termination.

[0079] Control unit 310 repeats the above series of processes periodically so that the application for payment is executed automatically when receiving an e-mail including the commands.

[0080] It will now be described that operations of Portables device 14 after execution of the application referring to fig. 15.

[0081] Firstly, Control unit 310 reads out from Storage area 233 an address such as Uniform Resource Locator (URL), to access Payment gateway 15 via Mobile communication network 12 (step Sc1). To ensure security Secure Socket Layer (SSL) is used for data exchange between Portable device 14 and Payment gateway 15.

[0082] To be more specific, when sending a request for access to Payment gateway 15, Portable device 14 requests transmission of an electronic certificate issued by a Certificate Authority (CA) which is not shown in the figure. In response to the request, Payment gateway 15 sends the certificate to be confirmed by Portable device 14. Therefore, Portable device 14 is able to check authenticity of Payment gateway 15, thereby avoiding a danger of communication with an unauthorized server posing as an authorized server. After confirmation of authenticity of Payment gateway 15, data exchange starts. Needles to say, SSL is applied for such data exchange. Since SSL has become a common technique, detailed description is omitted.

[0083] After establishment of the connection between Portable device 14 and Payment gateway 15, Portable device 14 retrieves an authentication result (authenticity), a user ID, and a device ID from Storage area 233. Next, Portable device 14 transmits a request for authentication of the device 14 to Payment gateway 15 via Mobile communication network 12 to request including the retrieved user ID and device ID (step Sc2). At the same time, Control unit 310 measures time (step Sc3). If Portable device 14 does not receive information from Payment gateway 15 in response to the transmission after predetermined time (two minutes, for example), Control unit 310 terminates this processing and performs time-out processing, for example, displaying a message notifying to a user that this payment processing is aborted and must be carried out from the beginning.

[0084] As described before, when Portable device 14 sends an authentication result, a user ID, and a device ID to Payment gateway 15, Payment gateway 15 authenticates confirms the authenticity of the user and device 14. If the authenticity is confirmed, detailed transaction information is sent to Portable device (step S7 and step S8 of fig.11)

[0085] When authenticity is confirmed and thus information on transaction details (name of goods, quantity price, tax, merchant, for example) is transmitted from Payment gateway 15, Control unit 310 displays the transaction details on the display (step Sc4) to be checked by the user.

[0086] Fig.16 shows an example of a screen on which

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 880 of 1360

the transaction details is displayed. As shown therein, a name of merchant (shop), a total amount to be paid by the user, and buttons for direction. A user selects one of the buttons of "Agree" and "Not agree" for proceeding or stop paying, respectively. Control unit 310 determines which buttons is selected, in other words, whether the user agrees with this transaction (step Sc5).

[0087] If "Not agree" is selected (step Sc5 "NO"), Control unit 310 stops payment processing (step Sc6). If "Agree" is selected (step Sc5 "YES"), Control unit 310 transmits request for proceeding payment to Payment gateway 15 via Mobile communication network 12 (step Sc7).

[0088] In response to the request for proceeding payment, information on payment methods is transmitted from Payment gateway 15 via Mobile communication network 12, (step Sc8 in fig.11). Upon receipt of the information on payment methods, Control unit 310 displays a list of available payment methods on the display (step Sc8), one of which is to be selected by the user. Fig.17 shows an example of a screen on which the list is displayed. As shown therein, check-boxes each corresponding to each payment method are displayed. A user selects a check-box and "OK" button, to determine a payment method the user would like.

[0089] After the determination, Control unit 310 transmits to Payment gateway 15 via Mobile communication network 12 information for identifying the determined payment method (step Sc9). Upon receipt of the information of payment method, Payment gateway 15 sends a request for credit to Credit server 13. Subsequently, Payment gateway 15 sends a completion message to Portable device 14. Upon receipt of the message, Control unit 310 displays a massage such as "Payment has now been completed." on the display.

B-3. Operations of POS terminal 11

[0090] It will now be described that operations carried out in POS terminal 11 referring to fig. 18. When a user conducts a financial transaction namely, buys goods at a shop, a clerk inputs transaction information including name of goods, quantity, price, and tax into POS terminal (step Sd1) to store the information into storage areas. Control unit 710 determines whether a user wants to use this electronic payment service (step Sd2).

[0091] If the user does not want to use this service, or the user pays in cash (step Sd2 "NO"), Control unit 710 performs processing similarly to a general POS terminal (step Sd3). If the user wants to use the service, in other words, the user inputs a request of this service to POS terminal, Control unit 710 accesses Mobile terminal 17 via Interface 740, to determine whether a user ID is received (step Sd4).

[0092] If Mobile terminal 17 has not yet received a user ID sent from Portable device 14 using a short-range radio communication, Control unit 710 repeat accessing periodically until Mobile terminal 17 receives a user ID. When Mobile terminal 17 has received a user ID, Control unit 710 obtains the user ID via Interface 740. Next, Control unit sends to Payment gateway 15 via Communication network 10 a request for transaction number including the transaction information, the merchant information, and the user ID (step Sd5).

[0093] Transaction number is transmitted from Payment gateway 15 to POS terminal 11, in response to the request (step S4 in fig.11). Upon receipt of the transaction number from Payment gateway 15, Control unit 710 stores the received transition number in relation with the transaction information stored in POS terminal earlier (step Sd6).

[0094] After that, Control unit 710 waits for a completion message sent from Payment gateway 15. When receiving a completion message after data exchange between Portable device 14 and Payment gateway 15, Control unit 710 stores the completion message in relation with the transaction information and transaction number (step Sd7) and finally prints out a receipt for the transaction.

B-4. Operations of Payment gateway 15

[0095] It will now be described that operations performed in Payment gateway15 referring to fig. 19. Upon receipt of a request for transaction number from POS terminal 11(step Se1), CPU 151 of Payment server 150 issues a transaction number and sends it to POS terminal 11 via Communication network 10 (step Se2). CPU 151 stores the transaction information, the merchant information, the transaction number, and the date and time included in the request for transaction number into Transaction table 154b (step Se3).

[0096] Next, CPU 151 sends the user ID included in the request for transaction number to Direction server 160 (step Se4). Upon receipt of the user ID sent from Payment server 150, CPU 161 of Direction server 160 generates and stores into a mailbox 164a of the user an e-mail including commands for execution of an application for proceeding payment processing stored and executed in Portable device 14 (step Se5). Next, CPU 161 sends a reception message to Portable device 14 identified by the user ID. When Portable device 14 sends, in response to the message, a request for the e-mail to Direction server 160, CPU 161 sends the e-mail to Portable device 14 (step Se7).

[0097] Upon receipt of the e-mail, Portable device 14 executes the application to make a request for connection with Payment server. CPU151 establishes a connection by using SSL (step Se8). After establishment of the connection, Portable device 14 sends the User ID authentication result (authenticity of the user), and the device ID to Payment server 150. Payment server 150 checks the authentication result and next authenticates Portable device 14 on the basis of the device ID (step Se9). Specifically, CPU 151 compares the device ID sent from Portable device 14 with a device ID stored in

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 881 of 1360

relation with the user ID in User table 154a. If the two device IDs coincide, CPU 151 determines authenticity of the device 14 (step Se10).

[0098] If authenticity of the device 14 is not confirmed, namely, the two device IDs do not coincide, CPU 151 sends an error message to Portable device 14 and carries out error processing, for example, stops processing (step Se11). If the authenticity is confirmed, CPU 151 reads out information including transaction details and merchant information stored in Transaction table 154b in step Sc3, to send to Portable device 14 via Mobile communication network 12 (step Sc12).

[0099] Upon receipt of the above information, Portable device 14 urges the user to confirm the transaction details (step Sc4 and Sc5 in fig.15). If the user agrees with the transaction, a confirmation is transmitted to Payment gateway 15. If the user does not agree, nothing is transmitted. CPU 151 determines whether the confirmation is received within a predetermined time from transmission of the information to Portable device 14 (step Se13). If the confirmation is not received within the time, CPU 151 carries out error processing, for example, stops processing (step Se11).

[0100] If the confirmation is received within the time, CPU 151 determines payment methods available for the transaction and sends information on the payment methods to Portable device 14 via Communication network 12 so that the user can select one among the methods (step Se14). Specifically, CPU 151 refers to User table 154a of fig.7 to specify a credit card number corresponding to the user ID sent from Portable device 14. When the card number is specified, CPU151 refers to Issuer table 154c shown in fig.9 to specify an issuer of the card.

[0101] More specifically, CPU 151 determines within which range the card number lies in 154ca to specify the company. After the company is specified, CPU 151 refers to Merchant table 154d (cf. fig.10), to determine payment methods on the basis of the company and the merchant information included in the request for transaction number sent from POS terminal 11. Suppose that Merchant table 154c shown in fig.10 is stored in HDD 154, that a company "A" whose code number is "2a11111", and that a merchant "A" whose code number is "1111111111", CPU would determine that the user can pay in lump sum, installments, and revolving system and cannot pay with bonus and partially with bonus.

[0102] After transmission of the payment methods to Portable device 14, Portable device 14 sends a payment method to Payment gateway 15. Upon receipt of the payment method, CPU 151 make a request for credit with data in a predetermined format containing the credit card number, the expiration date, the transaction details (name of goods, quantity, price), the merchant information, the payment method and other related information, to transmit to Credit server 13 via Payment network 16 (step Se15). It is possible that the predetermined format is conventional one used for data exchange between a conventional credit server and a payment device. Finally, CPU 151 terminates processing of the transaction.

[0103] After transmission of the request for credit, CPU 151 waits until a completion message notifying completion of credit sent from Credit server 13 is received. Upon receipt of the completion message, CPU 151 forwards the completion message to POS terminal via Communication network 10 and to Portable device 14 via Mobile communication network 12 (step Se16).

[0104] As described above, by using the electronic financial transaction service in which a method for electronic payment based on this embodiment is applied, a purchaser don't have to hand his/her credit card in payment to a third-party including a clerk. Furthermore, a purchaser doesn't have to carry a credit card for shopping. Therefore, the danger of card information leakage and possible abuse of cards decreases drastically.

[0105] Also, Portable device 14 authenticates a user at payment, if a third party or other improper person obtains Portable device 14 improperly, the person cannot pay on credit using Portable cevice 14, thereby preventing the danger of abuse of Portable device 14.

[0106] Since information necessary for payment including a card number and an expiration date is stored in Payment gateway 15, not in Portable device14 or UIM 18, if Portable device 14 or UIM is stolen or improperly obtained, there is little danger of card information leakage from Portable device 14 or UIM. Further, sensitive information such as a card number and expiration date is managed by Payment gateway 15 and cannot provided to public networks such as Mobile communication network 12 and Communication network 10. Therefore, the danger of wiretapping such sensitive information via a public network is reduced.

[0107] In this embodiment, sensitive information necessary for payment is stored in both Portable device 14 and detachable UIM 18. Thus, a user is able to detach UIM from Portable device 14 when it is not required, to prevent the danger of information leakage. Even if such information is leaked, an improper user cannot pay using the device 14 since Payment gateway 15 authenticates Portable device 14 as well a user. In other words, both a user and a portable device are checked.

[0108] In this embodiment, Portable device 14 sends a request for payment to Payment gateway 15 via POS terminal 11; and upon receipt of the request, Payment gateway 15 sends an e-mail to Portable device 14 to obtain a confirmation of transaction from the user. Thus, even if an improper person obtains a user ID and intends to pay using another portable device in combination with the obtained user ID, needless to say, it is the only authorized Portable device 14 that receives the e-mail. Therefore, the improper person does not receive the e-mail and thus is not able to conduct a transaction using the obtained user ID. Namely, the danger of leakage and abuse of a user ID is restricted.

[0109] In the prior art, Payment gateway 15 may sends to Portable device 14 an e-mail including a mes-

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 882 of 1360

sage like "Please connect with the Payment server for payment", to obtain an instruction of payment from the user. Namely, a user operates Portable device 14 one after another referring to messages. However in this way, it is often the case that a user forgets operation procedures, or carries out wrong operations. This will cause a problem that a transaction stops or remains uncompleted. On the other hand, in this embodiment Portable device14 "automatically" executes an application for payment according to commands included in the received e-mail, thereby preventing suspension or stop of payment due to a misoperation made by a user.

[0110] Further, a user is able to register a plurality of credit cards used for the electronic financial transaction service. Specifically, each password is stored in UIM correspondingly to each credit card. As a result, a user is able to select credit cards for use in its appropriate way by inputting each user ID, for example.

[0111] It is noted that a method for payment based on the present embodiment has advantages in a merchant as well as a user described. That is, although a request for transaction number sent from POS terminal 11 to Payment gateway 15 does not contain a card number and expiration date which are send from a POS terminal 1 to a credit server 4 as shown in fig.21 in a conventional system Payment gateway 15 does contain transaction details and a merchant information used in a conventional system. Therefore, a merchant can participate in this transaction service simply by making, at POS terminal 11, a data including information necessary for a transaction in a conventional format and sending it to Payment gateway 15. This provides benefits to a merchant because the merchant does not have to install a new POS terminal.

[0112] Further, Credit server 13 performs processing in the conventional way because Payment gateway sends a request for credit in a conventional format to Credit sever 13. This provides convenience to a credit company because the company does not have to install a new server.

[0113] Since Transaction table 154b stores transaction details conducted by a user, it is possible that Payment gateway collectively manages electronic records or payments (so called electronic receipt). In a conventional credit payment system, generally a merchant issues a payment voucher on which transaction details are entered and mails it to a depository for managing payment vouchers provided by an issuer. However in this embodiment, Payment gateway 15 is able to manage payment information collectively, thus the cost of issuing and managing payment vouchers can be reduced.

C. Modification of the first embodiment:

[0114] The present invention is susceptible to many modifications as follows.

[0115] In the above embodiment, Storage area 233 of UIM 18 stores a device ID for identifying Portable device 14 used for the electronic financial transaction service. Portable device14 transmits the device ID to Payment gateway 15 and Payment gateway 15 compares the transmitted device ID and a device ID stored in User table 154a for authentication of the device 14. However it is possible that the authentication is carried out using SSL, for example. In this case, Portable device 14 sends to Payment gateway 15 a digital certificate for client authentication which has been registered at Certificate Authority (CA). Payment gateway 15 authenticates a device using the certificate.

[0116] In the above embodiment, Portable device 14 urges a user to input a user ID and a password for a user authentication. However it is possible to use biometrics such as fingerprint, iris scan, or combined voice and face patterns for the authentication.

[0117] In the above embodiment, a user ID is transmitted to POS terminal 11 via Mobile terminal 17 when the user conducts a financial transaction at a shop. However, the present invention is not only applied to such an actual shop but can be applied to an online shopping via Internet, for example. An example of such applications is shown in fig.20 in which a Web server 130 is provided instead of POS terminal 11 and Mobile terminal 17.

[0118] Web server 130, so called an online shop server, receives a request for purchase from terminals including a personal computer and a mobile phone with features of Web browsing. To be more specific, when user selects or inputs a URL for connection with the Web server 130, a web page for selection of goods is displayed on the terminal. The user makes a request for purchase seeing the page and sends it to Web server 130. A method of the present invention can be applied to procedures used for such a system for payment.

[0119] Specifically, firstly Portable device14 authenticates a user. If authenticity is confirmed, a user ID is transmitted from Portable device 14 to Web server 130 via Mobile communication network 12 and a Communication network 10A. Upon receipt of the user ID Web server 130, instead of POS terminal 11, sends a request for transaction number including transaction information, the user ID, and merchant information. Next, payment processing is performed among Portable device 14, Payment gateway 15, and Credit server 13 similarly to the first embodiment. After completion of the payment processing, a completion message is sent from Payment gateway 15 to Web server 130 via Communication network 10A.

[0120] In the first embodiment transaction information conducted by a user is stored in Transaction table 154b. Thus, it is possible that a user checks transaction information of the user with Portable device 14, personal computer, or a mobile phone with features including Web browsing. Specifically, when receiving a request for the check from a terminal via Internet, Payment gateway 15 retrieves the transaction information form table

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 883 of 1360

154b and transforms it into a HTML format for transmission to the terminal.

[0121] In the first embodiment, information necessary for payment is stored in EEPROM 230 of detachable UIM 18 to be read out by Control unit 310. However, it is possible that a memory such as an EEPROM incorporated into Portable device 14 stores such information instead of UIM 18.

[0122] Further, a module such as an IC chip having high resistance to tampering in which information for payment including a user ID and a password is stored and read out by Control unit can be used instead of UIM 18. Needless to say, such a module can be mounted detachably.

[0123] In the first embodiment, a purchaser uses Portable device capable of communicating with Payment gateway by radio via Mobile communication network 12 for electronic payment. However, a personal computer can be used as a terminal for payment in the system, for example. Specifically, such a computer is connected with Internet via a fix telephone network and has an input device, display and other devices necessary for the electronic payment.

[0124] In the first embodiment, a user ID is transmitted via Mobile terminal 17 to POS terminal 11. However, if POS terminal 11 features Bluetooth for data exchange, Portable device 14 may transmit directly to POS terminal 11. It is possible that a user ID can be transmitted from Portable device 14 to POS terminal 11 using other communication methods.

[0125] In the first embodiment, data exchange is carried out between POS terminal 11 and Payment gateway 15 via Communication network 10. It is possible that Mobile terminal 17 is connected with Communication network 10 to exchange data between POS terminal 11 and Payment gateway via Mobile terminal 17 and Communication network 10.

[0126] In the first embodiment it is possible that if a user uses two or more credit cards for the electronic transaction system a user ID or a password is assigned to the cards. In this case, before selection of credit card (step Sa1 of fig 12), a user may input the user ID and a password before Portable device 14 authenticates the user. After the authentication, credit cards corresponding to the user ID and the password are displayed. Then the user selects one among the cards.

[0127] In the first embodiment, Control unit 310 executes application programs in data exchange between POS terminal and Payment gateway 11 and authentication of a user and a device 14. It is possible that a storage medium such as a CD-ROM or a floppy disk in which such programs for the electronic payment is stored is provided to users. The programs may be provided via Internet.

(Second embodiment)

[0128] A second embodiment of the present invention will now be described referring to the drawings.

D. Configuration of the system

D-1. Overall configuration

[0129] Fig.22 shows an electronic payment system using a method for electronic paying based on the second embodiment of the present invention.

[0130] As shown, Electronic payment system 15A has a POS terminal 11A and Credit server 13A. Payment gateway 15A is connected with Terminal 11A and Credit server 13A via a dedicated line (not shown) for data exchange. Terminal 11A and Payment gateway may be connected via a public network. Payment gateway 15A is also connected to Portable device 14A.

D-2. POS terminal

[0131] POS terminal 11A has a storage unit such as a hard drive and an input device such as a keyboard, a mouse or a card reader. In addition to Display, Control unit including a CPU, ROM, RAM, and a communication interface same as POS terminal 11 of the first embodiment. Fig.23 shows an example of information stored in the storage. As shown, "issuer code" "payment method", and "merchant code" are stored correspondingly. The "issuer code" identifies an issuer (credit card company) of a credit card by which a user can pay at a shop where POS terminal 11A is installed. The "payment method" is a payment method available for a purchaser at the shop such as a lump sum, installments, or with bonus. The "merchant code" identifies a shop of a merchant.

D-3. Credit server

[0132] Credit server 13A includes a CPU, a RAM, a ROM, an input device such as keyboard or mouse, a display, a storage unit such as a hard drive, and a communication interface such as a modem.

[0133] Figs.24A through 24D shows an example of information stored in the storage unit of Credit server 13A. Fig.24A shows information relating to POS terminal 11A. Specifically, "merchant code for credit", "payment method", and "merchant code" are stored correspondingly. The "merchant code for credit" allows an issuer (credit company) to identify a merchant or a shop with which a transaction is conducted. It may be an ID number of a shop or of POS terminal 11A.

[0134] Fig.24B shows information relating to users of credit cards. Specifically, "user name", "user address", "card number", "expiration", and "credit limit" are stored corresponding.

[0135] Fig.24C shows an example of histories of transactions conducted by users. "Card number", "decryption key", "type", "date", "transaction number", "merchant number", "amount", "payment method", and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 884 of 1360

"merchandise code" are stored correspondingly. Information stored in "card number" in fig.24C is same as stored in fig.24B. In fig.24C it is permitted that a card number is stored for several times because a user may conduct transactions several time with the card.

[0136] The "decryption key" is used for decrypting an encrypted card number which is sent from Payment gateway 15A to POS terminal 11A. The "type" represents types of transactions. The "date" represents date of payment. The "transaction number" is a serial number each assigned to a transaction. The "merchant number" identifies a shop of a merchant with which a transaction is conducted. The "amount" represents a price of merchandise (possibly including tax). The "payment method" represents payment in a lump sum, or installments, for example. The "merchandise code" identifies merchandise transacted.

[0137] Fig.24D shows an example of information on transaction details conducted at each shop. Specifically, "merchant number", "type", "date", "sales", "card number", and "payment method" are stored. Information stored in "merchant number", "type", and "date" is same as stored in fig. 24C. The "sales" represents a price of merchandise, which is same as "amount" in fig.24C if tax is not included in the "amount". The "payment method" represents a payment method selected by a user.

D-4. Portable device

[0138] Portable device14A is, for example, a cellular phone capable of carrying out data communications. To be more specific, it may use (Personal Digital Cellular (PDC) of Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), General Packet Radio Service (GPRS), or any other schemes for data communication. Further, Third generation (3G) scheme such as IMT-2000 may be applied. Needless to say, PDA and other portable devices can be applied.

D-5. Payment gateway

[0139] Payment gateway 15A includes a CPU, a RAM, a ROM, an input device such as a keyboard or a mouse, a display, a storage unit such as a hard drive, and a communication interface such as a modem. Functionally, Payment gateway 15A comprises a receiving unit 101, a checking unit 102, encryption unit 103, a number transmitting unit 104, a key generation unit 105, a key transmitting unit 106, a transmitting/receiving unit 107, a notifying unit 108, and a storage unit 109.

[0140] Transaction unit 101 receives a user ID to identify a user assigned to the user in advance and a merchant code to identify a shop, which is sent from POS terminal 11A where the user conducts a transaction. Upon receipt of a user ID and a merchant code, Receiving unit 101 transfers the user ID and the merchant code to Checking unit 102 and Transmitting/receiving unit 107.

[0141] Checking unit 102 retrieves a card number of a user from Storage unit 109 on the basis of a user ID received by Receiving unit 101. Specifically, Checking unit 102 retrieves a from Storage unit 109 a card number and an issuer code corresponding to a user ID received by Receiving unit 101. Checking unit 102 outputs the card number, the issuer code, and the merchant code to Encryption unit 103. If the user ID is not found or the expiration date has passed, Checking unit 102 outputs to Notifying unit 108 a message notifying failure of authentication.

[0142] Figs.25A and 25B show an example of information stored in Storage unit 109. As shown in Fig.25A information relating to shops which participate in the electronic payment service provided by Payment gateway 15A is stored. To be more specific, a merchant codes and corresponding shop name.

[0143] Fig.25B shows an example of information relating to users. Specifically, user IDs and corresponding passwords, user names, phone numbers, e-mail addresses, terminal numbers, card numbers, issuer codes, and expirations are stored correspondingly. The password is used for authentication of a user.

[0144] The phone number is a telephone number of portable device 14A. The e-mail address is an e-mail address for Portable device 14A. The device number is, for example, a serial number assigned for each Mobile station 14A which identifies Mobile station 14A. The card number is a number of a credit card by which a user pays. A user registers the card number to Payment gateway 15A in advance. The issuer code identifies an issuer of a card (credit company). The expiration represents an expiration date of the credit card.

[0145] Encryption unit 103 encrypts a card number obtained by Checking unit 102, to generate a "encrypted card number". Specifically, Checking unit 103 encrypts a card number, in a way that it can be decrypted using an encryption key generated by Key generating unit 105. Suppose that the decryption key is "0123" that the card number is "3456", and that the encryption calculation is an addition, the encrypted card number becomes "3579". In decryption, "0123" is subtracted from "3579" to be generated the card number "3456". Encryption unit 103 outputs to Key generating unit 105 a card number, its encrypted card number, and an issuer code. Further Encryption unit 103 outputs to Number transmitting unit 104 the encrypted card number and the merchant code.

[0146] Number transmitting unit 104 transmits an encrypted card number made by Encryption unit 103 to POS terminal 11A specified by the merchant code obtained from Encryption unit 103.

[0147] Key generating unit 105 generates a decryption key used for decryption of a card number. In this embodiment, a card number is encrypted by Encryption unit 103 using a decryption key. It is possible that the decryption key is generated using both the decryption key and the card number. Key generating unit 105 outputs to Key transmitting unit 106 the encrypted card number, the decryption key, and the issuer code.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 885 of 1360

[0148] Key transmitting unit 106 transmits to Credit server 13A an encrypted key generated by Key generating unit 105. Specifically, Key transmitting unit 106 transmits, to Credit server by a credit company specified by the issuer code provided form Key generating unit 105 the encrypted card number and the decryption key.

[0149] When Receiving unit 101 receives a user ID, Transmitting/receiving unit 107 transmits to portable device 14A a confirmation e-mail including transaction details. If Portable device 14A does not reply to the e-mail, Transmitting/receiving unit 107 stops at least one of Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, and Key transmitting unit 106 to cancel the transaction conducted on the basis of the user ID.

[0150] To be more specific, Transmitting/receiving unit 107 retrieves from Storage unit 109 an e-mail address on the basis of the user ID provided from Receiving unit 101. Transmitting/receiving unit 107 then transmits a confirmation e-mail including transaction details to Portable device 14A specified by the e-mail address. Upon receipt of a reply e-mail from Portable device 14A, Transmitting/receiving unit 107 checks a password included in the reply e-mail against a password stored in Storage unit 109, to authenticate the user.

[0151] If Transmitting/receiving unit 107 does not receive a reply e-mail or the both passwords does not agree, Transmitting/receiving unit 107 stops at least one of Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, and Key transmitting unit 106, to cancel the transaction conducted on the basis of the user ID. A method for obtaining a confirmation from a user is not limited to the e-mail. For example, Transmitting/receiving unit 107 can transmit to Portable device14A a recection message which is generally used for cellular phone. It is possible that, in the authentication of a user, Transmitting/receiving unit 107 uses in addition to a password, information to identify Portable device 14A uniquely such as a device ID.

[0152] If Checking unit 102 does not find the credit card corresponding to the user ID in Storage unit 109, Notifying unit 108 notifies POS terminal 11A of failure of authentication.

E. Operations of the system

[0153] Detailed procedures for payment processing in an electronic financial transaction system based on the second embodiment will now be described referring to figs. 26 and 27.

[0154] As shown in fig.26, firstly, POS terminal 11A obtains a user ID from a user and transmits the user ID and a merchant code to Payment gateway 15A (step S01). Specifically, a user inputs a user ID with the input device of POS terminal, for example. POS terminal 11A may obtain the user ID from Portable device 14A. Receiving unit 101 receives the user ID and the merchant code (step S02). Next, Receiving unit 101forwards the user ID and the merchant code to Checking unit 102 and Transmitting/receiving unit 107.

[0155] Upon receipt of the user ID, Transmitting/receiving unit 107 sends a confirmation e-mail to Portable device 14A corresponding to the user ID (step S03). After the sending, Transmitting/receiving unit 107 is ready for receiving reply e-mail (step S04). If Transmitting/receiving unit 107 does not receive a reply e-mail or the both passwords does not agree, Transmitting/receiving unit 107 stops at least one of Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, and Key transmitting unit 106 to cancel the transaction conducted on the basis of the user ID (step S05).

[0156] When Transmitting/receiving unit 107 receives the reply e-mail, Checking unit 102 retrieves from Storage unit 109 a card number stored correspondingly to the user ID provided from Receiving unit 101 (step S06). It is noted that steps S03 and S04 can be omitted.

[0157] Checking unit 102 checks the card number retrieved from Storage unit 109 against the card number provided from Receiving unit 101 (step S07). If the user ID is not found in Storage unit 109 or the expiration date has passed, Checking unit 102 notifies Notifying unit 108 of failure of authentication.

[0158] Upon receipt of the message from send from Checking unit 102, Notifying unit 108 sends a message notifying POS terminal of failure of authentication (step S08). POS terminal 11A receives the message to be notified the user (step S09).

[0159] If the credit card number corresponding to the user ID is retrieved form Storage unit 109 in step S07, Checking 102 outputs the card number, the issuer code, and the merchant code to Encryption unit 103. When Encryption unit 103 receives the card number, the issuer code, and the merchant code, Key generating unit 105 generates a decryption key used for decryption of an encrypted card number (step S10). Key generating unit 105 outputs the key to Encryption unit 103 to obtain the card number and the issuer code. Next, Key generating unit 105 sends to Key transmitting unit 106 the card number and the issuer code along with the key.

[0160] Upon receipt of the decryption key from Key generating unit 105, Encryption unit 103 encrypts the card number in a way that the encrypted card number is decrypted with the decryption key (step S11). Next, Encryption unit 103 outputs the encrypted card number and the merchant code to Number transmitting unit 104.

[0161] Referring to fig.27, Number transmitting unit 104 transmits the encrypted card number to POS terminal 11A indicated by the merchant code (step S12). Key transmitting unit 106 transmits the encrypted card number and the key to Credit server 13A indicated by the issuer code (step S13). The encryption key may be generated for each user, or for each credit company. In case a common key is used as the decryption key for this system, Key transmitting unit 106 does not necessarily transmit the key to Credit server 13A more than

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 886 of 1360

twice. But needless to say, when the key is updated, Key transmitting unit 106 transmits the updated key. Upon receipt of the encrypted card number and the decryption key, Credit server 13A stores the number and the key into a storage unit of Credit server 13A (step S14).

[0162] POS terminal 11A receives and stores into a storage unit of POS terminal 11A the encrypted card number (step S15). Next, POS terminal 11A makes a request for credit to transmit to Credit server 13A (step S16). Specifically, the request includes, a type, date, transaction number, merchant code for credit, amount, payment method, merchant code as described above, in addition to the encrypted card number.

[0163] Upon receipt of the request (step S17), Credit server 13A determines whether the request is accepted referring to the encrypted card number (step S18). Specifically Credit server 13A checks the encrypted card number and the decryption key which has already been transmitted by Payment gateway 15A against the decryption key transmitted by POS terminal 11A. If both keys coincide, Credit server 13A decrypts the encrypted card number using corresponding decryption key which has already been received from Payment gateway 15A. If the encrypted card number is not found Credit server 13A sends a message notifying a failure of authentication to POS terminal 11A to be provided to the user (step S19). POS terminal 11A receives the message (step S20). If the encrypted card number is found, Credit server 13A sends an allowance message (step S21). POS terminal 11A receives the message to be provided to the user.

[0164] A payment program 92 for making a computer to function as Payment gateway 15A and a storage medium 9 will now be described referring to fig.28. Fig.28 shows a functional structure of the storage medium. Storage media 9 is, for example, a magnetic disk, an optical disk including a CR-ROM, or a semiconductor memory.

[0165] As shown in fig.9, Storage medium 9 has a program area 91 and a data area 93. Data area stores a database 931 same as Storage unit 109 shown in fig.22.

[0166] Program area 91 stores Payment program 92. Payment program 92 includes a main module 921 for controlling the following modules, a module 922 for receiving transaction information, a module 923 for checking a card number, a module 924 for encrypting a card number, a module 925 for transmitting an encrypted card number, a module 926 for generating a decryption key, a module 927 for transmitting a decryption key, a module 928 for transmitting a confirmation message and receiving a reply message, and a module 929 for notifying a message of failure of authentication. These modules 922 through 929 have same functions as the Receiving unit 101, Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, Key transmitting unit 106, Transmitting/receiving unit 107, Notifying unit 108, respectively.

[0167] In the second embodiment, since the encrypted card number is transmitted from Payment gateway to POS terminal 11A and the encrypted card number is generated by Payment gateway 15A on the basis of a user ID transmitted from POS terminal, a merchant cannot obtain a card number. Therefore, security of transaction is ensured in this system. In other words, a user is able to send a card number safely to Payment gateway 15A to conduct a transaction. Payment gateway transmits a decryption key to Credit server 13A, thus Credit server 13A obtains a decryption key corresponding to the encrypted card number. Therefore, Credit server 13A is able to determine whether a request for credit should be accepted using an encrypted card number and corresponding decryption key. Furthermore, an encrypted card number is generated each time a transaction is conducted, thus a merchant can manage sales at the shop, not knowing a card number.

[0168] In this embodiment, when Payment gateway 15A does not receive a reply mail from Portable device 14A, payment processing related to the user ID is stopped. Therefore, if an authorized person obtains a user ID improperly, the person cannot conduct any transactions using the user ID.

[0169] If Payment gateway 102 cannot find a card number corresponding to a user ID, Payment gateway 102 transmits a message notifying failure of authentication to POS terminal 11A, thus a merchant and a user can recognize that the card is not available for the transaction.

Claims

1. An electronic payment method comprising the steps of:

   authenticating a user of a user terminal on the basis of user identification information inputted to said user terminal by said user, by said user terminal;

   storing an authentication result of said user, by said user terminal, when said user terminal confirms authenticity of said user;

   transmitting a user identification information stored beforehand in said user terminal to a merchant terminal when said user terminal confirms authenticity of said user, by said user terminal;

   transmitting to payment device via a first communication network said user identification information and transaction information transmitted from said user terminal, by said merchant terminal;

   receiving said user identification information and said transaction information transmitted from said merchant terminal, by said payment device;

   identifying said user terminal on the basis of

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 887 of 1360

said user identification information and transmitting commands for instructing transmission of said authentication result to said user terminal via a second communication network;
transmitting authenticity of said user to said payment device via said second communication network if said user terminal stores authenticity of said user, by said user terminal; and
performing payment processing on the basis of said transaction information upon receipt of said authenticity from said user terminal, by said payment device.

2. The method of claim 1, further comprising the steps of:

transmitting said transaction information to said user terminal via said second communication network upon receipt of said authenticity of said user from said user terminal, by said payment device;
receiving said transaction information transmitted from said payment device and notifying said user of said transaction information, to be checked by said user, by said user terminal; and
when said user inputs an instruction for proceeding payment processing to said user terminal, transmitting to said payment device a request for proceeding payment processing; and
wherein upon receipt of said request, said payment device performs payment processing on the basis of said transaction information.

3. The method of claim 1, wherein said user terminal transmits to said payment device terminal identification information for identifying said user terminal along with said authentication result;
said payment device authenticates said user terminal referring to said terminal identification information; and
when authenticity of said user terminal is confirmed, said payment device performs payment processing on the basis of said transaction information.

4. The method of claim 1, wherein said second communication network is a mobile communication network and said user terminal is a mobile station.

5. The method of claim 1, wherein upon receipt of said authenticity from said user terminal, said payment device retrieves a card number and an expiration date on the basis of said user identification information and sends a request for credit including the card number and the expiration date to a credit server provided by a credit company.

6. An electronic payment method comprising the steps of:

authenticating a user of a user terminal on the basis of user identification information inputted to said user terminal by said user, by said user terminal;
transmitting user identification information for identifying a user to a merchant terminal, by said user terminal, when said user terminal confirms authenticity of said user;
transmitting to a payment device via a first communication network said user identification information transmitted from said user terminal, by said merchant terminal;
receiving said user identification information from said merchant terminal, by said payment device;
identifying said user terminal referring to received user identification information and transmitting commands for executing an application for payment stored in said user terminal to identified user terminal via a second communication network, by said payment device;
upon receipt of said commands, executing said application to transmit a request for proceeding payment processing to said payment device via said second communication network, by said user; and
upon receipt of said request from said user terminal, performing a payment processing.

7. An electronic payment system having a payment device, a merchant terminal connected with said payment device via a first communication network, and a user terminal connected with said payment device via a second communication network **characterized in that**:

said user terminal authenticates a user of said user terminal on the basis of user identification information inputted to said user terminal by said user; if authenticity of said user is confirmed, stores authentication result; and transmits to said merchant terminal user identification information stored in said user terminal;
said merchant terminal transmits to said payment device via said first communication network said user identification information transmitted from said user terminal and transaction information
said payment device identifies said user terminal on the basis of said user identification information transmitted from said merchant terminal and
transmits to said identified user terminal via said second communication network commands for instructing transmission of said au-

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 888 of 1360

thentication result;
said user terminal transmits to said payment device via said second communication network according to said commands transmitted from said payment device when said user terminal stores said authentication result; and
upon receipt of said authentication result from said user terminal, said payment device performs payment processing on the basis of said transaction information.

8. The system of claim 7, wherein after reception of said authentication result from said user terminal, said payment device transmits said transaction information to said user terminal via said second communication network;
said user terminal receives said transaction information form said payment device;
notifies said user of said transaction information to be checked by said user; and
if said user inputs to said user terminal an instruction of proceeding a payment processing, transmits a request for proceeding payment processing to said payment device via said first communication network; and
upon receipt of said request, said payment device performs payment processing.

9. The system of claim 8, wherein said user terminal transmits to said payment device terminal identification information for identifying said user terminal stored in said user terminal along with said authentication result; and
said payment device authenticates said user terminal on the basis of said terminal identification information;
if authenticity of said user terminal is confirmed, performs payment processing on the basis of said transaction information.

10. The system of claim 7, wherein a detachable storage medium for storing said user identification information is mounted to said user terminal; and
when said user terminal confirms authenticity of said user on the basis of said user identification information, said user terminal transmits to said merchant terminal said user identification information stored in said storage medium.

11. The system of claim 7, wherein said second communication network is a mobile communication network and said user terminal is a mobile station.

12. The system of claim 7, wherein when receiving said authentication result from said user terminal, said payment device retrieves a card number and an expiration on the basis of said user identification information and sends a request for credit including said card number and said expiration to a credit server managed by a credit company.

13. An electronic payment system having a payment device, a merchant terminal connected with said payment device via a first communication network, and a user terminal connected with said payment device via a second communication network **characterized in that**:

said user terminal authenticates a user on the basis of said user identification information inputted to said user terminal by said user
if authenticity of said user is confirmed, transmits to said merchant terminal a user identification information for identifying said user;
said merchant terminal transfers said user identification information to said payment device via said first communication network;
said payment device identifies said user terminal on the basis of said user identification information and transmits to said identified user terminal via said second communication network commands for executing an application for payment stored in the user terminal;
said user terminal executes said application according to said commands and transmits a request for proceeding payment processing to said payment device via said second communication network; and
said payment device performs said payment processing according to said request.

14. A user terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network, comprising:

an authenticating means for authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user;
a storing means for storing an authentication result when authenticity of said user is confirmed by said authenticating means;
a storage medium for storing said user identification information;
a first transmitting means for transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information;
a receiving means for receiving commands for instructing transmission of said authentication result which is transmitted, in response to said

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 889 of 1360

request for payment, from said payment device via said second communication network; and
a second transmitting means for transmitting, upon receipt of said commands, a request for proceeding said payment processing including said authentication result to said payment device via said second communication network.

15. The user terminal of claim 14, wherein said storage medium further stores a terminal identification information for identifying said user terminal; and
said second transmitting means transmits, along with said authentication results, said terminal identification information stored in said storage medium to said payment device via said second communication network.

16. The user terminal of claims 14 or 15, wherein said storage medium is mounted detachably to said user terminal; and
said first transmitting means transmits to said merchant terminal said user identification information stored in said storage medium, when authenticity of said user is confirmed by said authenticating means on the basis of said user identification information.

17. The user terminal of claim 14 or 15, wherein said second communication network is a mobile communication network; and
said user terminal further comprises a radio communication means for exchanging data via said mobile communication network.

18. A user terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network, comprising:

an authenticating means for authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user;
a first transmitting means for transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information
a receiving means for receiving commands for executing an application for payment which is transmitted from said payment device via said second communication network; and
a second transmitting means for executing said application for payment stored in said user terminal and transmitting, according to said application, a request for proceeding payment processing to said payment device via said second communication network.

19. A payment device comprising

a receiver for receiving a request for payment including a user identification information for identifying a user of a user terminal from a merchant terminal via a first communication network;
an identifying means for identifying said user terminal among registered user terminal on the basis of said received user identification information; a transmitter for transmitting to said identified user terminal via a second communication network commands for executing an application for payment stored in the user terminal; and
a processing means for performing a payment processing on the basis of a request sent from the user terminal via said second communication network after transmission of said commands.

20. A computer program product for making a computer incorporated into a communication terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network to execute the steps of:

authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user; storing an authentication result into a storage means when authenticity of said user is confirmed by said authenticating means;
transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information;
receiving commands for instructing transmission of said authentication result which is transmitted, in response to said request for payment, from said payment device via said second communication network; and
transmitting, upon receipt of said commands a request for proceeding said payment processing including said authentication result to said payment device via said second communication network.

21. A storage medium for storing a computer program product for making a computer incorporated into a

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 890 of 1360

communication terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network to execute the steps of:

authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user; storing an authentication result into a storage means when authenticity of said user is confirmed by said authenticating means;
transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information;
receiving commands for instructing transmission of said authentication result which is transmitted, in response to said request for payment, from said payment device via said second communication network; and
transmitting, upon receipt of said commands, a request for proceeding said payment processing including said authentication result to said payment device via said second communication network.

22. A payment device comprising:

a storage unit for storing a user identification information for identifying a user of a user terminal and a card number of a credit card correspondingly; a receiving unit for receiving from a merchant terminal a user identification information;
a retrieving unit for retrieving from said storage unit a card number corresponding to said identified user;
an encrypting unit for encrypting the retrieved card number;
a generating unit for generating a key for decryption of said encrypted card number;
a first transmitting unit for transmitting to said merchant terminal said encrypted card number; and
a second transmitting unit for transmitting said key to a credit server managed by an issuer of the credit card.

23. The payment device of claim 22 further comprising a confirming means for transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information.

24. The payment device of claim 22 or 23, further comprising a notifying means for transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit.

25. An electronic payment method comprising the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal, by a receiving unit;
retrieving from a storage unit a card number corresponding to said identified user by a retrieving unit;
encrypting the retrieved card number, by an encrypting unit;
generating a key for decryption of said encrypted card number, by a generating unit;
transmitting to said merchant terminal said encrypted card number, by a first transmitting unit; and
transmitting said key to a credit server managed by an issuer of the credit card, by a second transmitting unit.

26. The electronic payment method of claim 25, further comprising the step of transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information, by a confirming means.

27. The electronic payment method of claim 25 or 26, further comprising the step of transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit, by a notifying means.

28. A computer program product for making a computer to execute the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 891 of 1360

retrieving from a storage unit a card number corresponding to said identified user;
encrypting the retrieved card number;
generating a key for decryption of said encrypted card number; transmitting to said merchant terminal said encrypted card number; and
transmitting said key to a credit server managed by an issuer of the credit card.

29. The computer program product of claim 28, for making said computer to further execute the step of transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information.

30. The computer program product of claim 28 or 29, for making said computer to further execute the step of transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit

31. A computer readable storage medium for storing a computer program product for making a computer to execute the steps of:

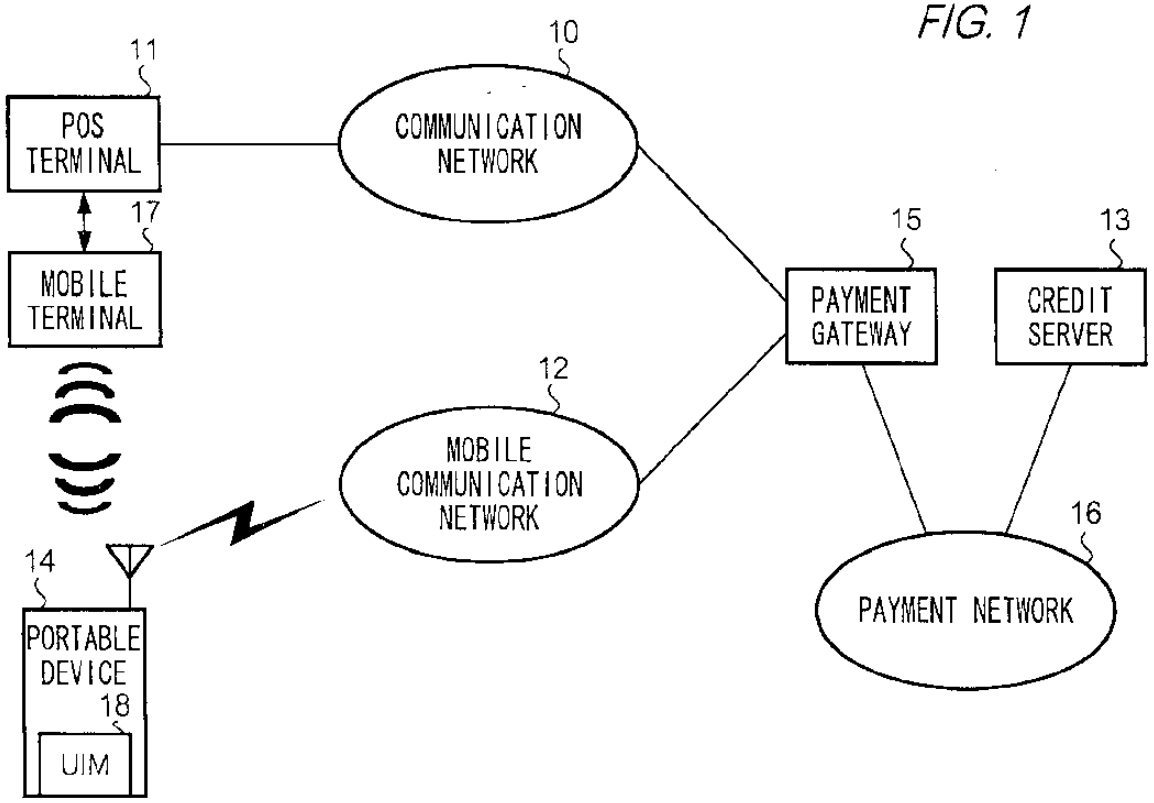
receiving from a merchant terminal a user identification information for identifying a user of a user terminal;
retrieving from a storage unit a card number corresponding to said identified user;
encrypting the retrieved card number;
generating a key for decryption of said encrypted card number; transmitting to said merchant terminal said encrypted card number; and
transmitting said key to a credit server managed by an issuer of the credit card.

32. The storage medium of claim 31, for storing a computer program product for making said computer to further execute the steps of transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information.

33. The storage medium of claim 31 or 32, for storing a computer program product for making said computer to further execute the step of transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit.

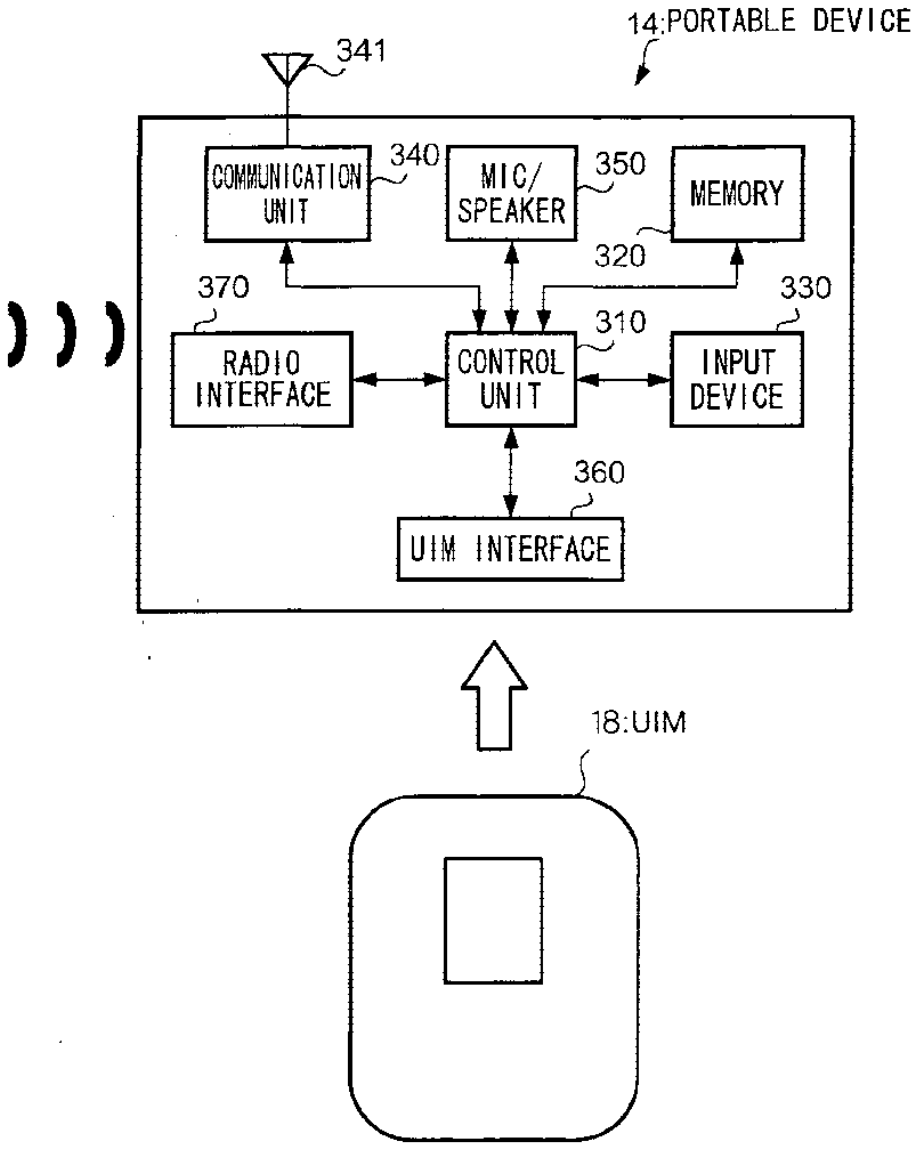
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 892 of 1360

FIG. 1



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 893 of 1360

FIG. 2



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 894 of 1360

FIG. 3

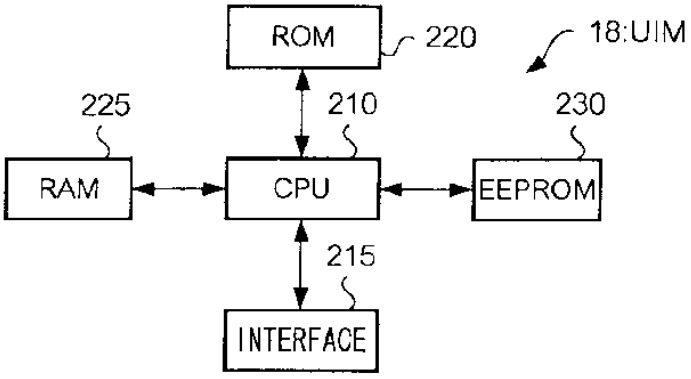
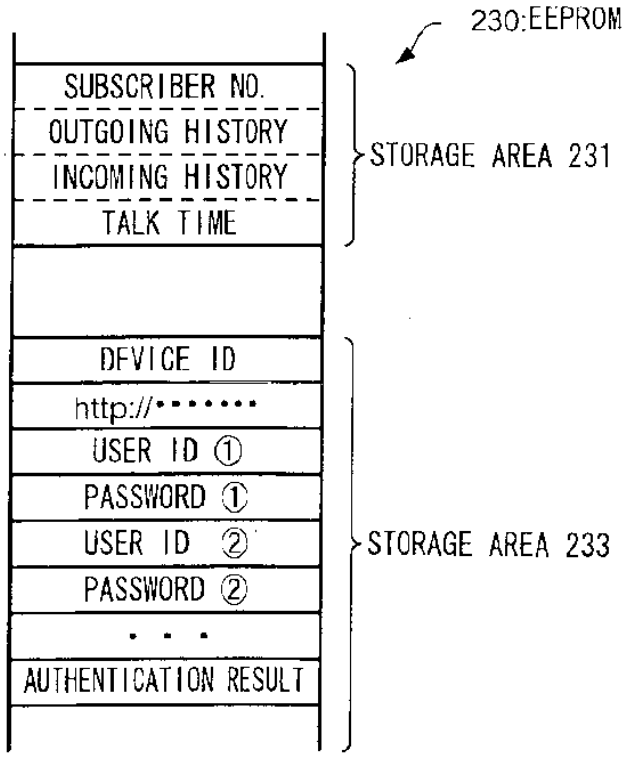
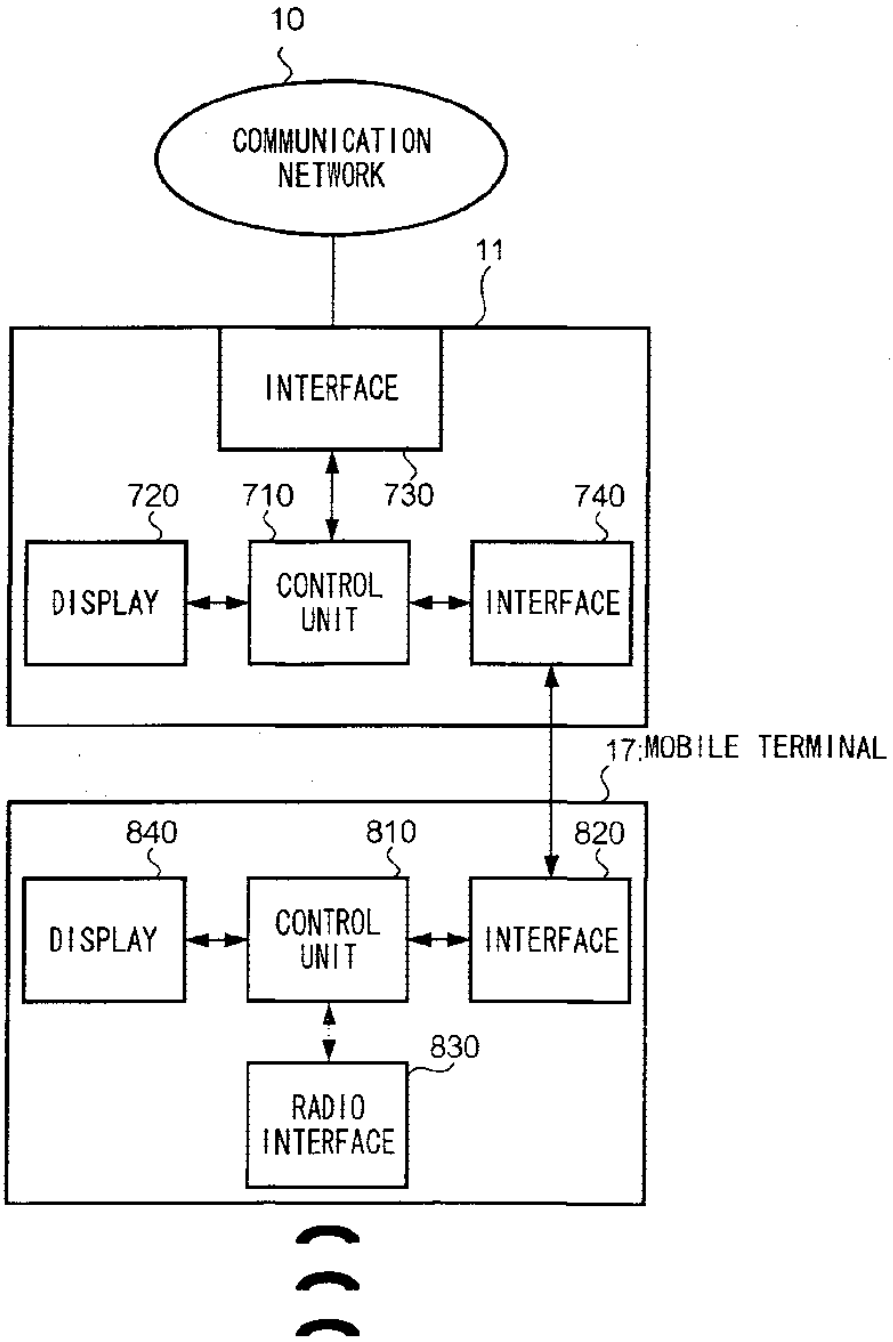


FIG. 4



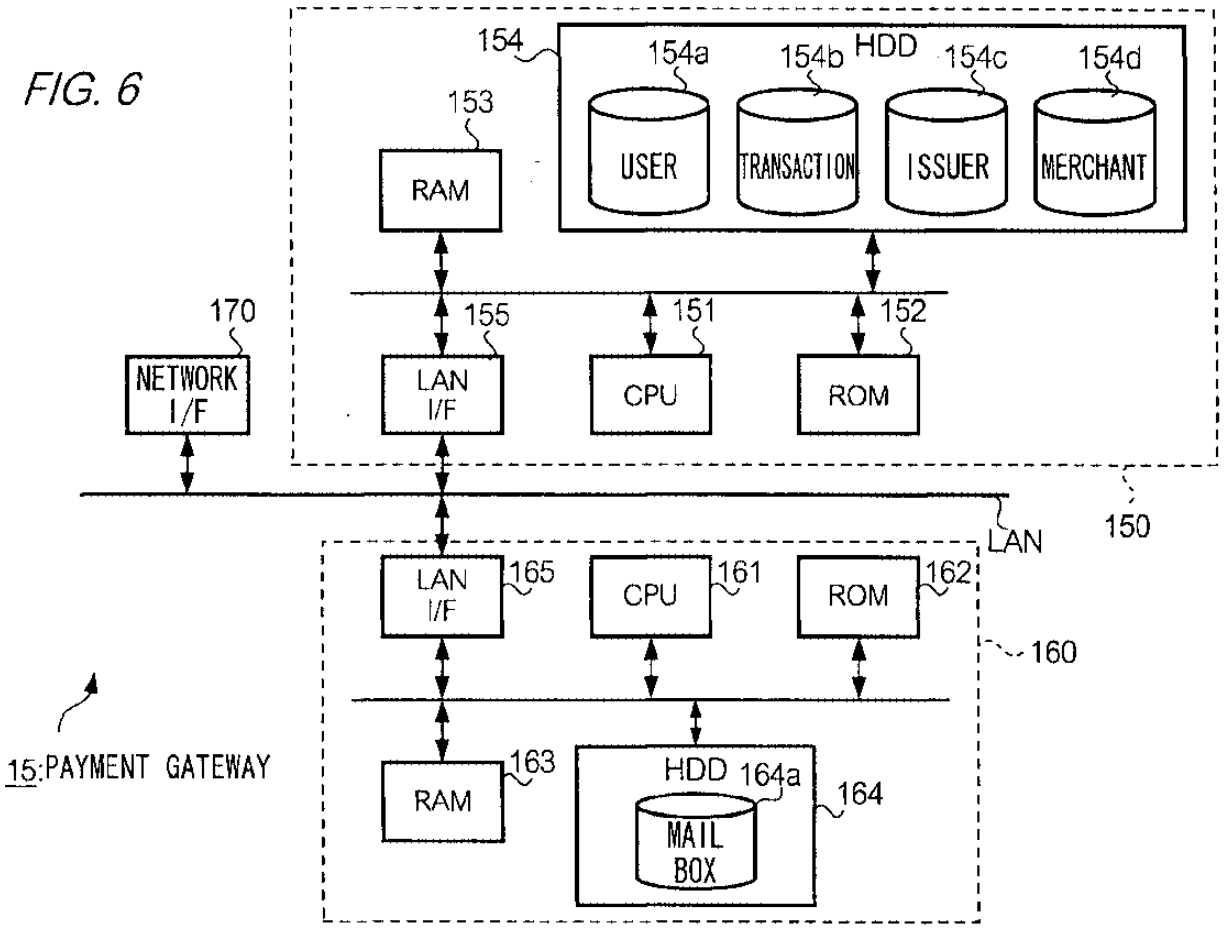
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 895 of 1360

FIG. 5



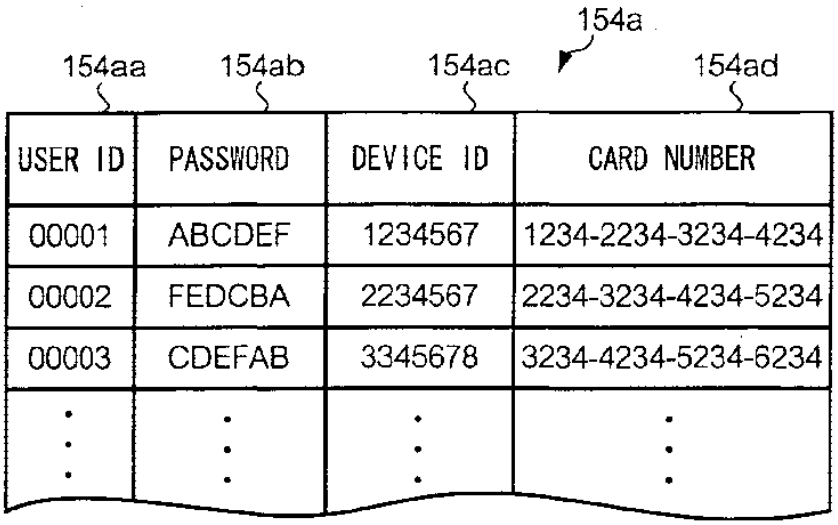
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 896 of 1360

FIG. 6



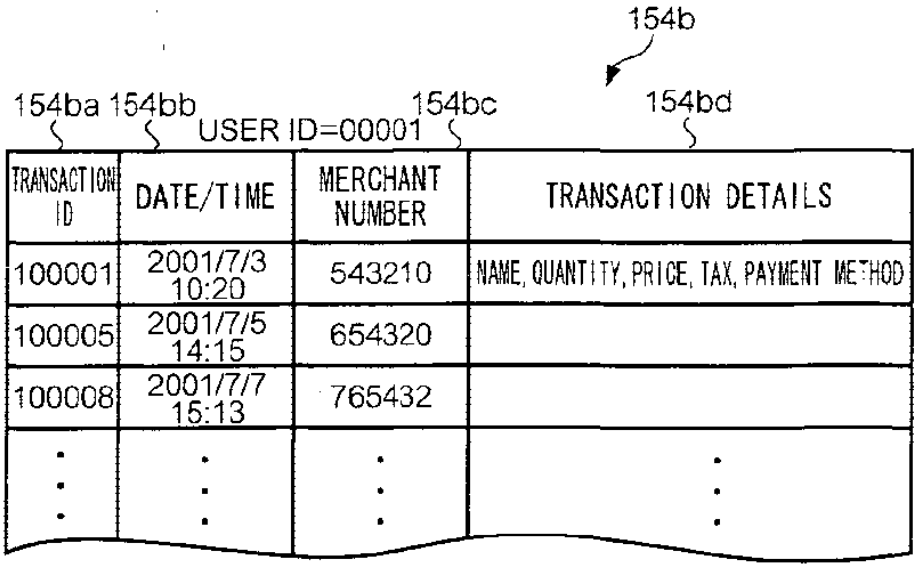
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 897 of 1360

FIG. 7



USER ID	PASSWORD	DEVICE ID	CARD NUMBER
00001	ABCDEF	1234567	1234-2234-3234-4234
00002	FEDCBA	2234567	2234-3234-4234-5234
00003	CDEFAB	3345678	3234-4234-5234-6234
⋮	⋮	⋮	⋮

FIG. 8



TRANSACTION ID	DATE/TIME	MERCHANT NUMBER	TRANSACTION DETAILS
100001	2001/7/3 10:20	543210	NAME, QUANTITY, PRICE, TAX, PAYMENT METHOD
100005	2001/7/5 14:15	654320	
100008	2001/7/7 15:13	765432	
⋮	⋮	⋮	⋮

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 898 of 1360

FIG. 9

154c

154ca 154cb 154cc

CARD NUMBER	ISSUER CODE	ISSUER NAME
1525000000~1525059999	2a11111	A
145259000~1452590000	2a22222	B
153996010~153996010	2s33333	C
13500~13560	2a11111	A
13600~13600	2s44444	D

FIG. 10

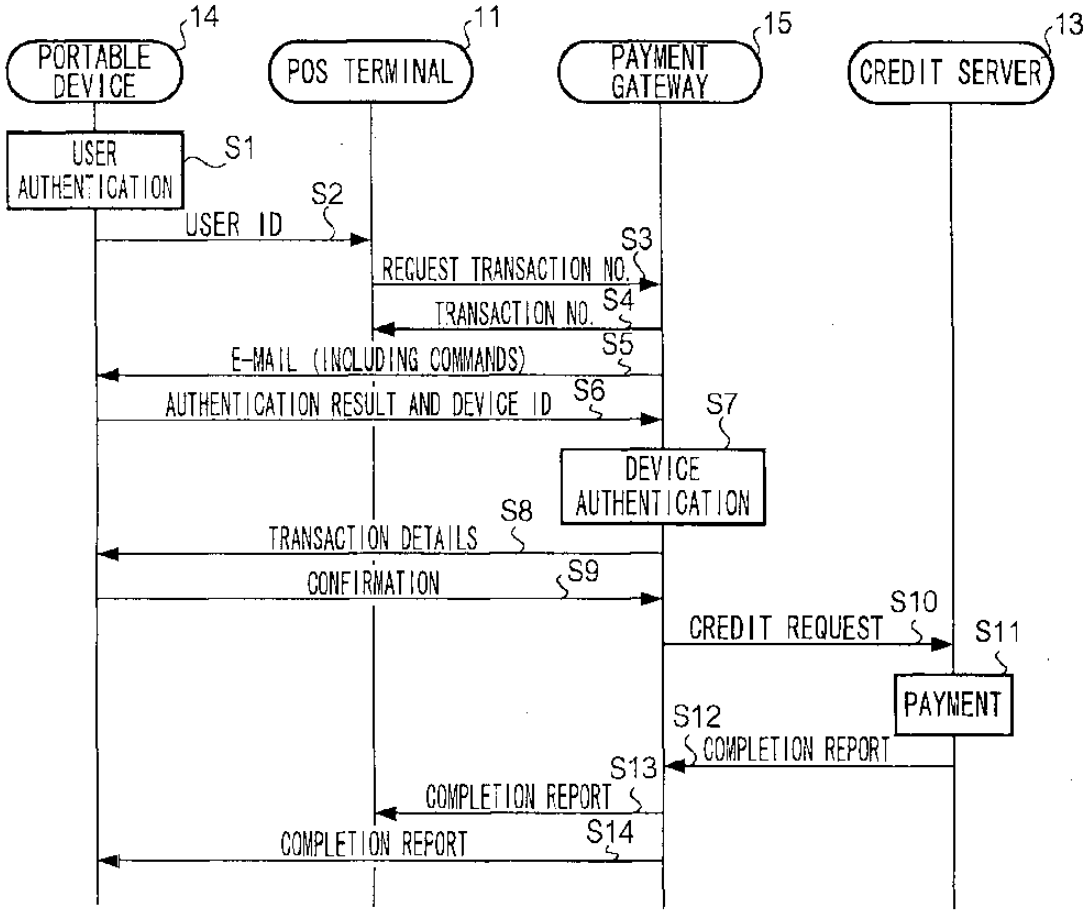
154d

154da 154db 154dc 154dd 154de

MERCHANT CODE	MERCHANT NAME	ISSUER NAME	ISSUER NAME	PAYMENT METHOD				
				L	I	B	PB	R
1111111111	A	2a11111	A	○	○	×	×	○
2222222222	B	2a22222	B	○	○	×	○	○
2222222222	B	2s44444	D	○	×	○	×	×
3333333333	C	2a22222	B	○	×	○	○	×
4444444444	D	2s33333	C	○	×	×	×	○

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 899 of 1360

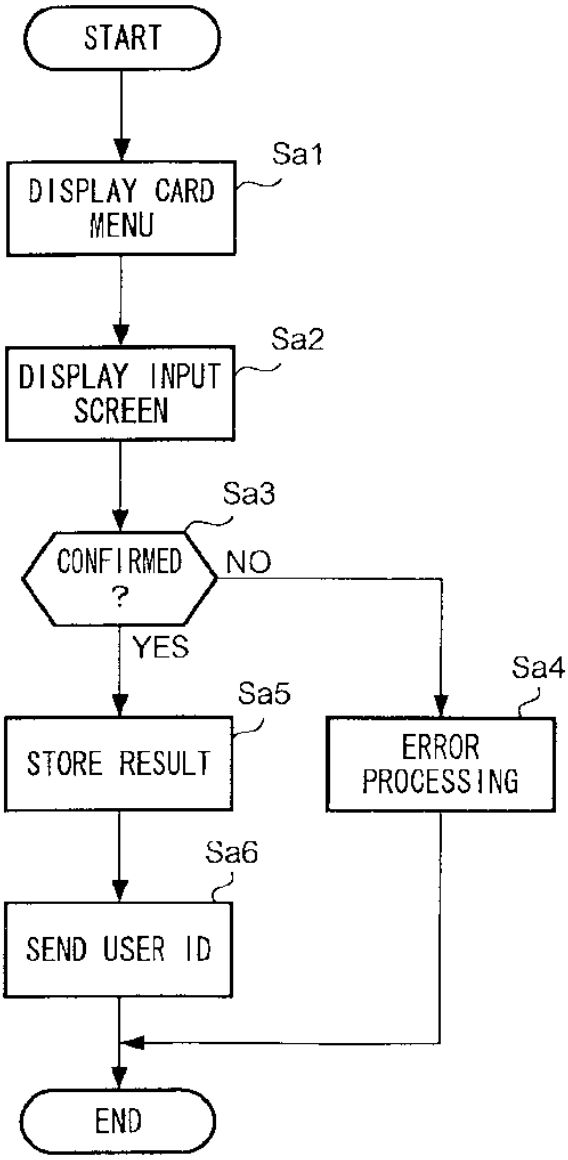
FIG. 11



EP 1 280 115 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 900 of 1360

FIG. 12



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 901 of 1360

FIG. 13

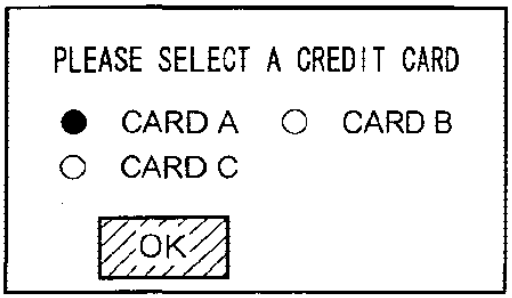
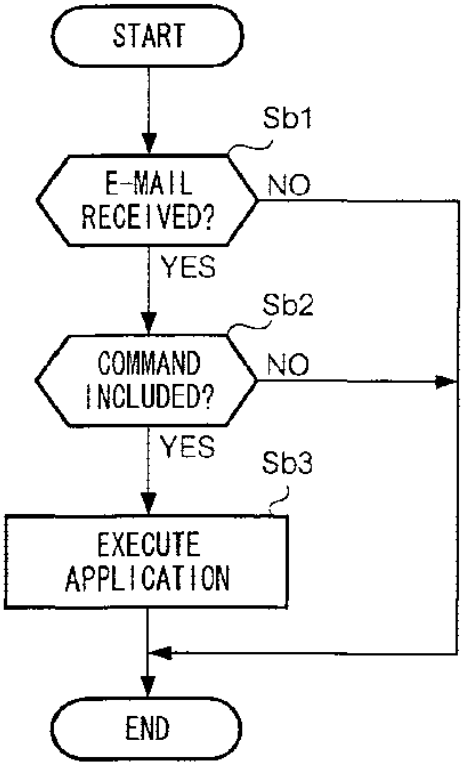
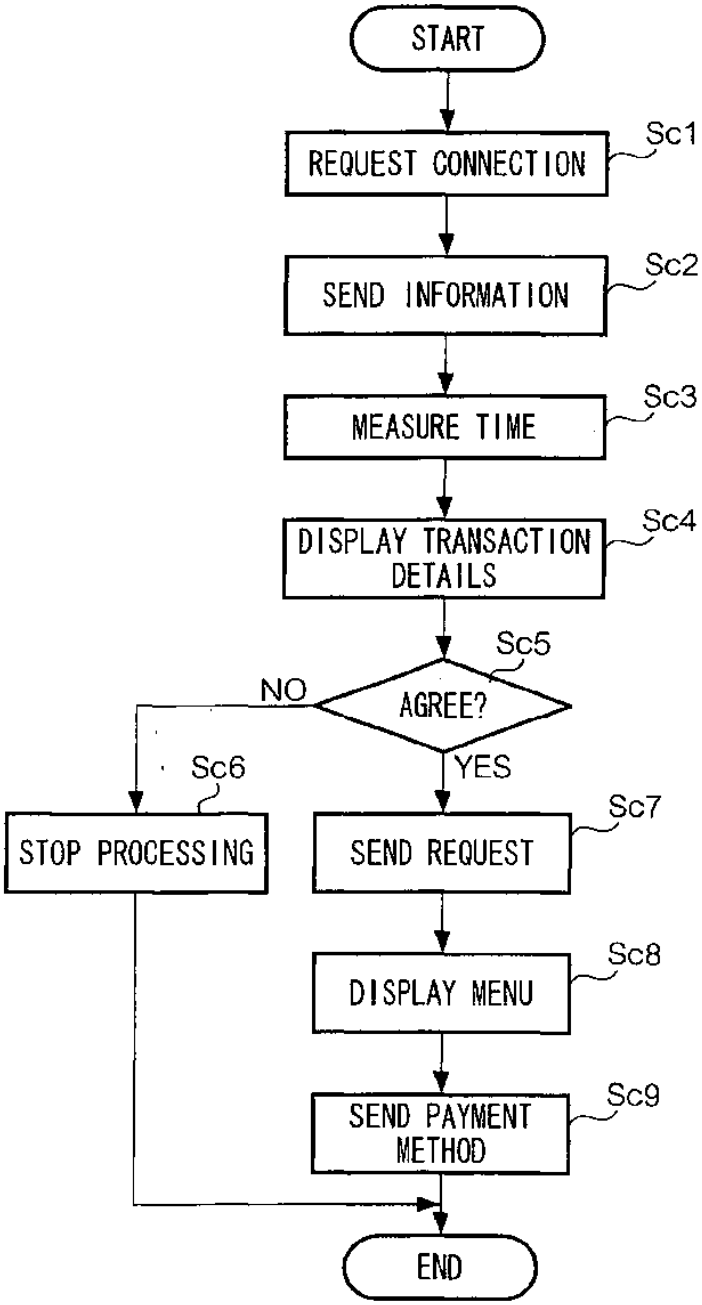


FIG. 14



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 902 of 1360

FIG. 15



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 903 of 1360

FIG. 16

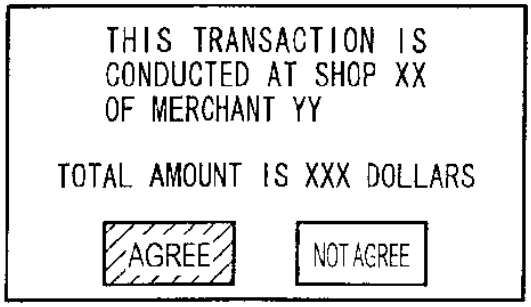
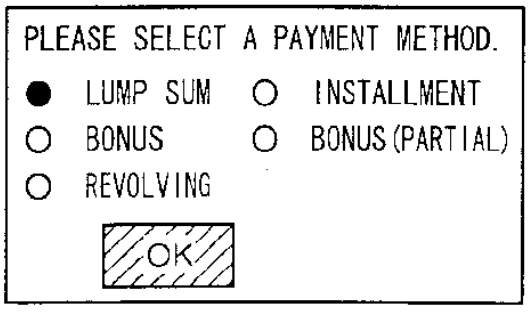
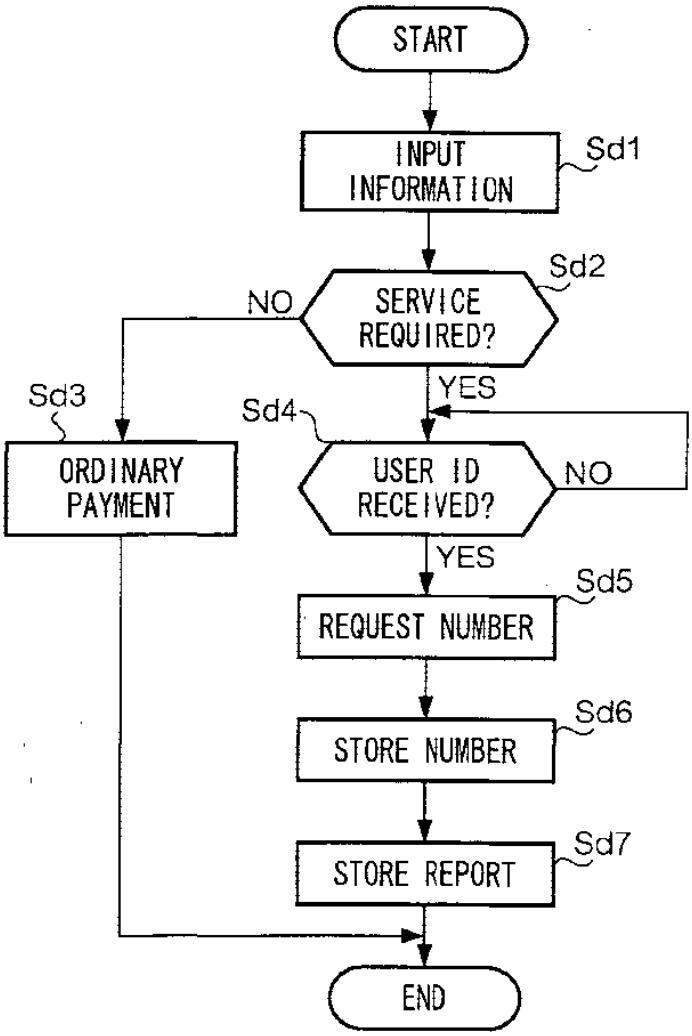


FIG. 17



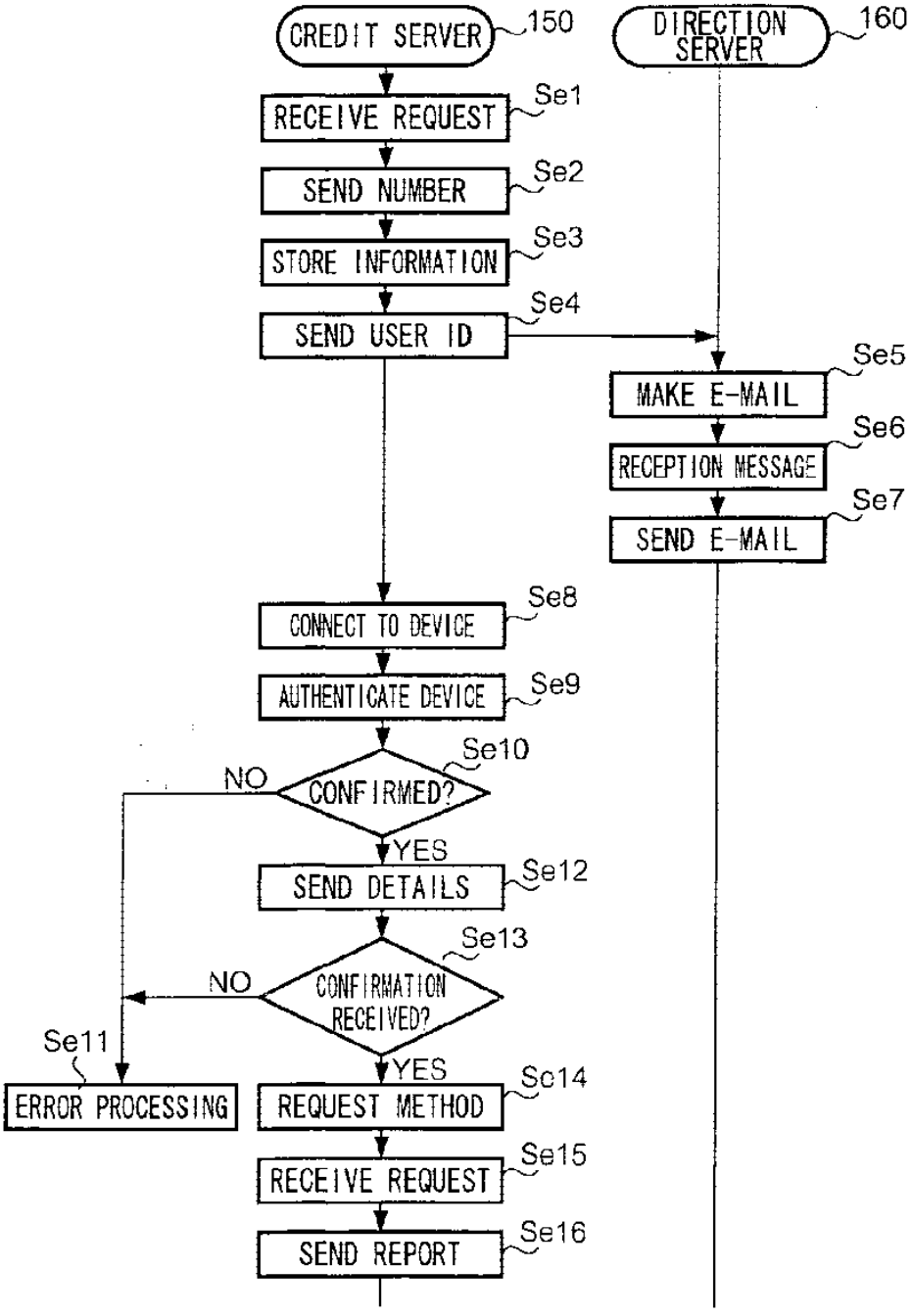
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 904 of 1360

FIG. 18



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 905 of 1360

FIG. 19



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 906 of 1360

FIG. 20

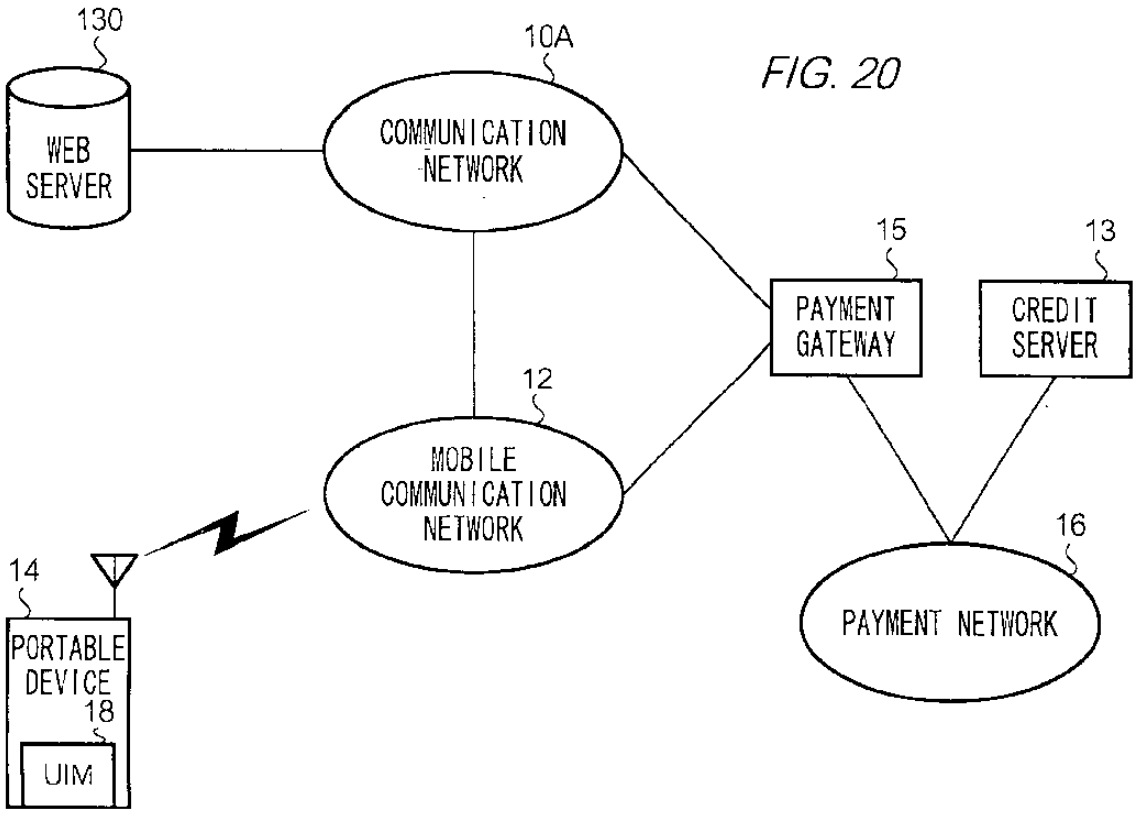
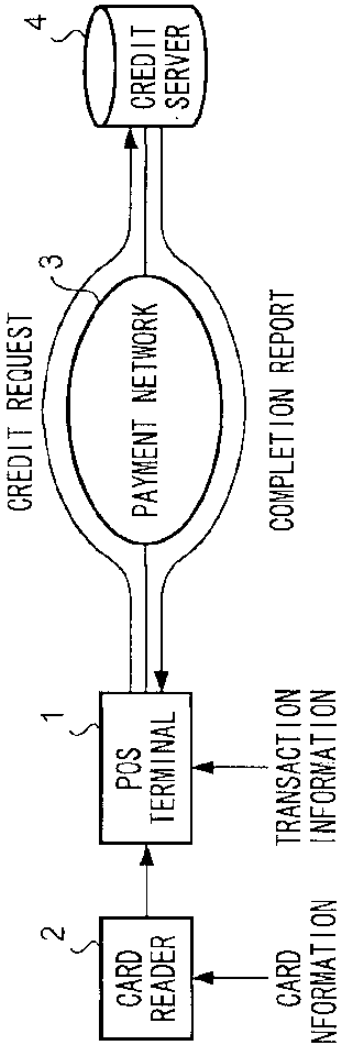
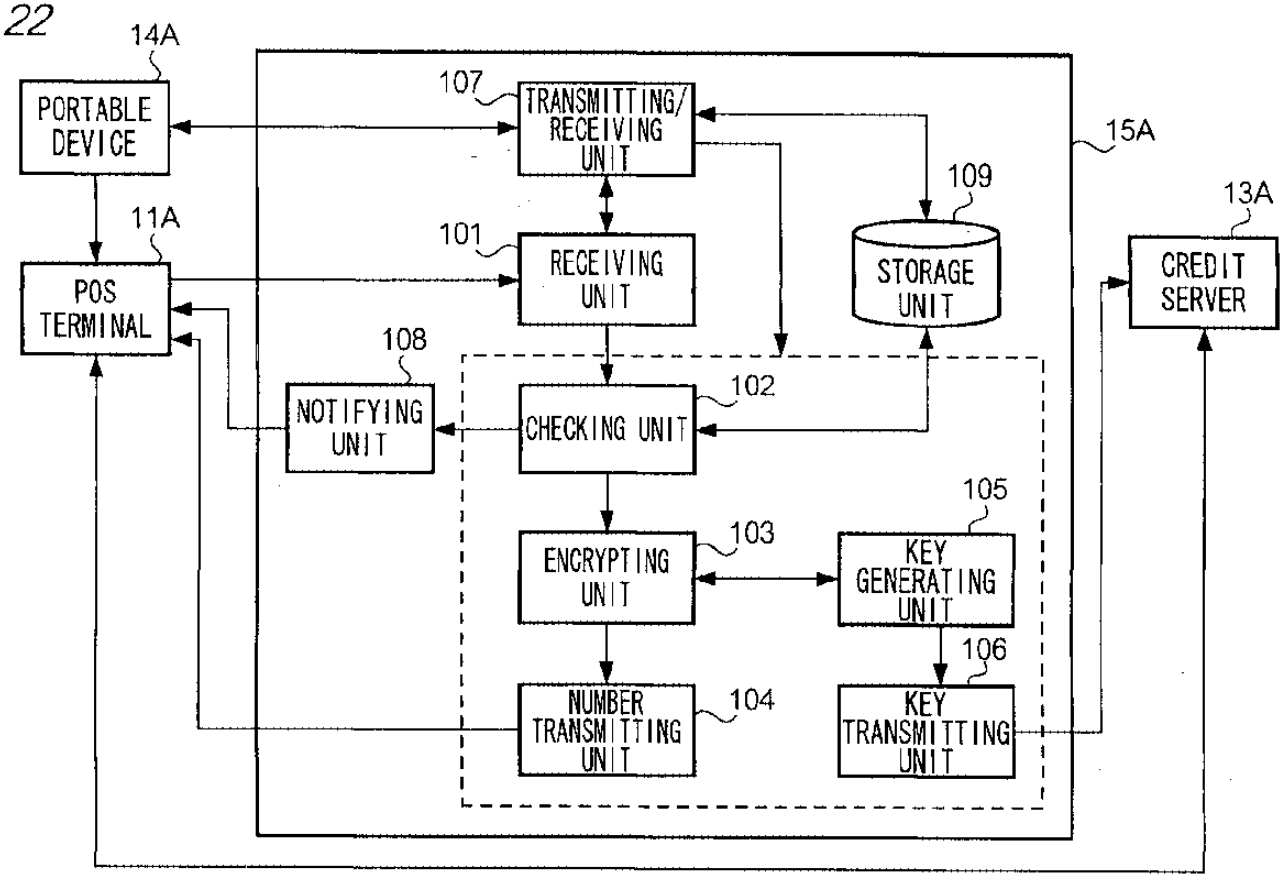

130
WEB SERVER
10A
COMMUNICATION NETWORK
15
PAYMENT GATEWAY
13
CREDIT SERVER
12
MOBILE COMMUNICATION NETWORK
16
PAYMENT NETWORK
14
PORTABLE DEVICE
18
UIM

FIG. 21



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 908 of 1360

FIG. 22



EP 1 280 115 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 909 of 1360

FIG. 23

ISSUER CODE	PAYMENT METHOD	MERCHANT CODE
.....	.....	.....
.....	.....	.....
.....	.....	.....
⋮	⋮	⋮

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 910 of 1360

FIG. 24A

MERCHANT CODE FOR CREDIT	PAYMENT METHOD	MERCHANT CODE
• • • •	• • • •	• • • •
• • • •	• • • •	• • • •
• • • •	• • • •	• • • •
⋮	⋮	⋮

FIG. 24B

USER NAME	ADDRESS	CARD NUMBER	EXPIRATION	LIMIT
• • • •	• • • •	• • • •	• • • •	• • • •
• • • •	• • • •	• • • •	• • • •	• • • •
• • • •	• • • •	• • • •	• • • •	• • • •
⋮	⋮	⋮	⋮	⋮

FIG. 24C

CARD NUMBER	KEY	TYPE	DATE	SERIAL NO.	MERCHANT NUMBER	AMOUNT NO.	PAYMENT METHOD	MERCHANDISE CODE
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

FIG. 24D

MERCHANT NUMBER	TYPE	DATE	SALES	CARD NUMBER	PAYMENT METHOD
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
	• • • •	• • • •	• • • •	• • • •	• • • •
	• • • •	• • • •	• • • •	• • • •	• • • •
⋮	⋮	⋮	⋮	⋮	⋮

EP 1 280 115 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 911 of 1360

FIG. 25A

MERCHANT CODE	MERCHANT NAME
• • • •	• • • •
• • • •	• • • •
• • • •	• • • •
⋮	⋮

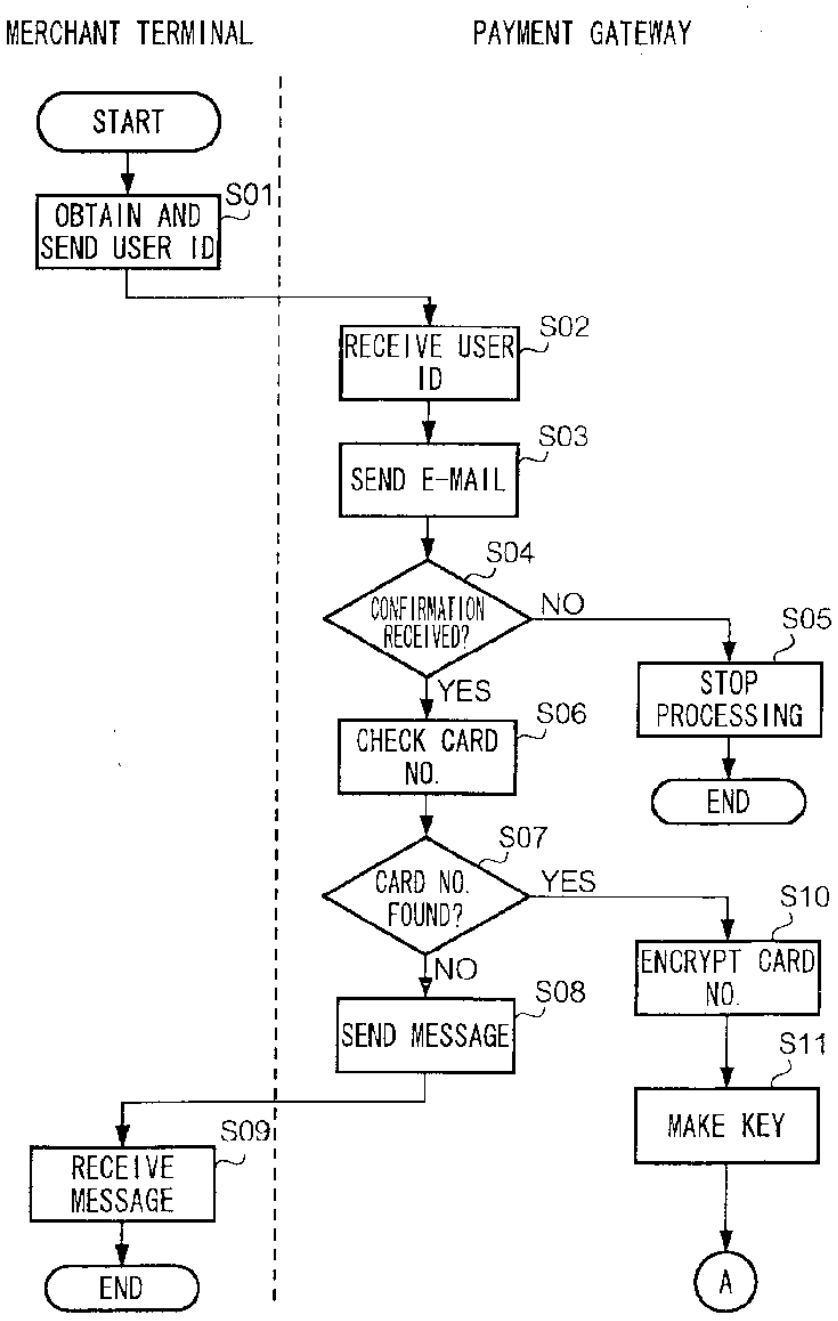
FIG. 25B

USER ID	PASSWORD	USER NAME	PHONE NUMBER	E-MAIL ADDRESS	DEVICE NO.	CARD NUMBER	ISSUER CODE	EXPIRATION
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

EP 1 280 115 A2

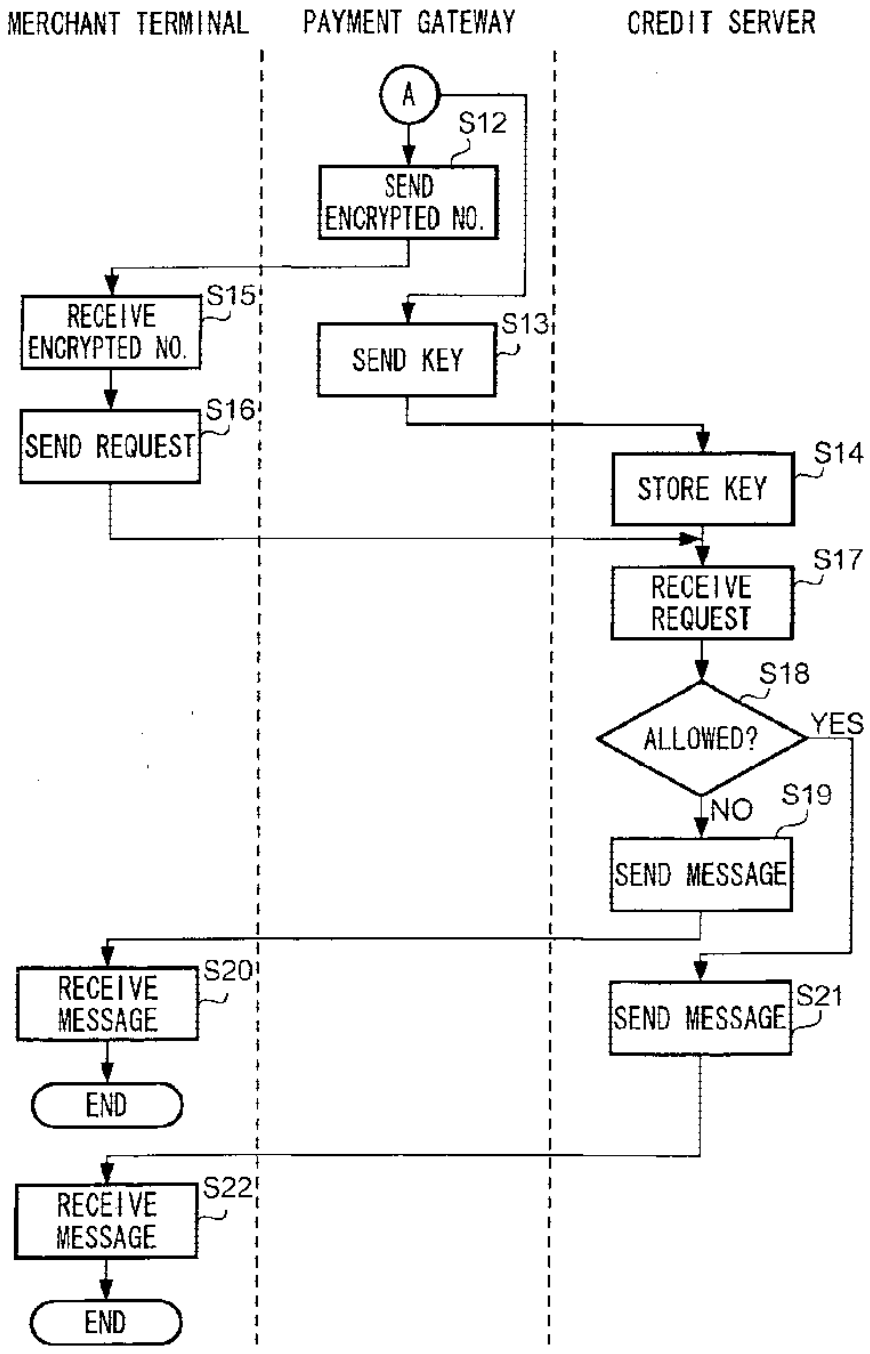
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 912 of 1360

FIG. 26



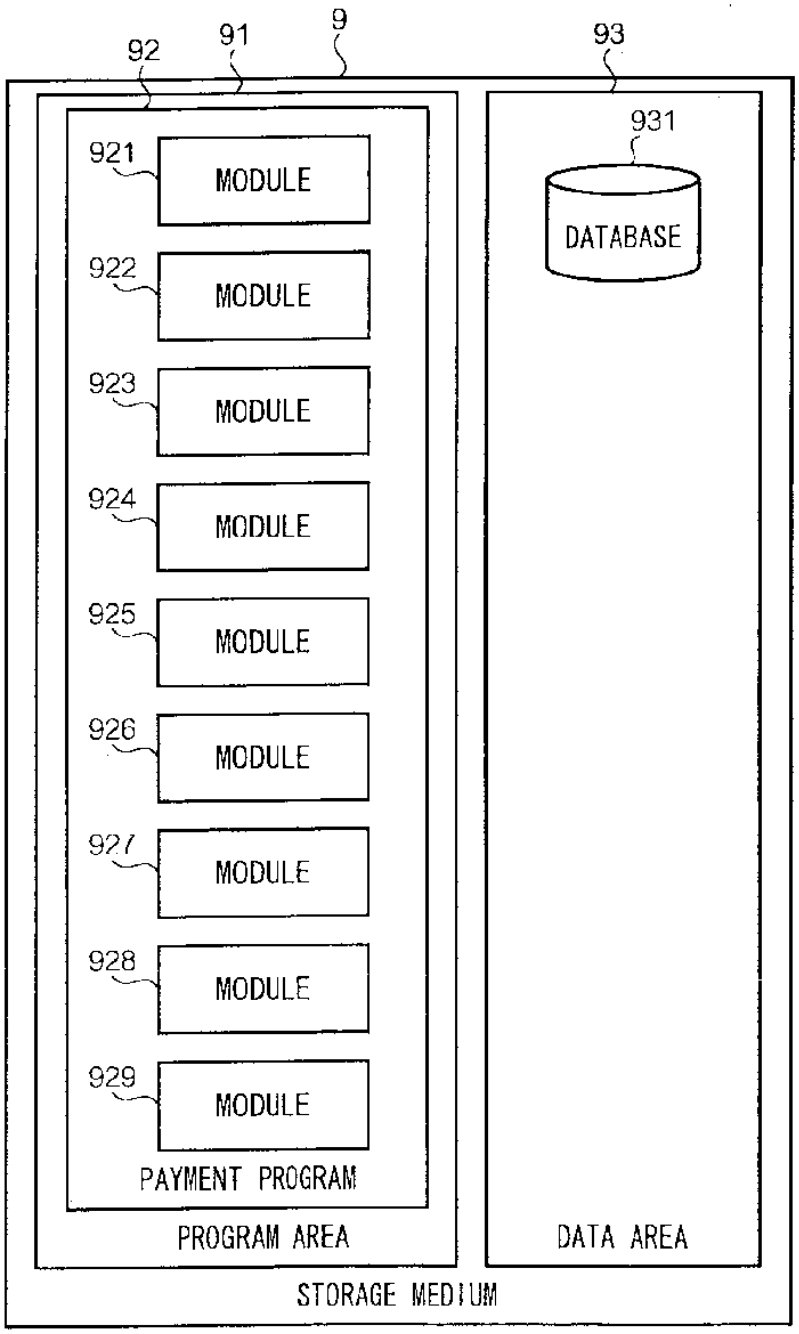
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 913 of 1360

FIG. 27



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 914 of 1360

FIG. 28



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 915 of 1360

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 280 115 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.01.2003 Bulletin 2003/05

(51) Int Cl.7: **G07F 19/00**, G07F 7/08

(21) Application number: **02015629.5**

(22) Date of filing: **16.07.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.07.2001 JP 2001222163**
29.01.2002 JP 2002020410

(71) Applicant: **NTT DoCoMo, Inc.**
Tokyo 100-6150 (JP)

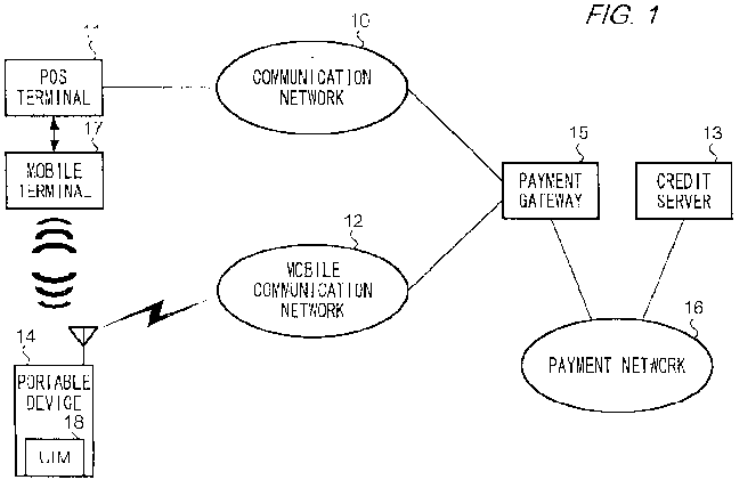
(72) Inventors:
- **Kinoshita, Masaki, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Yoshida, Junichi, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Nakajima, Atsushi, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Tanaka, Manabu, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Hanada, Kazutoyo, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Yasuda, Jun, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Tomita, Syuichi, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Nakamura, Taijiro, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Ishibashi, Hideaki, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**

(74) Representative: **HOFFMANN - EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) Electronic payment method, system, and devices

(57) A portable device authenticates a user of the portable device. If authenticity of the user is confirmed, a user ID is transmitted to a POS terminal. Upon receipt of the user ID, the POS terminal sends a request for payment including the user ID and transaction information to a payment gateway. Upon receipt of the request, the payment gateway sends an e-mail to the portable device to execute an application for payment stored in the portable device.

FIG. 1



EP 1 280 115 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 916 of 1360

Description

Background of the Invention

Field of the Invention

[0001] The present invention relates generally to a method, system and devices used for electronic financial transactions between financial institutions connected by a network.

Description of the Related Art

[0002] Electronic payment using a credit card is known in the art. As an example, a prior system for electronic payment is shown in fig. 21.

[0003] When a people (purchaser) buys goods at a shop, firstly, a clerk inputs transaction data including the name of goods, quantity, price, and tax into a Point of Sales (POS) terminal 1 provided at the shop. Secondly, he/she hand his/her credit card to the clerk. Thirdly, the clerk sets the card to a Card reader 2. Card reader reads out information such as a card number and expiration date stored in the card. Next, this card information is supplied to POS terminal 1. Upon receipt the information, POS terminal 1 makes a request for credit by adding information on the shop (merchant) to the card information and transaction data and sends it to a Credit server 4 managed by a credit card company via a Network 3 such as Credit Finance Information Switching Systems (CAFIS). Credit server 4 checks the card information included in the request sent by POS terminal 11. Finally if Credit server 4 accepts authenticity of the card, it sends a completion message to POS terminal 1. In such a system, a consumer buys goods without carrying cash.

[0004] However it is known that there is a security concern in such a system. Since a purchaser has to hand his/her credit card to a clerk in paying by a credit card, there is a danger that unauthorized persons improperly use the card. Furthermore, there is always a possibility of dropping off a credit card. In other words, a consumer necessarily takes risks that a stranger uses his/her credit card illegally.

[0005] The present invention has been made with a view to overcome the above problem and it is an object of the present invention to provide a method, system, server, terminal, computer program, and storage medium to conduct electronic financial transactions.

Summary of the Invention

[0006] To achieve the above aim, an electronic payment method of the present invention comprises the steps of:

authenticating a user of a user terminal on the basis of user identification information inputted to the user terminal by the user, by the user terminal;

storing an authentication result of the user, by the user terminal when the user terminal confirms authenticity of the user;

transmitting a user identification information stored beforehand in the user terminal to a merchant terminal when the user terminal confirms authenticity of the user, by the user terminal;

transmitting to payment device via a first communication network the user identification information and transaction information transmitted from the user terminal, by the merchant terminal;

receiving the user identification information and the transaction information transmitted from the merchant terminal, by the payment device;

identifying the user terminal on the basis of the user identification information and transmitting commands for instructing transmission of the authentication result to the user terminal via a second communication network;

transmitting authenticity of the user to the payment device via the second communication network if the user terminal stores authenticity of the user, by the user terminal; and

performing payment processing on the basis of the transaction information upon receipt of the authenticity from the user terminal, by the payment device.

[0007] In an electronic payment system in which the above method is applied, a user is able to pay by credit card using a terminal without handing a credit card to a clerk, thereby preventing a third-party including a clerk from using the card improperly. Furthermore, since the user terminal authenticates a user, if a third-party obtains a user terminal improperly, the terminal cannot be used for payment in the electronic payment system by the third-party. Furthermore, the payment device identifies a user to which authentication result is transmitted. In other words, the only user terminal that the payment device specifies can proceed payment processes. Thus, the danger of an improper use by a third-party of the user terminal is reduced. Furthermore, the user terminal transmits an authentication result according to the commands send from the payment device, in other words, a user does not have to operate the user terminal for the transmission. Therefore, the danger of stop of payment processing due to misoperation by a user is prevented.

[0008] In a preferred embodiment, an electronic payment method of the present invention comprises the steps of:

authenticating a user of a user terminal on the basis of user identification information inputted to the user terminal by the user, by the user terminal;

transmitting user identification information for identifying a user to a merchant terminal, by the user terminal, when the user terminal confirms authen-

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 917 of 1360

ficity of the user;
transmitting to a payment device via a first communication network the user identification information transmitted from the user terminal, by the merchant terminal;
receiving the user identification information from the merchant terminal, by the payment device;
identifying the user terminal referring to received user identification information and transmitting commands for executing an application for payment stored in the user terminal to identified user terminal via a second communication network, by the payment device;
upon receipt of the commands, executing the application to transmit a request for proceeding payment processing to the payment device via the second communication network, by the user; and
upon receipt of the request from the user terminal, performing a payment processing.

[0009] In this embodiment the payment device identifies a user terminal on the basis of user identification information and sends commands so that the user terminal can execute application for payment stored in the user terminal. In other words, both a user and a user terminal are authenticated, thereby ensuring security against authorized person greatly. In addition, a user's convenience is improved because a user does not have to carry out troublesome operation necessary for payment.

[0010] In another embodiment an electronic payment method comprises the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal, by a receiving unit
retrieving from a storage unit a card number corresponding to the
identified user, by a retrieving unit
encrypting the retrieved card number, by an encryting unit;
generating a key for decryption of the encrypted card number, by a generating unit;
transmitting to the merchant terminal the encrypted card number, by a first transmitting unit; and
transmitting the key to a credit server managed by an issuer of the credit card, by a second transmitting unit.

[0011] In an electronic payment system in which a method of this embodiment of the present invention is used, a user is able to pay by credit card to a merchant in a way that the merchant does not know a card number because a credit card number is encrypted for transmission to the merchant. Specifically, a payment device determines a card to be encrypted on the basis of the user identification information. On the other hand, the credit server obtains a card number by decrypting an encrypted card number using the key for decryption received from the payment device. Thus the credit server is able to carry out payment processing. Further, since the encrypted card number is generated each time a transaction is conducted, the merchant can manage sales at the shop using the encrypted card number although the merchant does not know card numbers.

[0012] An electronic payment system of the present invention has a payment device, a merchant terminal connected with the payment device via a first communication network and a user terminal connected with the payment device via a second communication network and is characterized in that:

the user terminal authenticates a user of the user terminal on the basis of user identification information inputted to the user terminal by the user;
if authenticity of the user is confirmed, stores authentication result; and
transmits to the merchant terminal user identification information stored in the user terminal;
the merchant terminal transmits to the payment device via the first communication network the user identification information transmitted from the user terminal and transaction information;
the payment device identifies the user terminal on the basis of the user identification information transmitted from the merchant terminal and
transmits to the identified user terminal via the second communication network commands for instructing transmission of the authentication result;
the user terminal transmits to the payment device via the second communication network according to the commands transmitted from the payment device when the user terminal stores the authentication result; and
upon receipt of the authentication result from the user terminal, the payment device performs payment processing on the basis of the transaction information.

[0013] In a preferred embodiment, an electronic payment system of the present invention is characterized in that:

the user terminal authenticates a user on the basis of the user identification information inputted to the user terminal by the user;
if authenticity of the user is confirmed, transmits to the merchant terminal a user identification information for identifying the user;
the merchant terminal transfers the user identification information to the payment device via the first communication network;
the payment device identifies the user terminal on the basis of the user identification information and transmits to the identified user terminal via the second communication network commands for execut-

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 918 of 1360

ing an application for payment stored in the user terminal;
the user terminal executes the application according to the commands and
transmits a request for proceeding payment processing to the payment device via the second communication network; and
the payment device performs the payment processing according to the request.

[0014] A communication terminal used for an electronic payment system of the present invention has a payment device connected with a first and a second communication network and a merchant terminal connected with the payment device via a first communication network and comprises

an authenticating means for authenticating a user of the communication terminal on the basis of a user identification information inputted to the user terminal by the user;
a storing means for storing an authentication result when authenticity of the user is confirmed by the authenticating means;
a storage medium for storing the user identification information;
a first transmitting means for transmitting, when authenticity of the user is confirmed, the user identification information stored in the storage means to the merchant terminal so that the merchant terminal transmits to the payment device a request for payment processing including the user identification information;
a receiving means for receiving commands for instructing transmission of the authentication result which is transmitted, in response to the request for payment, from the payment device via the second communication network; and
a second transmitting means for transmitting, upon receipt of the commands, a request for proceeding the payment processing including the authentication result to the payment device via the second communication network.

[0015] In a preferred embodiment, a communication terminal used for the electronic payment system comprises:

an authenticating means for authenticating a user of the communication terminal on the basis of a user identification information inputted to the user terminal by the user;
a first transmitting means for transmitting, when authenticity of the user is confirmed, the user identification information stored in the storage means to the merchant terminal so that the merchant terminal transmits to the payment device a request for payment processing including the user identification information
a receiving means for receiving commands for executing an application for payment which is transmitted from the payment device via the second communication network; and
a second transmitting means for executing the application for payment stored in the user terminal and transmitting, according to the application, a request for proceeding payment processing to the payment device via the second communication network.

[0016] A payment device of the present invention comprises:

a receiver for receiving a request for payment including a user identification information for identifying a user of a user terminal from a merchant terminal via a first communication network;
an identifying means for identifying the user terminal among registered user terminal on the basis of the received user identification information a transmitter for transmitting to the identified user terminal via a second communication network commands for executing an application for payment stored in the user terminal; and
a processing means for performing a payment processing on the basis of a request sent from the user terminal via the second communication network after transmission of the commands.

[0017] In another embodiment a payment device comprises:

a storage unit for storing a user identification information for identifying a user of a user terminal and a card number of a credit card correspondingly; a receiving unit for receiving from a merchant terminal a user identification information
a retrieving unit for retrieving from the storage unit a card number corresponding to the identified user;
an encrypting unit for encrypting the retrieved card number;
a generating unit for generating a key for decryption of the encrypted card number
a first transmitting unit for transmitting to the merchant terminal the encrypted card number and
a second transmitting unit for transmitting the key to a credit server managed by an issuer of the credit card.

[0018] A computer program product of the present invention makes a computer incorporated into a communication terminal used for the electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with the payment device via a first communication network to execute the steps of:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 919 of 1360

authenticating a user of the communication terminal on the basis of a user identification information inputted to the user terminal by the user;
storing an authentication result into a storage means when authenticity of the user is confirmed by the authenticating means;
transmitting, when authenticity of the user is confirmed, the user identification information stored in the storage means to the merchant terminal so that the merchant terminal transmits to the payment device a request for payment processing including the user identification information;
receiving commands for instructing transmission of the authentication result which is transmitted, in response to the request for payment, from the payment device via the second communication network and
transmitting, upon receipt of the commands, a request for proceeding the payment processing including the authentication result to the payment device via the second communication network.

[0019] In another embodiment, a computer program product makes a computer to execute the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal;
retrieving from a storage unit a card number corresponding to the identified user;
encrypting the retrieved card number;
generating a key for decryption of the encrypted card number transmitting to the merchant terminal the encrypted card number; and
transmitting the key to a credit server managed by an issuer of the credit card.

[0020] A storage medium of the present invention stores the above computer program products.

Brief description of the drawings

[0021]

Fig.1 is a conceptual block diagram to illustrate an electronic payment system based on the first embodiment of the present invention.
Fig.2 is a block diagram to illustrate a portable device used in the system.
Fig.3 illustrates a UIM mounted detachably to the portable device.
Fig.4 shows a storage area of EEPROM in the UIM.
Fig.5 is a block diagram to illustrate a POS terminal and a mobile terminal used in the system.
Fig.6 is a block diagram illustrating a payment gateway used in the system.
Fig.7 illustrates data items stored in a user table in a hard drive of the gateway.
Fig.8 illustrates data items stored in a transaction table in a hard drive of the gateway.
Fig.9 illustrates data items stored in an issuer table in a hard drive of the gateway.
Fig.10 illustrates data items stored in a merchant table in a hard drive of the gateway.
Fig.11 is a sequence flowchart illustrating payment processing in the system.
Fig.12 is a flowchart illustrating a processing performed by the portable device.
Fig.13 illustrates a screen displayed on a display of the portable device.
Fig.14 is a flowchart illustrating a processing performed by the portable device.
Fig.15 is a flowchart illustrating a processing performed by the portable device.
Fig.16 illustrates a screen displayed on a display of the portable device.
Fig.17 illustrates a screen displayed on a display of the portable device.
Fig.18 is a flowchart illustrating a processing performed by the POS terminal.
Fig.19 is a flowchart illustrating a processing performed by the payment gateway.
Fig.20 is a conceptual block diagram illustrating an electronic payment system based on a modification of the first embodiment.
Fig.21 illustrates an electronic payment system of the prior art.
Fig.22 illustrates an electronic payment system based on the second embodiment.
Fig.23 illustrates an example of date items stored in a POS terminal.
Fig.24 illustrates an example of date items stored in a credit server.
Fig.25 illustrates an example of date items stored in a storage unit of a payment gateway.
Fig.26 is a flowchart illustrating a method for payment used in the system.
Fig.27 is a flowchart illustrating a method for payment used in the system.
Fig.28 is a conceptual block diagram to illustrate a computer program for payment based on the second embodiment.

Detailed Description

(First embodiment)

[0022] The first embodiment of the present invention will now be described referring to the drawings.

A. Configuration of the system

A-1. Overall configuration

[0023] Fig. 1 shows that a system to which a method for electronic payment of the present invention based

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 920 of 1360

or the first embodiment is applied. As shown therein, the system comprises (a) a POS terminal 11 connected to a communication network 10, (b) a payment gateway 15 connected to Communication network 10, a mobile communication network 12, and a payment network 16, (c) a portable device 14 by which a user obtains communication services via Mobile communication network 12, (d) a credit server 13 connected to Payment network 16, and (e) a mobile terminal 17. For the sake of simplicity, only one POS terminal 11 and one Portable device 14 is shown in the figure. In actuality, a plurality of POS terminals are connected to Communication network 10 and many portable devices are connected to Mobile communication network 12.

[0024] A mobile communication network 12 includes mobile telephone networks in which Personal digital Cellular (PDC) scheme, Code Division Multiple Access (CDMA) scheme, or other schemes is used and data communication networks in which PDC-Packet (PDC-P) scheme is used. Each network has base stations which are not shown. Each base station covers an area and carries out radio communications with portable devices 14 within the area. Therefore, Portable device 14 is able to carry out voice and data communications by radio via Mobile communication network 12. A payment gateway 15 is connected to Mobile communication system 12, thus Portable device 14 is able to carry out data communications with Payment gateway 15.

[0025] A POS terminal 11 and Payment gateway 15 are connected via Communication network 10. Specifically, Communication network 10 is a dedicated line to which many POS terminals 11 and Gateway system 15 are connected. Needless to say, Communication network 10 can be a fixed telephone network, a public network such as Internet, or a mobile communication network (possibly Mobile communication network 12).

[0026] A credit server 13 managed by a credit company and Gateway system 15 are connected via a payment network 16. Specifically, Payment network 16 is designed especially for credit payment such as Credit and Finance Information Switching Systems (CAFIS). Credit server 13 is a conventional server for credit payment. Specifically, upon receipt of a request for credit transmitted by a POS terminal via Payment network 16, Credit server 13 checks authenticity of a credit card. If the authenticity is confirmed, Server 13 carries out a payment processing before sending a completion message to the POS terminal.

[0027] An essence of the electronic transaction service using a method for paying electronic transactions based on this embodiment is as follows. When a user of Portable device 14 buys goods at a shop, the user uses Portable device 14 to make request for payment to Credit server 13 via POS terminal 11 and Payment gateway 15. As such, a user is able to pay without handing a credit card to others including a clerk. Components of this system will be described in detail below.

A-2. Portable device

[0028] Portable device 14 has a function of carrying out wireless voice and data communications via Mobile communication network 12. Further, it has a function of carrying out short-range radio communication using Bluetooth, for example, to carry out data communications with POS terminal. In addition, the device 14 is able to mount a User Identity Module (UIM) detachably.

[0029] As shown in fig.2, Portable device 14 has a control unit 310, memory 320, control unit 330, communication unit 340, mic/speaker 350, UIM interface 360, and radio interface 370.

[0030] Control unit 310 has a Central processing unit (CPU) and other microprocessors to execute programs stored in Memory 320 to control each unit of the device 14 including reading/writing data from/to UIM 18.

[0031] Memory 320 includes a Read Only Memory (ROM), a Random Access Memory (RAM), and an Electrically Erasable and Programmable ROM (EEPROM) and has several storage areas, one of which is assigned for storing programs including programs for starting and proceeding payment described later, and another one of which is for storing data. Another program stored in Memory 320 is used for browsing, in other words, accessing a Web server on the Internet, downloading Hyper Text Markup Language (HTML) data or Compact-HTML (C-HTML) data, and displaying the data. Another one is used for sending and receiving e-mail. Control unit 310 executes these programs so that the user can browse and use e-mail.

[0032] Input device 330 has operation buttons such as a ten-key pad, which is not shown in the figure, to input information such as a telephone number and to select buttons or icons displayed on a liquid crystal display not shown in the figure. Communication unit 340 transmits data such as information on ordering via an antenna 341 under control of Control unit 34 and receives data send via Antenna 341. Mic/speaker 350 includes a microphone to input a sound and a speaker to output a sound.

[0033] UIM interface 360 supplies information outputted from Control unit 310 to UIM 18 and information outputted from UIM 18 to Control unit 310. Information stored in UIM 18 is used each time a user carries out voice and data communications by radio via Communication network 12. Radio interface 370 is used to carry out short-rage communication with POS terminal 11 by Bluetooth, for example.

A-3. UIM

[0034] As shown in fig.3, UIM 18 is an Integrated Circuit (IC) card which is detachable/attachable and includes a CPU 210, Interface 215, ROM 220, RAM225, and EEPROM 230. UIM 18 stores information unique to the user including a subscriber number and telephone book used for carrying out communication via Mobile

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 921 of 1360

communication network 12.

[0035] CPU210 executes a control program stored in ROM 220 to control each unit with n UIM 18. Interface 215 connects UIM 18 with Portable device 14. ROM 220 is a nonvolatile memory and stores programs for analyzing and executing commands supplied from Portable device 14 and for managing data, for example, as well as the control program. RAM 225 is a rewritable memory for temporarily storing data supplied from Portable device 14. EEPROM 230 is a versatile and is rewritable. EEPROM 230 stores information necessary for communication with Portable device 14.

[0036] Fig.4 shows storage areas in EEPROM. As shown, EEPROM 230 has storage areas 231 and 233.

[0037] Storage area 231 stores subscriber numbers, outgoing history, incoming history, talk time, telephone book data, and other information specific to user(s) of UIM 18. Storage area 233 stores information used when Portable device 14 starts a payment operation. Specifically, a device ID for identifying Portable device 14 uniquely is stored. For example, a user registers in advance, Portable device 14 at a provider of this electronic financial transaction service to obtain the service using the device 14. After the registration, the provider gives the user the device ID.

[0038] In addition, Storage area 233 stores an address such as Uniform Resource Locator (URL), to connect with Payment gateway 15. Further, Storage area 233 stores pairs of a user ID and a password, each of which is used for an application for payment executed at the Portable device 14 when the user uses the electronic payment service. If the user possesses two or more credit cards, it is possible that each pair of a user ID and a password corresponds to each credit card. Furthermore, Storage area 233 has an area for authentication results which is used for the payment application.

[0039] When UIM 18 is attached to Portable device 14, information stored in UIM 18 can be supplied to Portable device via UIM interface 360, thereby allowing for Portable device 14 to carry out various functions including radio communication.

A-4. POS terminal

[0040] POS terminal 11 is installed at a shop of a merchant participating in the electronic payment service. POS terminal 11 stores data necessary for managing information on financial transactions, sales, and customers, for example.

[0041] As shown in fig.5, POS terminal 11 has a control unit 710, a display 720, communication interface 730, and an interface 740.

[0042] Control unit 710 includes a CPU, a ROM, and a RAM and controls all units of POS terminal 11. Control unit 710 has the same function as a general POS terminal for managing information on financial transactions, sales, and customers. In addition, Control unit 710 has functions of controlling each unit to perform processing necessary for the electronic payment service. Display 720 includes a liquid crystal panel, for example, on which information on merchandise such as a name, price, quantity, tax, and total amount is displayed. Communication interface 730 carries out communication with Gateway system 15 via Communication network 10. Interface 740 is, for example, a general interface such as RS-232C or Universal Serial Bus (USB). POS terminal 11 is connected to Mobile terminal 17 through a cable to carry out data communication.

[0043] Mobile terminal 17 is, for example, a Personal Digital Assistants (PDA) or a laptop computer, which includes a control unit 810, interface 820, display 840, and radio interface 830.

[0044] Control unit 810 includes a CPU, ROM, RAM, and other modules and controls all units of POS terminal. Control unit 810 has the same functions as a general mobile terminal such as PDA. In addition, Control unit 810 has a function of controlling each unit to carry out processing necessary for the electronic transaction service.

[0045] Display 840 includes a liquid crystal panel to display information, for example. Interface 820 is, for example, a general interface such as RS-232C or Universal Serial Bus (USB). POS terminal 11 is connected to Mobile terminal 17 through a cable to carry out data communication. Radio interface 830 features short-range wireless communication with Portable device 14 via Bluetooth, for example.

A-5. Payment gateway

[0046] Payment gateway 15 for providing the electronic payment service using a method for electronic payment based on this embodiment is installed by a provider of the service. As shown in fig.6, Payment gateway 15 includes a payment server 150 connected to a Local Area Network (LAN), direction server 160, and a network interface (I/F) 170.

[0047] Network interface 170 is, for example, a router. Payment server 150 and direction server 160 exchanges data with POS terminal 10, Portable device 14, and Credit server 13 via Communication network, Mobile communication network, and Payment network 16, respectively.

[0048] Payment server 150 may be a personal computer or a workstation, including a CPU 151, ROM 152, RAM 153, hard drive 154, and LAN interface 155. Further, Payment server 150 includes an input device such as a keyboard and Cathode-ray Tube (CRT) or Liquid Crystal Display (LCD) allowing an administrator of Gateway system 15 to make reconfigurations including registration of users.

[0049] LAN interface 155 is used for exchange of data between Network interface 170 and Direction server 160 connected to the LAN.

[0050] CPU 151 performs arrhythmic computation as well controls each unit of Payment server 150. ROM 152

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 922 of 1360

stores programs to be read out and executed by CPU 151. CPU uses RAM 153 as a work area.

[0051] Hard drive 154 stores application programs and data to be read out and executed by CPU 151 to control each unit for provision of the electronic transaction service. Hard drive 154 includes a user table 154a, transaction table 154b, issuer table 154c and merchant table 154d.

[0052] As shown in fig.7, user table 154a has four areas for user ID 154aa, password 154ab, terminal ID 154ac, and credit card number 154ad. A staffer of the provider of this service inputs the above information into User table 154a when a user subscribes to the service. It is possible that, if a subscriber has more than two credit cards and wants to obtain the service using these credit cards, the subscriber (user) has a plurality of user IDs each of which is corresponding to each credit card.

[0053] Area 154aa stores user IDs each of which identifies a subscriber uniquely. Area 154ab stores passwords each of which is used for authentication of a user. Area 154ac stores identification information on each to identify Portable device 14 used for the electronic transaction service. The user IDs, passwords, and identification information stored in Hard drive 154 are the same stored in Storage area 233 in EEPROM 230 of UIM 18 shown in fig. 4. Area 154ad stores credit card numbers of users. If a user has two or more credit cards, the user can specify one or more credit cards to be used for this service and thus stored in Area 154ad when the user subscribes to the service. In addition, Area 154ad stores expiration dates of the cards, which are not shown in the figures.

[0054] Referring back to fig. 6, Transaction table 154ab has areas for storing details of transactions conducted by users. Specifically, as shown in fig. 8, Transaction table 154ab corresponding to a subscriber having a user ID "00001" has four areas for transaction 154ba, for date 154bb, for merchant number 154bc, and for transaction details 154bd. Area 154ba stores IDs each of which identifies a transaction conducted by a user. It is noted that CPU 151 gives a transaction ID every time a transaction is conducted. Area 154ab stores dates and times of transactions each corresponding to each transaction ID. Area 154bc stores merchant numbers each identifying a shop where the transaction was conducted. A unique merchant number is assigned to all merchants in advance. Area 154bd stores details of transactions each corresponding to each transaction ID. Specifically, merchandise name, quantity, price, tax, payment method (lump-sum, installment, payment with bonus, payment partially with bonus, and, revolving, for example), and other related information on the transaction.

[0055] Referring again to fig. 6, Issuer table 154c stores information on credit companies and credit cards available for the service. Specifically, as shown in fig. 9, Issuer table 154c has three areas. Area 154ca stores ranges of card numbers. Area 154cb stores company codes each of which identifies corresponding credit company. Area 154cc stores names of credit companies. For example, fig. 9 shows that a credit card whose number lies within a range between "1525000000" and "1525059999" is issued by credit company "A".

[0056] Referring again to fig. 6, Merchant table 154c stores information on which cards and which methods of payment are available at a shop. Specifically, as shown in fig. 10, Merchant table 154d has four areas of 154da, 154db, 154dc, and 154dd. Area 154da stores codes each of which identifies each merchant. Area 154db stores merchants names. Area 154dc stores codes each of which identifies a credit company, namely, issuer of a credit card available for the merchant, which is the same stored in Area 154cb shown in fig. 9. Area 154dd stores credit company's names. Area 154de stores payment methods in which a user can pay by a card. As an example, fig. 10 shows that a user is able to arrange payment in a lump-sum, installments or revolving system but neither payment with bonus nor payment partially with bonus is accepted. "_", "I", "B", "pB", and "R" represents lump sum, installments, bonus, bonus (partially), and revolving, respectively. Furthermore, detailed information such as the number of payment in installments and an available period in payment with bonus may be stored.

[0057] Direction server 160 will now be described referring to fig. 6. Direction server 160 may be a personal computer or a workstation, including a CPU 161, ROM 162, RAM 163, hard drive 164, and LAN interface 165. Further, Payment server 150 includes an input device such as a keyboard and Cathode-ray Tube (CRT) or Liquid Crystal Display (LCD). Detailed description of these devices is omitted.

[0058] LAN interface 165 is used for exchange of data between Network interface 170 and Payment server 150 connected to the LAN. CPU 161 performs arithmetic computation as well controls each unit of Direction server 160. ROM 162 stores programs to be read out and executed by CPU 161. CPU uses RAM 163 as a work area. Hard drive 164 stores application programs and data to be read out and executed by CPU 161, to control each unit for provision of the electronic payment service. In addition, Hard drive 164 stores a mail box 164a used for the electronic transaction service. To be more specific, Mail box 164a includes mailboxes each corresponding to an e-mail account of Portable device 14.

[0059] Upon receipt of a request from Payment server 150, CPU 161 generates and stores e-mail into a mail box assigned to each Portable device 14 in Mail box 164a and sends a reception message to the Portable terminal 14 having an address indicated by the request. Upon receipt of the reception message, Portable device 14 accesses Mailbox 164a via Mobile communication network to obtain e-mails for Portable device 14. Namely, Direction server 160 a function as a mail server with features including sending a reception message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 923 of 1360

B. Operations of the system

B-1. Overall sequence of the operations

[0060] An outline of sequence of operations carried out in this electronic payment system will now be described.

[0061] Fig. 11 is a sequence flowchart showing an outline of sequence of operations in which a user of Portable device 14 conducts a transaction (purchases goods) at a shop at which POS terminal 11 and Mobile terminal 17 are installed and obtains this electronic payment service for payment using Portable device 14.

[0062] As shown in fig. 11, firstly, a clerk inputs information on a transaction including a merchandise name, quantity, price, tax into POS terminal 11 at a shop. If a purchaser wants to pay using this electronic payment service, the purchaser operates his/her Portable device 14 to execute an application program for the electronic payment. And an input screen for a user ID and a password to be used for authentication is displayed on a display of Portable device 14.

[0063] The purchaser (the user of Portable device 14) operates ten-key pad or the like, to input a user ID and a password. Portable device 14 checks the user ID and password against those stored in UIM 18, to authenticate the user (step S1).

[0064] If the authentication failed, Portable device 14 notifies the user that the user is not a right person and thus rejected before carrying out error processing, for example, terminating the processing. If the authentication is completed, Portable device 14 sends the user ID stored in UIM 18 to Mobile terminal 17 by short-range wireless communication. The user ID is transferred from Mobile terminal 17 to POS terminal 11 (step S2). In addition, Portable device 14 stores the authentication result representing authenticity of the user into Storage area 233 of UIM18. It is noted that Mobile terminal 17 is omitted in fig. 1 for sake of simplicity. But in reality data is exchanged via Mobile terminal 17 between POS terminal 11 and Portable device 14.

[0065] Upon receipt of a user ID sent from portable device 14 via Mobile terminal 17, POS terminal 11 sends to Payment gateway 15 via Communication network 10 transaction information, the user ID, and a request for transaction number including information to identify the shop (merchant), which is inputted buy a clerk (step S3). Upon receipt of the request sent from POS terminal, Payment gateway 15 stores the transaction information included in the request into Transaction table 154b and adds a transaction number to the transaction information to send back to POS terminal 11 via Communication network 10 (step S4).

[0066] Further, Payment gateway 15 sends an e-mail including commands for direction of payment to Portable device 14 indicated by the user ID included in the request (step S5). Upon receipt of the e-mail sent from Payment gateway 15 via Mobile communication system 12, Portable device 14 executes an application for payment according to the commands included in the e-mail.

[0067] Specifically, the authentication result and the device ID both stored in UIM 18 are transmitted to Payment gateway 15 via Mobile communication network 12, to make a request for proceeding payment processing (step S6). Therefore, the user need not do complicated procedures for payment, for example inputting information on the transaction which is often bothersome for a user. In this system a request for proceeding payment processing is sent to Payment gateway 15 automatically after completion of the authenticity.

[0068] Upon receipt of the authentication result and the request including the device ID both sent from Portable device 14 via Mobile communication network 12, Payment gateway 15 confirms authenticity of the user through the result. Next, Payment gateway 15 authenticates the Portable device 14 by checking the device ID (step S7). Specifically, Payment gateway 15 checks the device ID sent from Portable device 14 against a device ID stored correspondingly to the user ID in User table 154a. If the two IDs coincide, authenticity of Portable device 14 is established. Otherwise Payment Gateway 15 stops payment processing.

[0069] If the authenticity of Portable device 14 is established, Payment gateway 15 sends to Portable device 14 via Mobile communication network 12 transaction details including name of goods, quantity and price and information on possible payment methods (step S8). Upon receipt of a payment method and a confirmation from Portable device 14 (step S9), Payment gateway 15 retrieves transaction information from Transaction table 154b and a credit card number and its expiration date from User table 154a. Next, Payment gateway 15 sends to Credit server 13 via Payment network 16 a request for credit including information on the merchant and the payment method along with the retrieved transaction information (step S10).

[0070] Upon receipt of the request Credit server 13checks the credit card number and its expiration date, to determine whether to conduct the payment processing. If the credit card number and the expiration date are proper, Credit server 13 carries out payment processing (step S11) and sends a completion report to Payment gateway 15 via Payment network 15 (step S12). This report is transferred from Payment gateway 15 to POS terminal 11 via Communication network 10 and to Portable device 14 via Mobile communication network 12 (step S13 and step S14, respectively). B-2. Operations of portable device

[0071] It will now be described that processing carried out by Portable device 14 when a user obtains the electronic payment service. As shown in fig. 12, if a user wants to use the service using his/her Portable device 14 when purchasing goods at a shop, the user inputs with input device 330 a direction for Portable device to execute an application for payment. Control unit 310 of Portable device 14 displays credit cards available for the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 924 of 1360

user on a display

[0072] An example of a screen for selection of a credit card displayed on a display of Portable device 14 is shown in fig.13. This screen shows a list of credit cards registered in advance by the user at a provider of the service. When the user operates Input device 350 to select a check box and clicks an "OK" button, a credit card for use in the payment is determined.

[0073] After selection of a credit card, Control unit 310 displays an input screen for a user ID and a password on the display. When the user inputs a user ID and a password, Control unit 310 authenticates the user by the inputted user ID and password (step Sa3). Specifically, Control unit 310 compares a user ID and a password each corresponding to the selected credit card stored in Storage area 233 in EEPROM of UIM 18 with the inputted user ID and password. If the two user IDs and two passwords coincide, Control unit 310 confirms authenticity of the user. If not, it confirms inauthenticity. If the authenticity is confirmed (step Sa3 "NO"), Control unit 310 carries out error processing (step Sa4) for example, displays an error message on the display. If the authenticity is confirmed (step S3 "YES"), Control unit 310 stores the authentication result (authenticity) into Storage area 233 (step Sa5) and outputs the user ID stored in Storage area 233 to Radio interface 370 to transmit to Mobile terminal 17 (step Sa6). Then Control unit 310 terminates processing.

[0074] It is noted that when storing the authentication result into Storage area 233, Control unit 310 may write an expiration time of the authentication result, which is an hour, for example. After the expiration, Control unit 310 deletes the authentication result.

[0075] As a result, a user ID is sent from Portable device 14 to Mobile terminal 17 and subsequently a request for payment is sent from POS terminal to Payment gateway 15 (step S3 in fig.11). Next, an e-mail including commands to execute an application for payment (step S5 in fig.11) is transmitted from Payment gateway 15 to Portable device 14.

[0076] It will now be described that operations of Portable device 14 after reception of the e-mail sent from Payment gateway 15 referring to fig.14. Firstly, Control unit 310 checks whether an e-mail is received (step Sb1).

[0077] If Portable device 14 receives any e-mails, Control unit 310 terminates processing. If Portable device receives e-mail, Control unit 310 determines whether the e-mail is sent from Payment gateway 15 and checks whether the e-mail contains predetermined commands referring to the content of the e-mail (step Sb2).

[0078] If a sender of the e-mail is not Payment gateway 15 or the e-mail does not contain predetermined commands, Control unit 310 terminates the processing. If the sender is Payment gateway 15 and the e-mail contains predetermined commands, Control unit 310 executes an application for payment (step Sb3) before termination.

[0079] Control unit 310 repeats the above series of processes periodically so that the application for payment is executed automatically when receiving an e-mail including the commands.

[0080] It will now be described that operations of Portables device 14 after execution of the application referring to fig. 15.

[0081] Firstly, Control unit 310 reads out from Storage area 233 an address such as Uniform Resource Locator (URL), to access Payment gateway 15 via Mobile communication network 12 (step Sc1). To ensure security Secure Socket Layer (SSL) is used for data exchange between Portable device 14 and Payment gateway 15.

[0082] To be more specific, when sending a request for access to Payment gateway 15, Portable device 14 requests transmission of an electronic certificate issued by a Certificate Authority (CA) which is not shown in the figure. In response to the request, Payment gateway 15 sends the certificate to be confirmed by Portable device 14. Therefore, Portable device 14 is able to check authenticity of Payment gateway 15, thereby avoiding a danger of communication with an unauthorized server posing as an authorized server. After confirmation of authenticity of Payment gateway 15, data exchange starts. Needles to say, SSL is applied for such data exchange. Since SSL has become a common technique, detailed description is omitted.

[0083] After establishment of the connection between Portable device 14 and Payment gateway 15, Portable device 14 retrieves an authentication result (authenticity), a user ID, and a device ID from Storage area 233. Next, Portable device 14 transmits a request for authentication of the device 14 to Payment gateway 15 via Mobile communication network 12 to request including the retrieved user ID and device ID (step Sc2). At the same time, Control unit 310 measures time (step Sc3). If Portable device 14 does not receive information from Payment gateway 15 in response to the transmission after predetermined time (two minutes, for example), Control unit 310 terminates this processing and performs time-out processing, for example, displaying a message notifying to a user that this payment processing is aborted and must be carried out from the beginning.

[0084] As described before, when Portable device 14 sends an authentication result, a user ID, and a device ID to Payment gateway 15, Payment gateway 15 authenticates confirms the authenticity of the user and device 14. If the authenticity is confirmed, detailed transaction information is sent to Portable device (step S7 and step S8 of fig.11)

[0085] When authenticity is confirmed and thus information on transaction details (name of goods, quantity price, tax, merchant, for example) is transmitted from Payment gateway 15, Control unit 310 displays the transaction details on the display (step Sc4) to be checked by the user.

[0086] Fig.16 shows an example of a screen on which

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 925 of 1360

the transaction details is displayed. As shown therein, a name of merchant (shop), a total amount to be paid by the user, and buttons for direction. A user selects one of the buttons of "Agree" and "Not agree" for proceeding or stop paying, respectively. Control unit 310 determines which buttons is selected, in other words, whether the user agrees with this transaction (step Sc5).

[0087] If "Not agree" is selected (step Sc5 "NO"), Control unit 310 stops payment processing (step Sc6). If "Agree" is selected (step Sc5 "YES"), Control unit 310 transmits request for proceeding payment to Payment gateway 15 via Mobile communication network 12 (step Sc7).

[0088] In response to the request for proceeding payment, information on payment methods is transmitted from Payment gateway 15 via Mobile communication network 12, (step Sc8 in fig.11). Upon receipt of the information on payment methods, Control unit 310 displays a list of available payment methods on the display (step Sc8), one of which is to be selected by the user. Fig.17 shows an example of a screen on which the list is displayed. As shown therein, check-boxes each corresponding to each payment method are displayed. A user selects a check-box and "OK" button, to determine a payment method the user would like.

[0089] After the determination, Control unit 310 transmits to Payment gateway 15 via Mobile communication network 12 information for identifying the determined payment method (step Sc9). Upon receipt of the information of payment method, Payment gateway 15 sends a request for credit to Credit server 13. Subsequently, Payment gateway 15 sends a completion message to Portable device 14. Upon receipt of the message, Control unit 310 displays a massage such as "Payment has now been completed." on the display.

B-3. Operations of POS terminal 11

[0090] It will now be described that operations carried out in POS terminal 11 referring to fig. 18. When a user conducts a financial transaction namely, buys goods at a shop, a clerk inputs transaction information including name of goods, quantity, price, and tax into POS terminal (step Sd1) to store the information into storage areas. Control unit 710 determines whether a user wants to use this electronic payment service (step Sd2).

[0091] If the user does not want to use this service, or the user pays in cash (step Sd2 "NO"), Control unit 710 performs processing similarly to a general POS terminal (step Sd3). If the user wants to use the service, in other words, the user inputs a request of this service to POS terminal, Control unit 710 accesses Mobile terminal 17 via Interface 740, to determine whether a user ID is received (step Sd4).

[0092] If Mobile terminal 17 has not yet received a user ID sent from Portable device 14 using a short-range radio communication, Control unit 710 repeat accessing periodically until Mobile terminal 17 receives a user ID. When Mobile terminal 17 has received a user ID, Control unit 710 obtains the user ID via Interface 740. Next, Control unit sends to Payment gateway 15 via Communication network 10 a request for transaction number including the transaction information, the merchant information, and the user ID (step Sd5).

[0093] Transaction number is transmitted from Payment gateway 15 to POS terminal 11, in response to the request (step S4 in fig.11). Upon receipt of the transaction number from Payment gateway 15, Control unit 710 stores the received transition number in relation with the transaction information stored in POS terminal earlier (step Sd6).

[0094] After that, Control unit 710 waits for a completion message sent from Payment gateway 15. When receiving a completion message after data exchange between Portable device 14 and Payment gateway 15, Control unit 710 stores the completion message in relation with the transaction information and transaction number (step Sd7) and finally prints out a receipt for the transaction.

B-4. Operations of Payment gateway 15

[0095] It will now be described that operations performed in Payment gateway15 referring to fig. 19. Upon receipt of a request for transaction number from POS terminal 11(step Se1), CPU 151 of Payment server 150 issues a transaction number and sends it to POS terminal 11 via Communication network 10 (step Se2). CPU 151 stores the transaction information, the merchant information, the transaction number, and the date and time included in the request for transaction number into Transaction table 154b (step Se3).

[0096] Next, CPU 151 sends the user ID included in the request for transaction number to Direction server 160 (step Se4). Upon receipt of the user ID sent from Payment server 150, CPU 161 of Direction server 160 generates and stores into a mailbox 164a of the user an e-mail including commands for execution of an application for proceeding payment processing stored and executed in Portable device 14 (step Se5). Next, CPU 161 sends a reception message to Portable device 14 identified by the user ID. When Portable device 14 sends, in response to the message, a request for the e-mail to Direction server 160, CPU 161 sends the e-mail to Portable device 14 (step Se7).

[0097] Upon receipt of the e-mail, Portable device 14 executes the application to make a request for connection with Payment server. CPU151 establishes a connection by using SSL (step Se8). After establishment of the connection, Portable device 14 sends the User ID authentication result (authenticity of the user), and the device ID to Payment server 150. Payment server 150 checks the authentication result and next authenticates Portable device 14 on the basis of the device ID (step Se9). Specifically, CPU 151 compares the device ID sent from Portable device 14 with a device ID stored in

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 926 of 1360

relation with the user ID in User table 154a. If the two device IDs coincide, CPU 151 determines authenticity of the device 14 (step Se10).

[0098] If authenticity of the device 14 is not confirmed, namely, the two device IDs do not coincide, CPU 151 sends an error message to Portable device 14 and carries out error processing, for example, stops processing (step Se11). If the authenticity is confirmed, CPU 151 reads out information including transaction details and merchant information stored in Transaction table 154b in step Sc3, to send to Portable device 14 via Mobile communication network 12 (step Sc12).

[0099] Upon receipt of the above information, Portable device 14 urges the user to confirm the transaction details (step Sc4 and Sc5 in fig.15). If the user agrees with the transaction, a confirmation is transmitted to Payment gateway 15. If the user does not agree, nothing is transmitted. CPU 151 determines whether the confirmation is received within a predetermined time from transmission of the information to Portable device 14 (step Se13). If the confirmation is not received within the time, CPU 151 carries out error processing, for example, stops processing (step Se11).

[0100] If the confirmation is received within the time, CPU 151 determines payment methods available for the transaction and sends information on the payment methods to Portable device 14 via Communication network 12 so that the user can select one among the methods (step Se14). Specifically, CPU 151 refers to User table 154a of fig.7 to specify a credit card number corresponding to the user ID sent from Portable device 14. When the card number is specified, CPU151 refers to Issuer table 154c shown in fig.9 to specify an issuer of the card.

[0101] More specifically, CPU 151 determines within which range the card number lies in 154ca to specify the company. After the company is specified, CPU 151 refers to Merchant table 154d (cf. fig.10), to determine payment methods on the basis of the company and the merchant information included in the request for transaction number sent from POS terminal 11. Suppose that Merchant table 154c shown in fig.10 is stored in HDD 154, that a company "A" whose code number is "2a11111", and that a merchant "A" whose code number is "1111111111". CPU would determine that the user can pay in lump sum, installments, and revolving system and cannot pay with bonus and partially with bonus.

[0102] After transmission of the payment methods to Portable device 14, Portable device 14 sends a payment method to Payment gateway 15. Upon receipt of the payment method, CPU 151 make a request for credit with data in a predetermined format containing the credit card number, the expiration date, the transaction details (name of goods, quantity, price), the merchant information, the payment method and other related information, to transmit to Credit server 13 via Payment network 16 (step Se15). It is possible that the predetermined format is conventional one used for data exchange between a conventional credit server and a payment device. Finally, CPU 151 terminates processing of the transaction.

[0103] After transmission of the request for credit, CPU 151 waits until a completion message notifying completion of credit sent from Credit server 13 is received. Upon receipt of the completion message, CPU 151 forwards the completion message to POS terminal via Communication network 10 and to Portable device 14 via Mobile communication network 12 (step Se16).

[0104] As described above, by using the electronic financial transaction service in which a method for electronic payment based on this embodiment is applied, a purchaser don't have to hand his/her credit card in payment to a third-party including a clerk. Furthermore, a purchaser doesn't have to carry a credit card for shopping. Therefore, the danger of card information leakage and possible abuse of cards decreases drastically.

[0105] Also, Portable device 14 authenticates a user at payment, if a third party or other improper person obtains Portable device 14 improperly, the person cannot pay on credit using Portable cevice 14, thereby preventing the danger of abuse of Portable device 14.

[0106] Since information necessary for payment including a card number and an expiration date is stored in Payment gateway 15, not in Portable device14 or UIM 18, if Portable device 14 or UIM is stolen or improperly obtained, there is little danger of card information leakage from Portable device 14 or UIM. Further, sensitive information such as a card number and expiration date is managed by Payment gateway 15 and cannot provided to public networks such as Mobile communication network 12 and Communication network 10. Therefore, the danger of wiretapping such sensitive information via a public network is reduced.

[0107] In this embodiment, sensitive information necessary for payment is stored in both Portable device 14 and detachable UIM 18. Thus, a user is able to detach UIM from Portable device 14 when it is not required, to prevent the danger of information leakage. Even if such information is leaked, an improper user cannot pay using the device 14 since Payment gateway 15 authenticates Portable device 14 as well a user. In other words, both a user and a portable device are checked.

[0108] In this embodiment, Portable device 14 sends a request for payment to Payment gateway 15 via POS terminal 11; and upon receipt of the request, Payment gateway 15 sends an e-mail to Portable device 14 to obtain a confirmation of transaction from the user. Thus, even if an improper person obtains a user ID and intends to pay using another portable device in combination with the obtained user ID, needless to say, it is the only authorized Portable device 14 that receives the e-mail. Therefore, the improper person does not receive the e-mail and thus is not able to conduct a transaction using the obtained user ID. Namely, the danger of leakage and abuse of a user ID is restricted.

[0109] In the prior art, Payment gateway 15 may sends to Portable device 14 an e-mail including a mes-

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 927 of 1360

sage like "Please connect with the Payment server for payment", to obtain an instruction of payment from the user. Namely, a user operates Portable device 14 one after another referring to messages. However in this way, it is often the case that a user forgets operation procedures, or carries out wrong operations. This will cause a problem that a transaction stops or remains uncompleted. On the other hand, in this embodiment Portable device14 "automatically" executes an application for payment according to commands included in the received e-mail, thereby preventing suspension or stop of payment due to a misoperation made by a user.

[0110] Further, a user is able to register a plurality of credit cards used for the electronic financial transaction service. Specifically, each password is stored in UIM correspondingly to each credit card. As a result, a user is able to select credit cards for use in its appropriate way by inputting each user ID, for example.

[0111] It is noted that a method for payment based on the present embodiment has advantages in a merchant as well as a user described. That is, although a request for transaction number sent from POS terminal 11 to Payment gateway 15 does not contain a card number and expiration date which are send from a POS terminal 1 to a credit server 4 as shown in fig.21 in a conventional system Payment gateway 15 does contain transaction details and a merchant information used in a conventional system. Therefore, a merchant can participate in this transaction service simply by making, at POS terminal 11, a data including information necessary for a transaction in a conventional format and sending it to Payment gateway 15. This provides benefits to a merchant because the merchant does not have to install a new POS terminal.

[0112] Further, Credit server 13 performs processing in the conventional way because Payment gateway sends a request for credit in a conventional format to Credit sever 13. This provides convenience to a credit company because the company does not have to install a new server.

[0113] Since Transaction table 154b stores transaction details conducted by a user, it is possible that Payment gateway collectively manages electronic records or payments (so called electronic receipt). In a conventional credit payment system, generally a merchant issues a payment voucher on which transaction details are entered and mails it to a depository for managing payment vouchers provided by an issuer. However in this embodiment, Payment gateway 15 is able to manage payment information collectively, thus the cost of issuing and managing payment vouchers can be reduced.

C. Modification of the first embodiment:

[0114] The present invention is susceptible to many modifications as follows.

[0115] In the above embodiment, Storage area 233 of UIM 18 stores a device ID for identifying Portable device 14 used for the electronic financial transaction service. Portable device14 transmits the device ID to Payment gateway 15 and Payment gateway 15 compares the transmitted device ID and a device ID stored in User table 154a for authentication of the device 14. However it is possible that the authentication is carried out using SSL, for example. In this case, Portable device 14 sends to Payment gateway 15 a digital certificate for client authentication which has been registered at Certificate Authority (CA). Payment gateway 15 authenticates a device using the certificate.

[0116] In the above embodiment, Portable device 14 urges a user to input a user ID and a password for a user authentication. However it is possible to use biometrics such as fingerprint, iris scan, or combined voice and face patterns for the authentication.

[0117] In the above embodiment, a user ID is transmitted to POS terminal 11 via Mobile terminal 17 when the user conducts a financial transaction at a shop. However, the present invention is not only applied to such an actual shop but can be applied to an online shopping via Internet, for example. An example of such applications is shown in fig.20 in which a Web server 130 is provided instead of POS terminal 11 and Mobile terminal 17.

[0118] Web server 130, so called an online shop server, receives a request for purchase from terminals including a personal computer and a mobile phone with features of Web browsing. To be more specific, when user selects or inputs a URL for connection with the Web server 130, a web page for selection of goods is displayed on the terminal. The user makes a request for purchase seeing the page and sends it to Web server 130. A method of the present invention can be applied to procedures used for such a system for payment.

[0119] Specifically, firstly Portable device14 authenticates a user. If authenticity is confirmed, a user ID is transmitted from Portable device 14 to Web server 130 via Mobile communication network 12 and a Communication network 10A. Upon receipt of the user ID Web server 130, instead of POS terminal 11, sends a request for transaction number including transaction information, the user ID, and merchant information. Next, payment processing is performed among Portable device 14, Payment gateway 15, and Credit server 13 similarly to the first embodiment. After completion of the payment processing, a completion message is sent from Payment gateway 15 to Web server 130 via Communication network 10A.

[0120] In the first embodiment transaction information conducted by a user is stored in Transaction table 154b. Thus, it is possible that a user checks transaction information of the user with Portable device 14, personal computer, or a mobile phone with features including Web browsing. Specifically, when receiving a request for the check from a terminal via Internet, Payment gateway 15 retrieves the transaction information form table

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 928 of 1360

154b and transforms it into a HTML format for transmission to the terminal.

[0121] In the first embodiment, information necessary for payment is stored in EEPROM 230 of detachable UIM 18 to be read out by Control unit 310. However, it is possible that a memory such as an EEPROM incorporated into Portable device 14 stores such information instead of UIM 18.

[0122] Further, a module such as an IC chip having high resistance to tampering in which information for payment including a user ID and a password is stored and read out by Control unit can be used instead of UIM 18. Needless to say, such a module can be mounted detachably.

[0123] In the first embodiment, a purchaser uses Portable device capable of communicating with Payment gateway by radio via Mobile communication network 12 for electronic payment. However, a personal computer can be used as a terminal for payment in the system, for example. Specifically, such a computer is connected with Internet via a fix telephone network and has an input device, display and other devices necessary for the electronic payment.

[0124] In the first embodiment, a user ID is transmitted via Mobile terminal 17 to POS terminal 11. However, if POS terminal 11 features Bluetooth for data exchange, Portable device 14 may transmit directly to POS terminal 11. It is possible that a user ID can be transmitted from Portable device 14 to POS terminal 11 using other communication methods.

[0125] In the first embodiment, data exchange is carried out between POS terminal 11 and Payment gateway 15 via Communication network 10. It is possible that Mobile terminal 17 is connected with Communication network 10 to exchange data between POS terminal 11 and Payment gateway via Mobile terminal 17 and Communication network 10.

[0126] In the first embodiment it is possible that if a user uses two or more credit cards for the electronic transaction system a user ID or a password is assigned to the cards. In this case, before selection of credit card (step Sa1 of fig 12), a user may input the user ID and a password before Portable device 14 authenticates the user. After the authentication, credit cards corresponding to the user ID and the password are displayed. Then the user selects one among the cards.

[0127] In the first embodiment, Control unit 310 executes application programs in data exchange between POS terminal and Payment gateway 11 and authentication of a user and a device 14. It is possible that a storage medium such as a CD-ROM or a floppy disk in which such programs for the electronic payment is stored is provided to users. The programs may be provided via Internet.

(Second embodiment)

[0128] A second embodiment of the present invention will now be described referring to the drawings.

D. Configuration of the system

D-1. Overall configuration

[0129] Fig.22 shows an electronic payment system using a method for electronic paying based on the second embodiment of the present invention.

[0130] As shown, Electronic payment system 15A has a POS terminal 11A and Credit server 13A. Payment gateway 15A is connected with Terminal 11A and Credit server 13A via a dedicated line (not shown) for data exchange. Terminal 11A and Payment gateway may be connected via a public network. Payment gateway 15A is also connected to Portable device 14A.

D-2. POS terminal

[0131] POS terminal 11A has a storage unit such as a hard drive and an input device such as a keyboard, a mouse or a card reader. In addition to Display, Control unit including a CPU, ROM, RAM, and a communication interface same as POS terminal 11 of the first embodiment. Fig.23 shows an example of information stored in the storage. As shown, "issuer code" "payment method", and "merchant code" are stored correspondingly. The "issuer code" identifies an issuer (credit card company) of a credit card by which a user can pay at a shop where POS terminal 11A is installed. The "payment method" is a payment method available for a purchaser at the shop such as a lump sum, installments, or with bonus. The "merchant code" identifies a shop of a merchant.

D-3. Credit server

[0132] Credit server 13A includes a CPU, a RAM, a ROM, an input device such as keyboard or mouse, a display, a storage unit such as a hard drive, and a communication interface such as a modem.

[0133] Figs.24A through 24D shows an example of information stored in the storage unit of Credit server 13A. Fig.24A shows information relating to POS terminal 11A. Specifically, "merchant code for credit", "payment method", and "merchant code" are stored correspondingly. The "merchant code for credit" allows an issuer (credit company) to identify a merchant or a shop with which a transaction is conducted. It may be an ID number of a shop or of POS terminal 11A.

[0134] Fig.24B shows information relating to users of credit cards. Specifically, "user name", "user address", "card number", "expiration", and "credit limit" are stored corresponding.

[0135] Fig.24C shows an example of histories of transactions conducted by users. "Card number", "decryption key", "type", "date", "transaction number", "merchant number", "amount", "payment method", and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 929 of 1360

"merchandise code" are stored correspondingly. Information stored in "card number" in fig.24C is same as stored in fig.24B. In fig.24C it is permitted that a card number is stored for several times because a user may conduct transactions several time with the card.

[0136] The "decryption key" is used for decrypting an encrypted card number which is sent from Payment gateway 15A to POS terminal 11A. The "type" represents types of transactions. The "date" represents date of payment. The "transaction number" is a serial number each assigned to a transaction. The "merchant number" identifies a shop of a merchant with which a transaction is conducted. The "amount" represents a price of merchandise (possibly including tax). The "payment method" represents payment in a lump sum, or installments, for example. The "merchandise code" identifies merchandise transacted.

[0137] Fig.24D shows an example of information on transaction details conducted at each shop. Specifically, "merchant number", "type", "date", "sales", "card number", and "payment method" are stored. Information stored in "merchant number", "type", and "date" is same as stored in fig. 24C. The "sales" represents a price of merchandise, which is same as "amount" in fig.24C if tax is not included in the "amount". The "payment method" represents a payment method selected by a user.

D-4. Portable device

[0138] Portable device14A is, for example, a cellular phone capable of carrying out data communications. To be more specific, it may use (Personal Digital Cellular (PDC) of Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), General Packet Radio Service (GPRS), or any other schemes for data communication. Further, Third generation (3G) scheme such as IMT-2000 may be applied. Needless to say, PDA and other portable devices can be applied.

D-5. Payment gateway

[0139] Payment gateway 15A includes a CPU, a RAM, a ROM, an input device such as a keyboard or a mouse, a display, a storage unit such as a hard drive, and a communication interface such as a modem. Functionally, Payment gateway 15A comprises a receiving unit 101, a checking unit 102, encryption unit 103, a number transmitting unit 104, a key generation unit 105, a key transmitting unit 106, a transmitting/receiving unit 107, a notifying unit 108, and a storage unit 109.

[0140] Transaction unit 101 receives a user ID to identify a user assigned to the user in advance and a merchant code to identify a shop, which is sent from POS terminal 11A where the user conducts a transaction. Upon receipt of a user ID and a merchant code, Receiving unit 101 transfers the user ID and the merchant code to Checking unit 102 and Transmitting/receiving unit 107.

[0141] Checking unit 102 retrieves a card number of a user from Storage unit 109 on the basis of a user ID received by Receiving unit 101. Specifically, Checking unit 102 retrieves a from Storage unit 109 a card number and an issuer code corresponding to a user ID received by Receiving unit 101. Checking unit 102 outputs the card number, the issuer code, and the merchant code to Encryption unit 103. If the user ID is not found or the expiration date has passed, Checking unit 102 outputs to Notifying unit 108 a message notifying failure of authentication.

[0142] Figs.25A and 25B show an example of information stored in Storage unit 109. As shown in Fig.25A information relating to shops which participate in the electronic payment service provided by Payment gateway 15A is stored. To be more specific, a merchant codes and corresponding shop name.

[0143] Fig.25B shows an example of information relating to users. Specifically, user IDs and corresponding passwords, user names, phone numbers, e-mail addresses, terminal numbers, card numbers, issuer codes, and expirations are stored correspondingly. The password is used for authentication of a user.

[0144] The phone number is a telephone number of portable device 14A. The e-mail address is an e-mail address for Portable device 14A. The device number is, for example, a serial number assigned for each Mobile station 14A which identifies Mobile station 14A. The card number is a number of a credit card by which a user pays. A user registers the card number to Payment gateway 15A in advance. The issuer code identifies an issuer of a card (credit company). The expiration represents an expiration date of the credit card.

[0145] Encryption unit 103 encrypts a card number obtained by Checking unit 102, to generate a "encrypted card number". Specifically, Checking unit 103 encrypts a card number, in a way that it can be decrypted using an encryption key generated by Key generating unit 105. Suppose that the decryption key is "0123" that the card number is "3456", and that the encryption calculation is an addition, the encrypted card number becomes "3579". In decryption, "0123" is subtracted from "3579" to be generated the card number "3456". Encryption unit 103 outputs to Key generating unit 105 a card number, its encrypted card number, and an issuer code. Further, Encryption unit 103 outputs to Number transmitting unit 104 the encrypted card number and the merchant code.

[0146] Number transmitting unit 104 transmits an encrypted card number made by Encryption unit 103 to POS terminal 11A specified by the merchant code obtained from Encryption unit 103.

[0147] Key generating unit 105 generates a decryption key used for decryption of a card number. In this embodiment, a card number is encrypted by Encryption unit 103 using a decryption key. It is possible that the decryption key is generated using both the decryption key and the card number. Key generating unit 105 outputs to Key transmitting unit 106 the encrypted card number, the decryption key, and the issuer code.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 930 of 1360

[0148] Key transmitting unit 106 transmits to Credit server 13A an encrypted key generated by Key generating unit 105. Specifically, Key transmitting unit 106 transmits, to Credit server by a credit company specified by the issuer code provided form Key generating unit 105 the encrypted card number and the decryption key.

[0149] When Receiving unit 101 receives a user ID, Transmitting/receiving unit 107 transmits to portable device 14A a confirmation e-mail including transaction details. If Portable device 14A does not reply to the e-mail, Transmitting/receiving unit 107 stops at least one of Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, and Key transmitting unit 106 to cancel the transaction conducted on the basis of the user ID.

[0150] To be more specific, Transmitting/receiving unit 107 retrieves from Storage unit 109 an e-mail address on the basis of the user ID provided from Receiving unit 101. Transmitting/receiving unit 107 then transmits a confirmation e-mail including transaction details to Portable device 14A specified by the e-mail address. Upon receipt of a reply e-mail from Portable device 14A, Transmitting/receiving unit 107 checks a password included in the reply e-mail against a password stored in Storage unit 109, to authenticate the user.

[0151] If Transmitting/receiving unit 107 does not receive a reply e-mail or the both passwords does not agree, Transmitting/receiving unit 107 stops at least one of Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, and Key transmitting unit 106, to cancel the transaction conducted on the basis of the user ID. A method for obtaining a confirmation from a user is not limited to the e-mail. For example, Transmitting/receiving unit 107 can transmit to Portable device14A a recection message which is generally used for cellular phone. It is possible that, in the authentication of a user, Transmitting/receiving unit 107 uses in addition to a password, information to identify Portable device 14A uniquely such as a device ID.

[0152] If Checking unit 102 does not find the credit card corresponding to the user ID in Storage unit 109, Notifying unit 108 notifies POS terminal 11A of failure of authentication.

E. Operations of the system

[0153] Detailed procedures for payment processing in an electronic financial transaction system based on the second embodiment will now be described referring to figs. 26 and 27.

[0154] As shown in fig.26, firstly, POS terminal 11A obtains a user ID from a user and transmits the user ID and a merchant code to Payment gateway 15A (step S01). Specifically, a user inputs a user ID with the input device of POS terminal, for example. POS terminal 11A may obtain the user ID from Portable device 14A. Receiving unit 101 receives the user ID and the merchant code (step S02). Next, Receiving unit 101forwards the user ID and the merchant code to Checking unit 102 and Transmitting/receiving unit 107.

[0155] Upon receipt of the user ID, Transmitting/receiving unit 107 sends a confirmation e-mail to Portable device 14A corresponding to the user ID (step S03). After the sending, Transmitting/receiving unit 107 is ready for receiving reply e-mail (step S04). If Transmitting/receiving unit 107 does not receive a reply e-mail or the both passwords does not agree, Transmitting/receiving unit 107 stops at least one of Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, and Key transmitting unit 106 to cancel the transaction conducted on the basis of the user ID (step S05).

[0156] When Transmitting/receiving unit 107 receives the reply e-mail, Checking unit 102 retrieves from Storage unit 109 a card number stored correspondingly to the user ID provided from Receiving unit 101 (step S06). It is noted that steps S03 and S04 can be omitted.

[0157] Checking unit 102 checks the card number retrieved from Storage unit 109 against the card number provided from Receiving unit 101 (step S07). If the user ID is not found in Storage unit 109 or the expiration date has passed, Checking unit 102 notifies Notifying unit 108 of failure of authentication.

[0158] Upon receipt of the message from send from Checking unit 102, Notifying unit 108 sends a message notifying POS terminal of failure of authentication (step S08). POS terminal 11A receives the message to be notified the user (step S09).

[0159] If the credit card number corresponding to the user ID is retrieved form Storage unit 109 in step S07, Checking 102 outputs the card number, the issuer code, and the merchant code to Encryption unit 103. When Encryption unit 103 receives the card number, the issuer code, and the merchant code, Key generating unit 105 generates a decryption key used for decryption of an encrypted card number (step S10). Key generating unit 105 outputs the key to Encryption unit 103 to obtain the card number and the issuer code. Next, Key generating unit 105 sends to Key transmitting unit 106 the card number and the issuer code along with the key.

[0160] Upon receipt of the decryption key from Key generating unit 105, Encryption unit 103 encrypts the card number in a way that the encrypted card number is decrypted with the decryption key (step S11). Next, Encryption unit 103 outputs the encrypted card number and the merchant code to Number transmitting unit 104.

[0161] Referring to fig.27, Number transmitting unit 104 transmits the encrypted card number to POS terminal 11A indicated by the merchant code (step S12). Key transmitting unit 106 transmits the encrypted card number and the key to Credit server 13A indicated by the issuer code (step S13). The encryption key may be generated for each user, or for each credit company. In case a common key is used as the decryption key for this system, Key transmitting unit 106 does not necessarily transmit the key to Credit server 13A more than

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 931 of 1360

twice. But needless to say, when the key is updated, Key transmitting unit 106 transmits the updated key. Upon receipt of the encrypted card number and the decryption key, Credit server 13A stores the number and the key into a storage unit of Credit server 13A (step S14).

[0162] POS terminal 11A receives and stores into a storage unit of POS terminal 11A the encrypted card number (step S15). Next, POS terminal 11A makes a request for credit to transmit to Credit server 13A (step S16). Specifically, the request includes, a type, date, transaction number, merchant code for credit, amount, payment method, merchant code as described above, in addition to the encrypted card number.

[0163] Upon receipt of the request (step S17), Credit server 13A determines whether the request is accepted referring to the encrypted card number (step S18). Specifically Credit server 13A checks the encrypted card number and the decryption key which has already been transmitted by Payment gateway 15A against the decryption key transmitted by POS terminal 11A. If both keys coincide, Credit server 13A decrypts the encrypted card number using corresponding decryption key which has already been received from Payment gateway 15A. If the encrypted card number is not found Credit server 13A sends a message notifying a failure of authentication to POS terminal 11A to be provided to the user (step S19). POS terminal 11A receives the message (step S20). If the encrypted card number is found, Credit server 13A sends an allowance message (step S21). POS terminal 11A receives the message to be provided to the user.

[0164] A payment program 92 for making a computer to function as Payment gateway 15A and a storage medium 9 will now be described referring to fig.28. Fig.28 shows a functional structure of the storage medium. Storage media 9 is, for example, a magnetic disk, an optical disk including a CR-ROM, or a semiconductor memory.

[0165] As shown in fig.9, Storage medium 9 has a program area 91 and a data area 93. Data area stores a database 931 same as Storage unit 109 shown in fig.22.

[0166] Program area 91 stores Payment program 92. Payment program 92 includes a main module 921 for controlling the following modules, a module 922 for receiving transaction information, a module 923 for checking a card number, a module 924 for encrypting a card number, a module 925 for transmitting an encrypted card number, a module 926 for generating a decryption key, a module 927 for transmitting a decryption key, a module 928 for transmitting a confirmation message and receiving a reply message, and a module 929 for notifying a message of failure of authentication. These modules 922 through 929 have same functions as the Receiving unit 101, Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, Key transmitting unit 106, Transmitting/receiving unit 107, Notifying unit 108, respectively.

[0167] In the second embodiment, since the encrypted card number is transmitted from Payment gateway to POS terminal 11A and the encrypted card number is generated by Payment gateway 15A on the basis of a user ID transmitted from POS terminal, a merchant cannot obtain a card number. Therefore, security of transaction is ensured in this system. In other words, a user is able to send a card number safely to Payment gateway 15A to conduct a transaction. Payment gateway transmits a decryption key to Credit server 13A, thus Credit server 13A obtains a decryption key corresponding to the encrypted card number. Therefore, Credit server 13A is able to determine whether a request for credit should be accepted using an encrypted card number and corresponding decryption key. Furthermore, an encrypted card number is generated each time a transaction is conducted, thus a merchant can manage sales at the shop, not knowing a card number.

[0168] In this embodiment, when Payment gateway 15A does not receive a reply mail from Portable device 14A, payment processing related to the user ID is stopped. Therefore, if an authorized person obtains a user ID improperly, the person cannot conduct any transactions using the user ID.

[0169] If Payment gateway 102 cannot find a card number corresponding to a user ID, Payment gateway 102 transmits a message notifying failure of authentication to POS terminal 11A, thus a merchant and a user can recognize that the card is not available for the transaction.

Claims

1. An electronic payment method comprising the steps of:

   authenticating a user of a user terminal on the basis of user identification information inputted to said user terminal by said user, by said user terminal;

   storing an authentication result of said user, by said user terminal, when said user terminal confirms authenticity of said user;

   transmitting a user identification information stored beforehand in said user terminal to a merchant terminal when said user terminal confirms authenticity of said user, by said user terminal;

   transmitting to payment device via a first communication network said user identification information and transaction information transmitted from said user terminal, by said merchant terminal;

   receiving said user identification information and said transaction information transmitted from said merchant terminal, by said payment device;

   identifying said user terminal on the basis of

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 932 of 1360

said user identification information and transmitting commands for instructing transmission of said authentication result to said user terminal via a second communication network;
transmitting authenticity of said user to said payment device via said second communication network if said user terminal stores authenticity of said user, by said user terminal; and
performing payment processing on the basis of said transaction information upon receipt of said authenticity from said user terminal, by said payment device.

2. The method of claim 1, further comprising the steps of:

transmitting said transaction information to said user terminal via said second communication network upon receipt of said authenticity of said user from said user terminal, by said payment device;
receiving said transaction information transmitted from said payment device and notifying said user of said transaction information, to be checked by said user, by said user terminal; and
when said user inputs an instruction for proceeding payment processing to said user terminal, transmitting to said payment device a request for proceeding payment processing; and
wherein upon receipt of said request, said payment device performs payment processing on the basis of said transaction information.

3. The method of claim 1, wherein said user terminal transmits to said payment device terminal identification information for identifying said user terminal along with said authentication result;
said payment device authenticates said user terminal referring to said terminal identification information; and
when authenticity of said user terminal is confirmed, said payment device performs payment processing on the basis of said transaction information.

4. The method of claim 1, wherein said second communication network is a mobile communication network and said user terminal is a mobile station.

5. The method of claim 1, wherein upon receipt of said authenticity from said user terminal, said payment device retrieves a card number and an expiration date on the basis of said user identification information and sends a request for credit including the card number and the expiration date to a credit server provided by a credit company.

6. An electronic payment method comprising the steps of:

authenticating a user of a user terminal on the basis of user identification information inputted to said user terminal by said user, by said user terminal;
transmitting user identification information for identifying a user to a merchant terminal, by said user terminal, when said user terminal confirms authenticity of said user;
transmitting to a payment device via a first communication network said user identification information transmitted from said user terminal, by said merchant terminal;
receiving said user identification information from said merchant terminal, by said payment device;
identifying said user terminal referring to received user identification information and transmitting commands for executing an application for payment stored in said user terminal to identified user terminal via a second communication network, by said payment device;
upon receipt of said commands, executing said application to transmit a request for proceeding payment processing to said payment device via said second communication network, by said user; and
upon receipt of said request from said user terminal, performing a payment processing.

7. An electronic payment system having a payment device, a merchant terminal connected with said payment device via a first communication network, and a user terminal connected with said payment device via a second communication network **characterized in that**:

said user terminal authenticates a user of said user terminal on the basis of user identification information inputted to said user terminal by said user; if authenticity of said user is confirmed, stores authentication result; and transmits to said merchant terminal user identification information stored in said user terminal;
said merchant terminal transmits to said payment device via said first communication network said user identification information transmitted from said user terminal and transaction information
said payment device identifies said user terminal on the basis of said user identification information transmitted from said merchant terminal and
transmits to said identified user terminal via said second communication network commands for instructing transmission of said au-

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 933 of 1360

thentication result;
said user terminal transmits to said payment device via said second communication network according to said commands transmitted from said payment device when said user terminal stores said authentication result; and
upon receipt of said authentication result from said user terminal, said payment device performs payment processing on the basis of said transaction information.

8. The system of claim 7, wherein after reception of said authentication result from said user terminal, said payment device transmits said transaction information to said user terminal via said second communication network;
said user terminal receives said transaction information form said payment device;
notifies said user of said transaction information to be checked by said user; and
if said user inputs to said user terminal an instruction of proceeding a payment processing, transmits a request for proceeding payment processing to said payment device via said first communication network; and
upon receipt of said request, said payment device performs payment processing.

9. The system of claim 8, wherein said user terminal transmits to said payment device terminal identification information for identifying said user terminal stored in said user terminal along with said authentication result; and
said payment device authenticates said user terminal on the basis of said terminal identification information;
if authenticity of said user terminal is confirmed, performs payment processing on the basis of said transaction information.

10. The system of claim 7, wherein a detachable storage medium for storing said user identification information is mounted to said user terminal; and
when said user terminal confirms authenticity of said user on the basis of said user identification information, said user terminal transmits to said merchant terminal said user identification information stored in said storage medium.

11. The system of claim 7, wherein said second communication network is a mobile communication network and said user terminal is a mobile station.

12. The system of claim 7, wherein when receiving said authentication result from said user terminal, said payment device retrieves a card number and an expiration on the basis of said user identification information and sends a request for credit including said card number and said expiration to a credit server managed by a credit company.

13. An electronic payment system having a payment device, a merchant terminal connected with said payment device via a first communication network, and a user terminal connected with said payment device via a second communication network **characterized in that**:

said user terminal authenticates a user on the basis of said user identification information inputted to said user terminal by said user;
if authenticity of said user is confirmed, transmits to said merchant terminal a user identification information for identifying said user;
said merchant terminal transfers said user identification information to said payment device via said first communication network;
said payment device identifies said user terminal on the basis of said user identification information and transmits to said identified user terminal via said second communication network commands for executing an application for payment stored in the user terminal;
said user terminal executes said application according to said commands and transmits a request for proceeding payment processing to said payment device via said second communication network; and
said payment device performs said payment processing according to said request.

14. A user terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network, comprising:

an authenticating means for authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user;
a storing means for storing an authentication result when authenticity of said user is confirmed by said authenticating means;
a storage medium for storing said user identification information;
a first transmitting means for transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information;
a receiving means for receiving commands for instructing transmission of said authentication result which is transmitted, in response to said

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 934 of 1360

request for payment, from said payment device via said second communication network; and
a second transmitting means for transmitting, upon receipt of said commands, a request for proceeding said payment processing including said authentication result to said payment device via said second communication network.

15. The user terminal of claim 14, wherein said storage medium further stores a terminal identification information for identifying said user terminal; and
said second transmitting means transmits, along with said authentication results, said terminal identification information stored in said storage medium to said payment device via said second communication network.

16. The user terminal of claims 14 or 15, wherein said storage medium is mounted detachably to said user terminal; and
said first transmitting means transmits to said merchant terminal said user identification information stored in said storage medium, when authenticity of said user is confirmed by said authenticating means on the basis of said user identification information.

17. The user terminal of claim 14 or 15, wherein said second communication network is a mobile communication network; and
said user terminal further comprises a radio communication means for exchanging data via said mobile communication network.

18. A user terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network, comprising:

an authenticating means for authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user;
a first transmitting means for transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information
a receiving means for receiving commands for executing an application for payment which is transmitted from said payment device via said second communication network; and
a second transmitting means for executing said application for payment stored in said user terminal and transmitting, according to said application, a request for proceeding payment processing to said payment device via said second communication network.

19. A payment device comprising

a receiver for receiving a request for payment including a user identification information for identifying a user of a user terminal from a merchant terminal via a first communication network;
an identifying means for identifying said user terminal among registered user terminal on the basis of said received user identification information; a transmitter for transmitting to said identified user terminal via a second communication network commands for executing an application for payment stored in the user terminal; and
a processing means for performing a payment processing on the basis of a request sent from the user terminal via said second communication network after transmission of said commands.

20. A computer program product for making a computer incorporated into a communication terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network to execute the steps of:

authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user; storing an authentication result into a storage means when authenticity of said user is confirmed by said authenticating means;
transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information;
receiving commands for instructing transmission of said authentication result which is transmitted, in response to said request for payment, from said payment device via said second communication network; and
transmitting, upon receipt of said commands a request for proceeding said payment processing including said authentication result to said payment device via said second communication network.

21. A storage medium for storing a computer program product for making a computer incorporated into a

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 935 of 1360

communication terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network to execute the steps of:

authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user; storing an authentication result into a storage means when authenticity of said user is confirmed by said authenticating means;
transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information;
receiving commands for instructing transmission of said authentication result which is transmitted, in response to said request for payment, from said payment device via said second communication network; and
transmitting, upon receipt of said commands, a request for proceeding said payment processing including said authentication result to said payment device via said second communication network.

22. A payment device comprising:

a storage unit for storing a user identification information for identifying a user of a user terminal and a card number of a credit card correspondingly; a receiving unit for receiving from a merchant terminal a user identification information;
a retrieving unit for retrieving from said storage unit a card number corresponding to said identified user;
an encrypting unit for encrypting the retrieved card number;
a generating unit for generating a key for decryption of said encrypted card number;
a first transmitting unit for transmitting to said merchant terminal said encrypted card number; and
a second transmitting unit for transmitting said key to a credit server managed by an issuer of the credit card.

23. The payment device of claim 22 further comprising a confirming means for transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information.

24. The payment device of claim 22 or 23, further comprising a notifying means for transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit.

25. An electronic payment method comprising the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal, by a receiving unit;
retrieving from a storage unit a card number corresponding to said identified user by a retrieving unit;
encrypting the retrieved card number, by an encrypting unit;
generating a key for decryption of said encrypted card number, by a generating unit;
transmitting to said merchant terminal said encrypted card number, by a first transmitting unit; and
transmitting said key to a credit server managed by an issuer of the credit card, by a second transmitting unit.

26. The electronic payment method of claim 25, further comprising the step of transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information, by a confirming means.

27. The electronic payment method of claim 25 or 26, further comprising the step of transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit, by a notifying means.

28. A computer program product for making a computer to execute the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 936 of 1360

retrieving from a storage unit a card number corresponding to said identified user;
encrypting the retrieved card number;
generating a key for decryption of said encrypted card number; transmitting to said merchant terminal said encrypted card number; and
transmitting said key to a credit server managed by an issuer of the credit card.

29. The computer program product of claim 28, for making said computer to further execute the step of transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information.

30. The computer program product of claim 28 or 29, for making said computer to further execute the step of transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit

31. A computer readable storage medium for storing a computer program product for making a computer to execute the steps of:

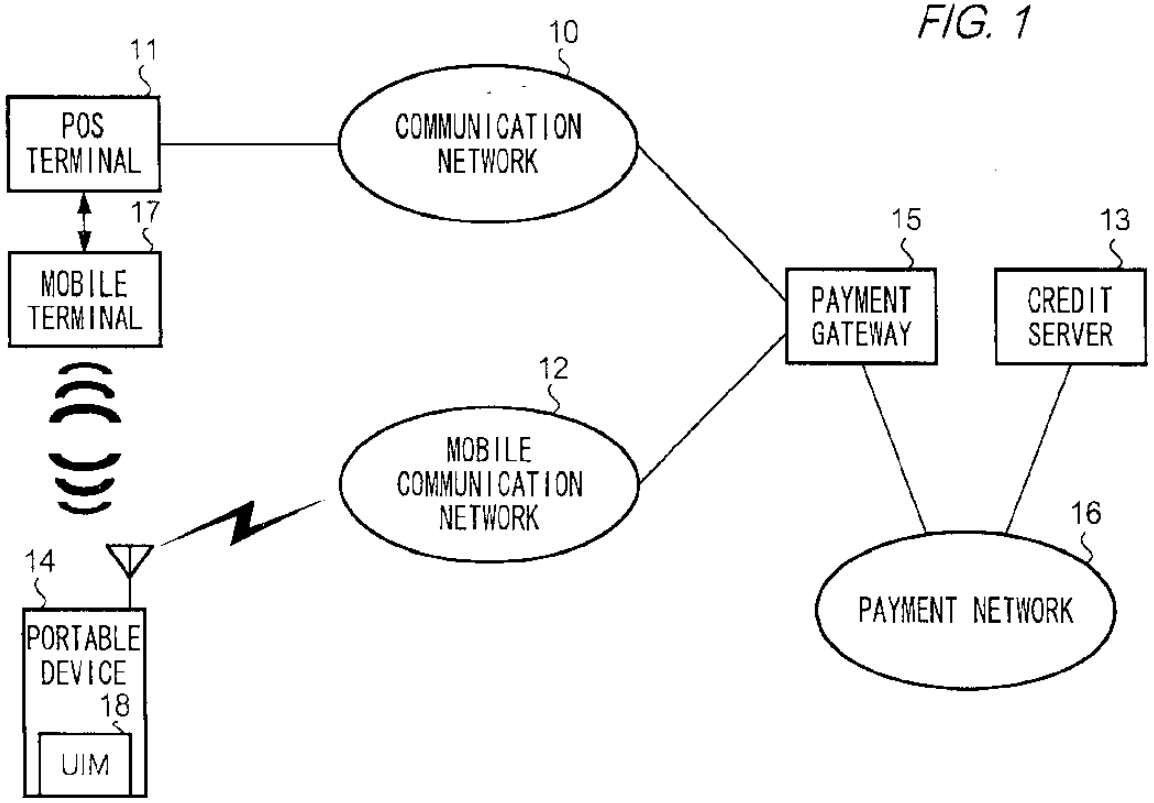
receiving from a merchant terminal a user identification information for identifying a user of a user terminal;
retrieving from a storage unit a card number corresponding to said identified user;
encrypting the retrieved card number;
generating a key for decryption of said encrypted card number; transmitting to said merchant terminal said encrypted card number; and
transmitting said key to a credit server managed by an issuer of the credit card.

32. The storage medium of claim 31, for storing a computer program product for making said computer to further execute the steps of transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information.

33. The storage medium of claim 31 or 32, for storing a computer program product for making said computer to further execute the step of transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit.

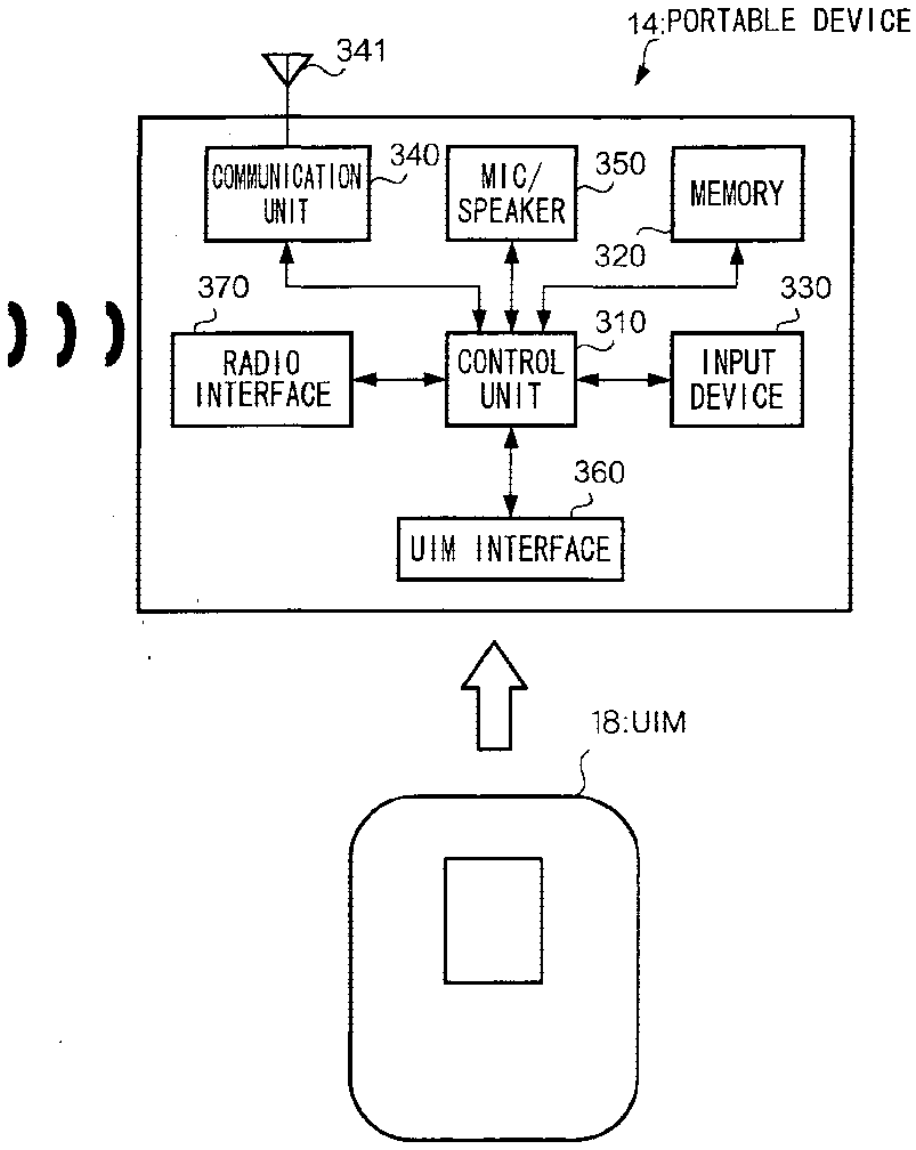
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 937 of 1360

FIG. 1



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 938 of 1360

FIG. 2



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 939 of 1360

FIG. 3

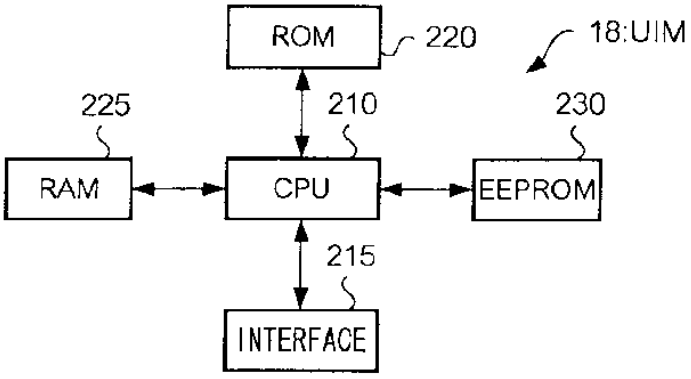
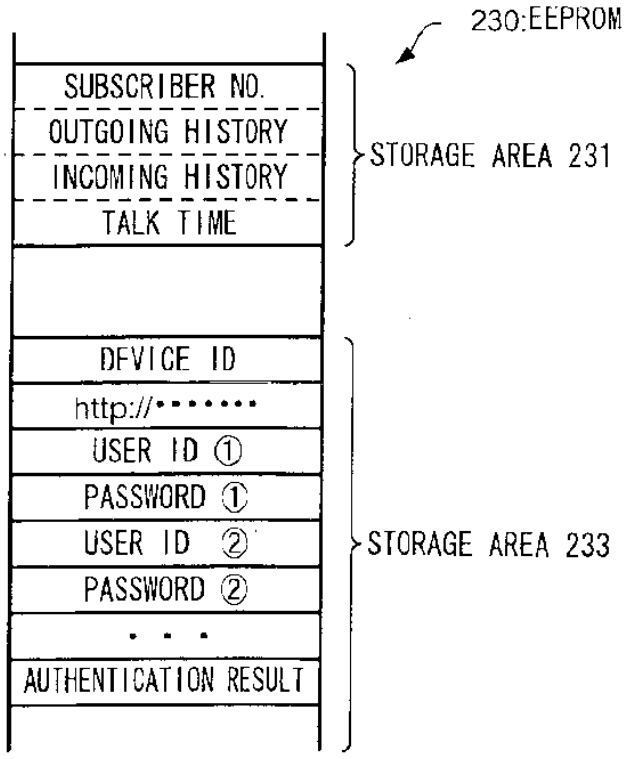
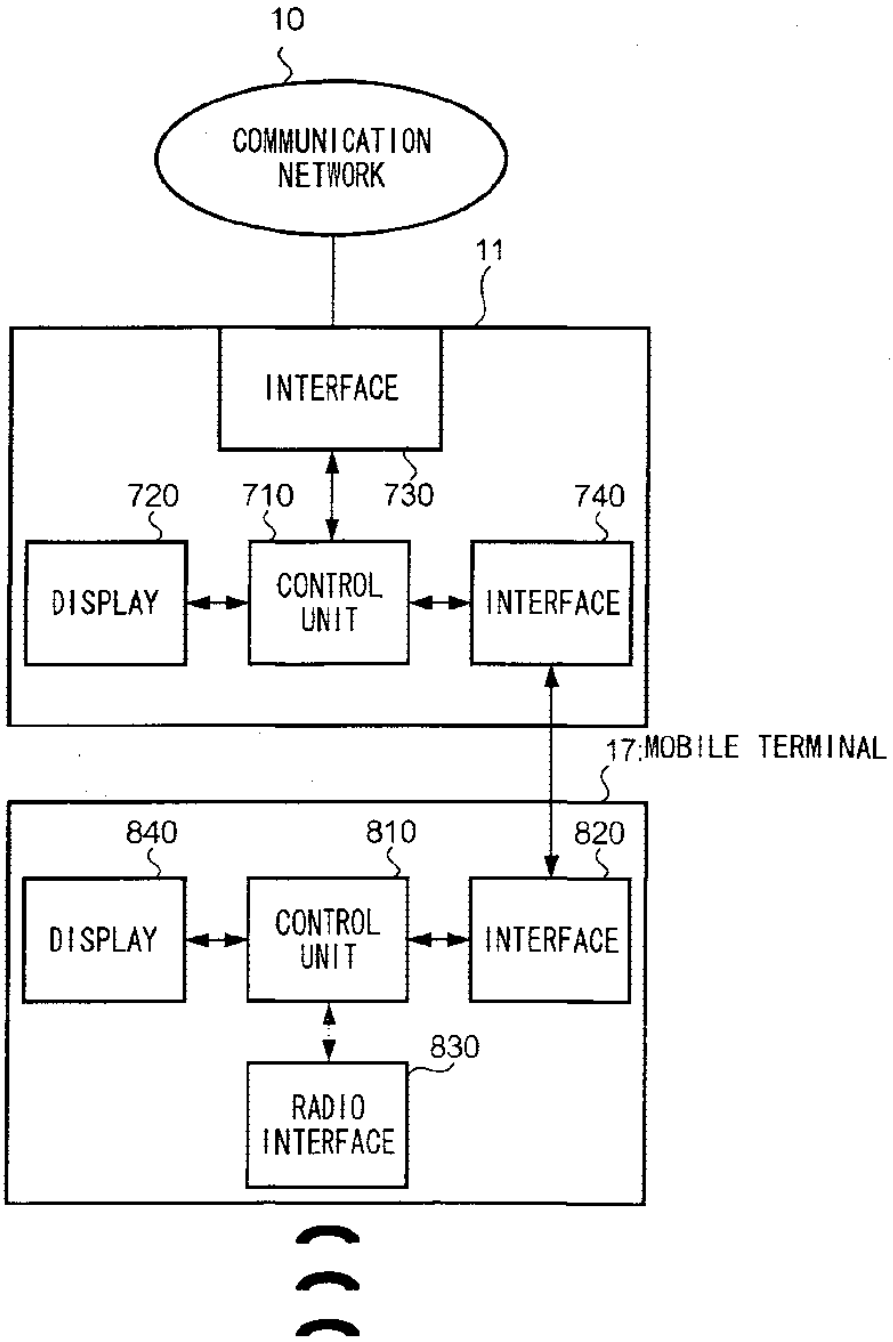


FIG. 4



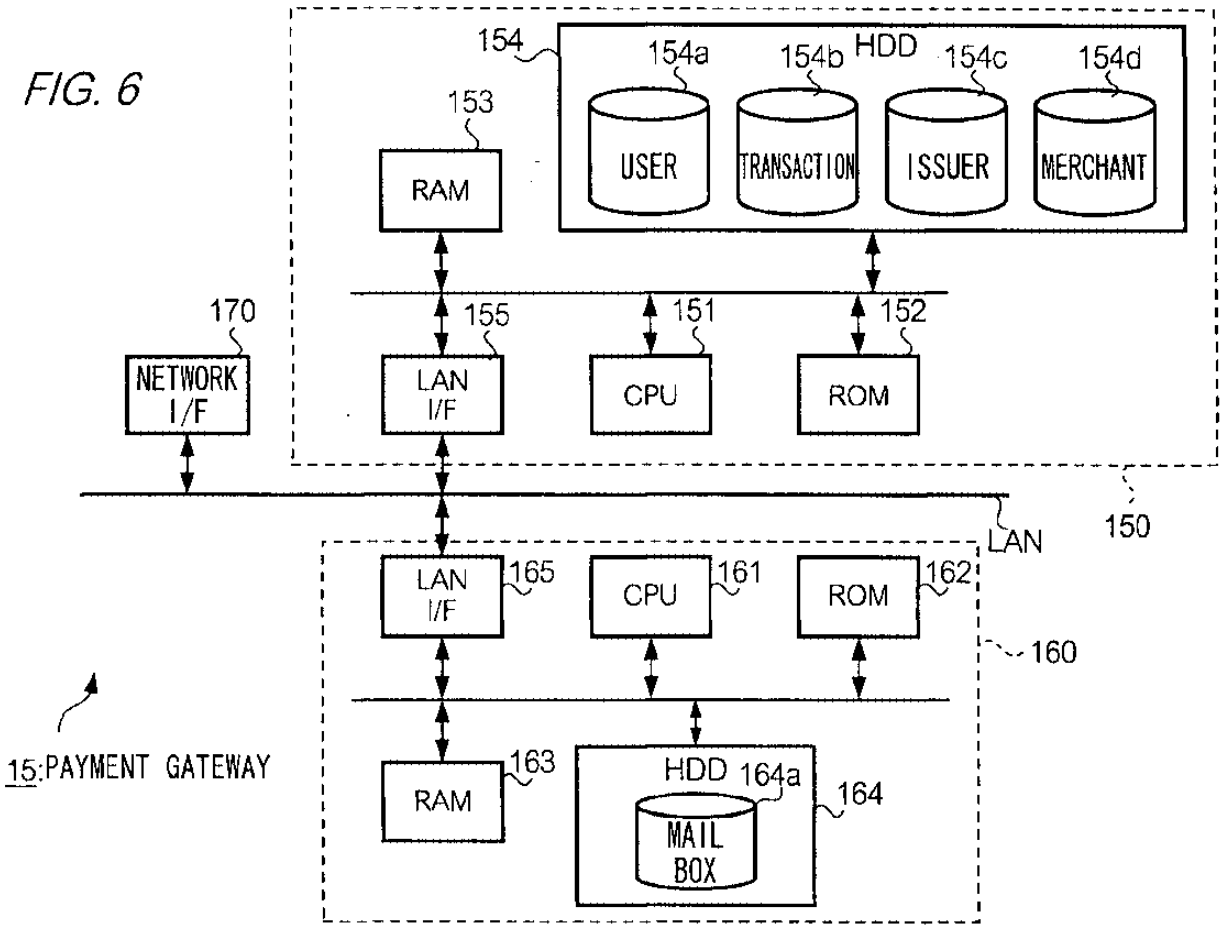
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 940 of 1360

FIG. 5



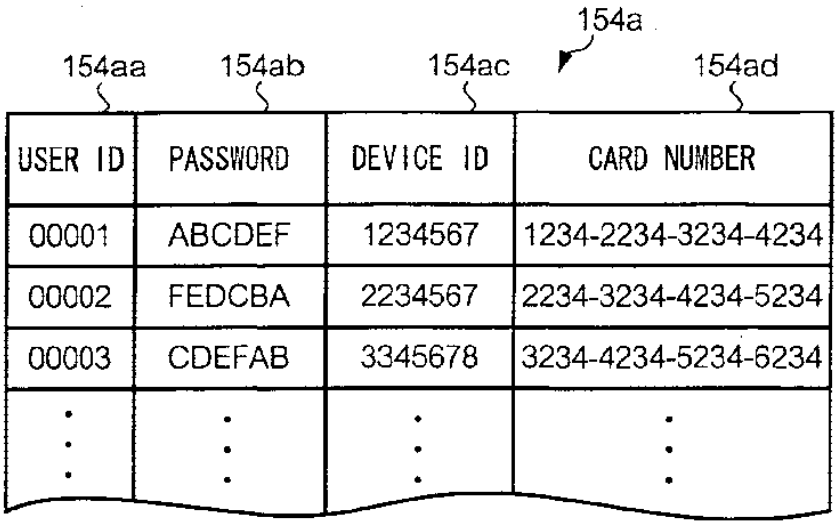
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 941 of 1360

FIG. 6



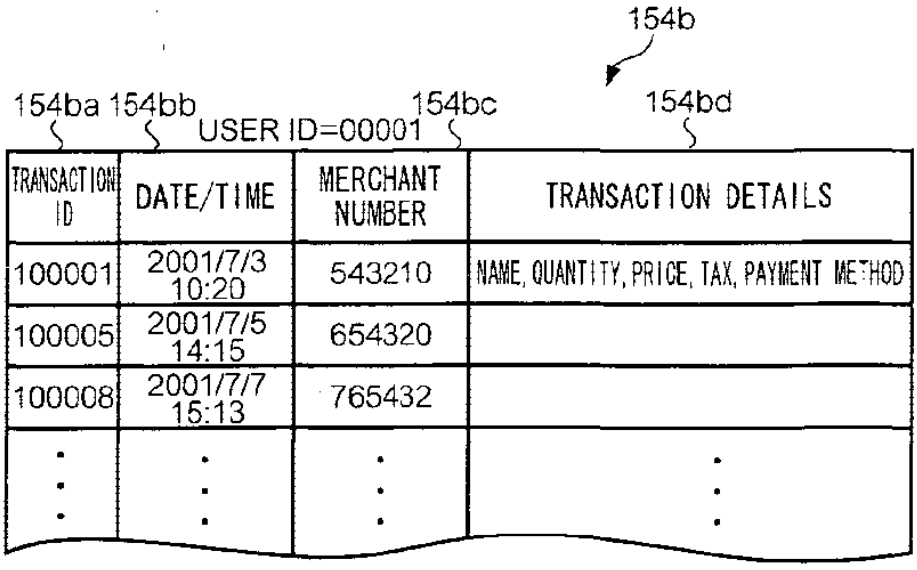
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 942 of 1360

FIG. 7



USER ID	PASSWORD	DEVICE ID	CARD NUMBER
00001	ABCDEF	1234567	1234-2234-3234-4234
00002	FEDCBA	2234567	2234-3234-4234-5234
00003	CDEFAB	3345678	3234-4234-5234-6234
⋮	⋮	⋮	⋮

FIG. 8



TRANSACTION ID	DATE/TIME	MERCHANT NUMBER	TRANSACTION DETAILS
100001	2001/7/3 10:20	543210	NAME, QUANTITY, PRICE, TAX, PAYMENT METHOD
100005	2001/7/5 14:15	654320	
100008	2001/7/7 15:13	765432	
⋮	⋮	⋮	⋮

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 943 of 1360

FIG. 9

154c

154ca 154cb 154cc

CARD NUMBER	ISSUER CODE	ISSUER NAME
1525000000～1525059999	2a11111	A
145259000～1452590000	2a22222	B
153996010～153996010	2s33333	C
13500～13560	2a11111	A
13600～13600	2s44444	D

FIG. 10

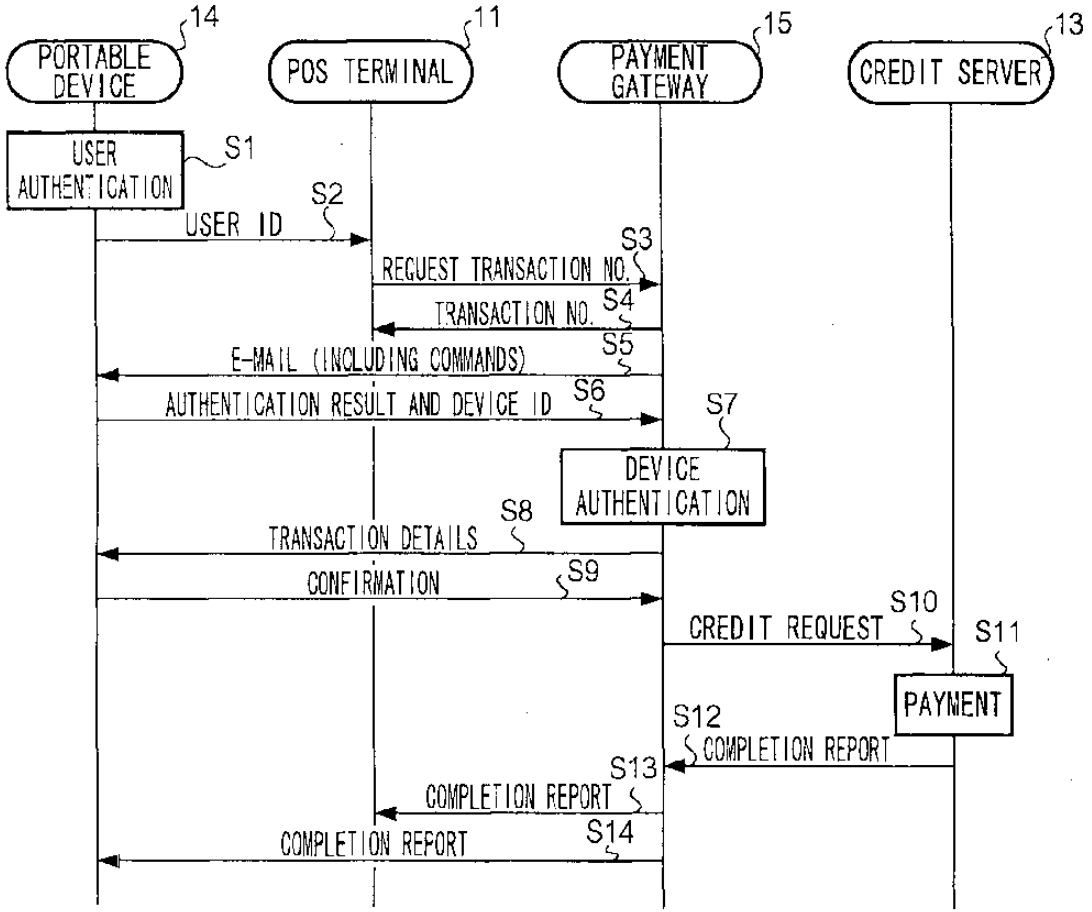
154d

154da 154db 154dc 154dd 154de

MERCHANT CODE	MERCHANT NAME	ISSUER NAME	ISSUER NAME	PAYMENT METHOD				
				L	I	B	PB	R
1111111111	A	2a11111	A	○	○	×	×	○
2222222222	B	2a22222	B	○	○	×	○	○
2222222222	B	2s44444	D	○	×	○	×	×
3333333333	C	2a22222	B	○	×	○	○	×
4444444444	D	2s33333	C	○	×	×	×	○

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 944 of 1360

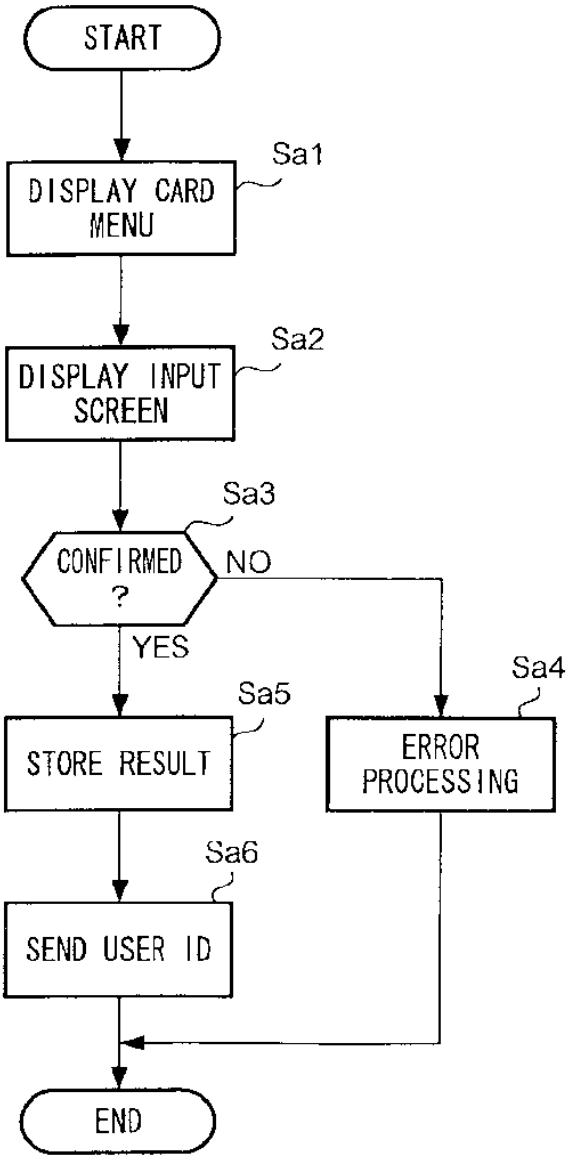
FIG. 11



EP 1 280 115 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 945 of 1360

FIG. 12



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 946 of 1360

FIG. 13

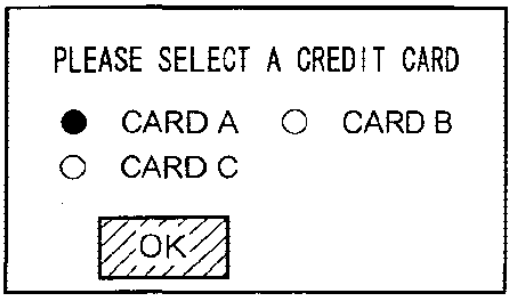
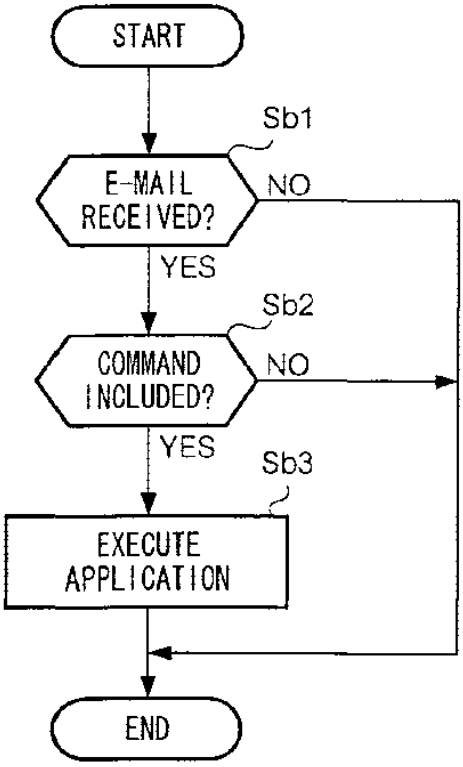
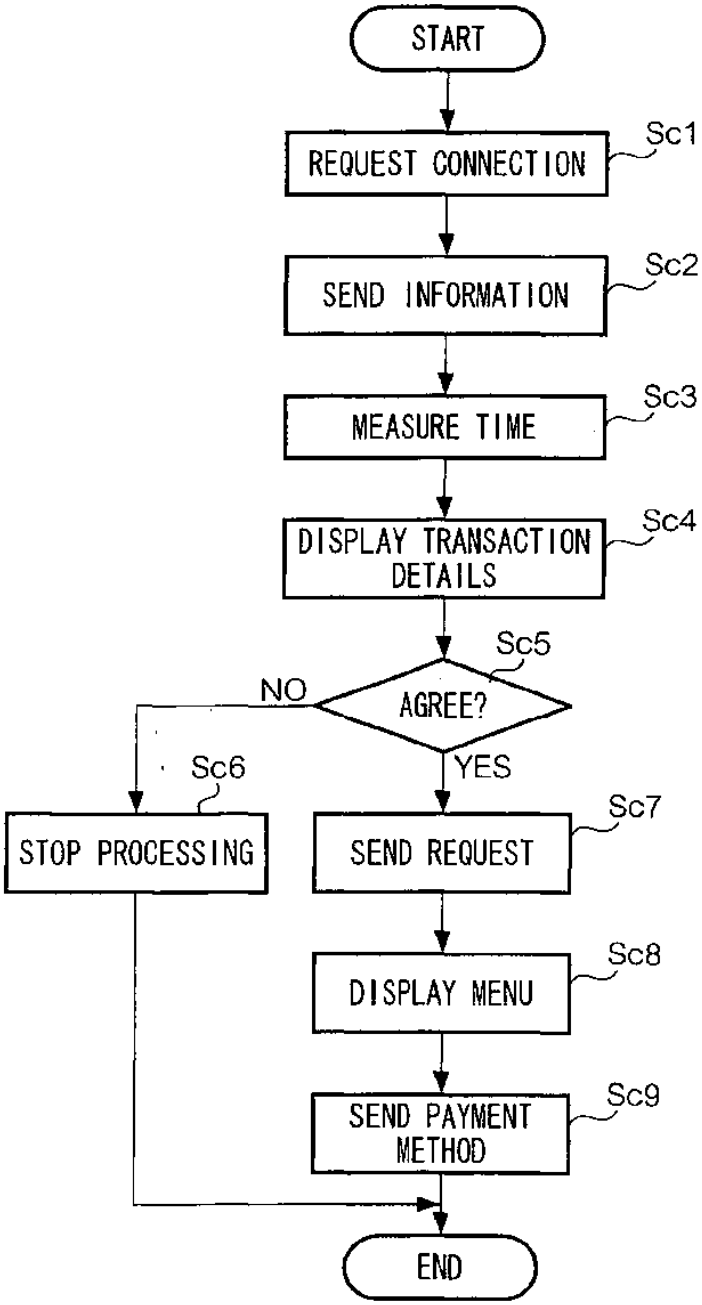


FIG. 14



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 947 of 1360

FIG. 15



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 948 of 1360

FIG. 16

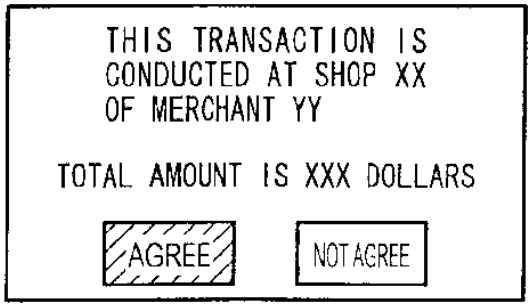
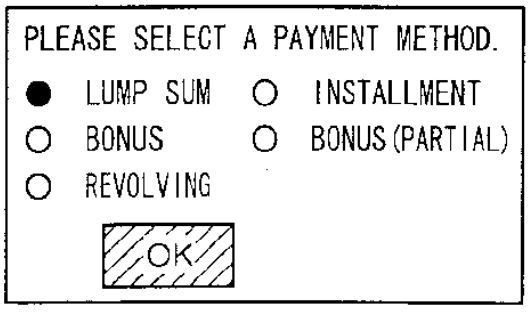
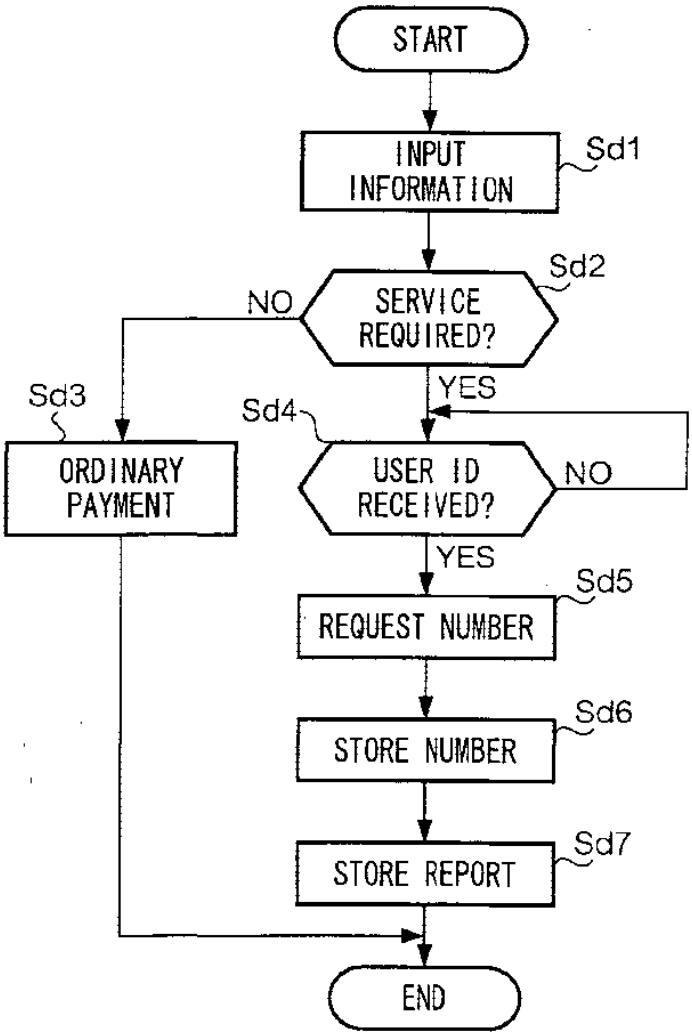


FIG. 17



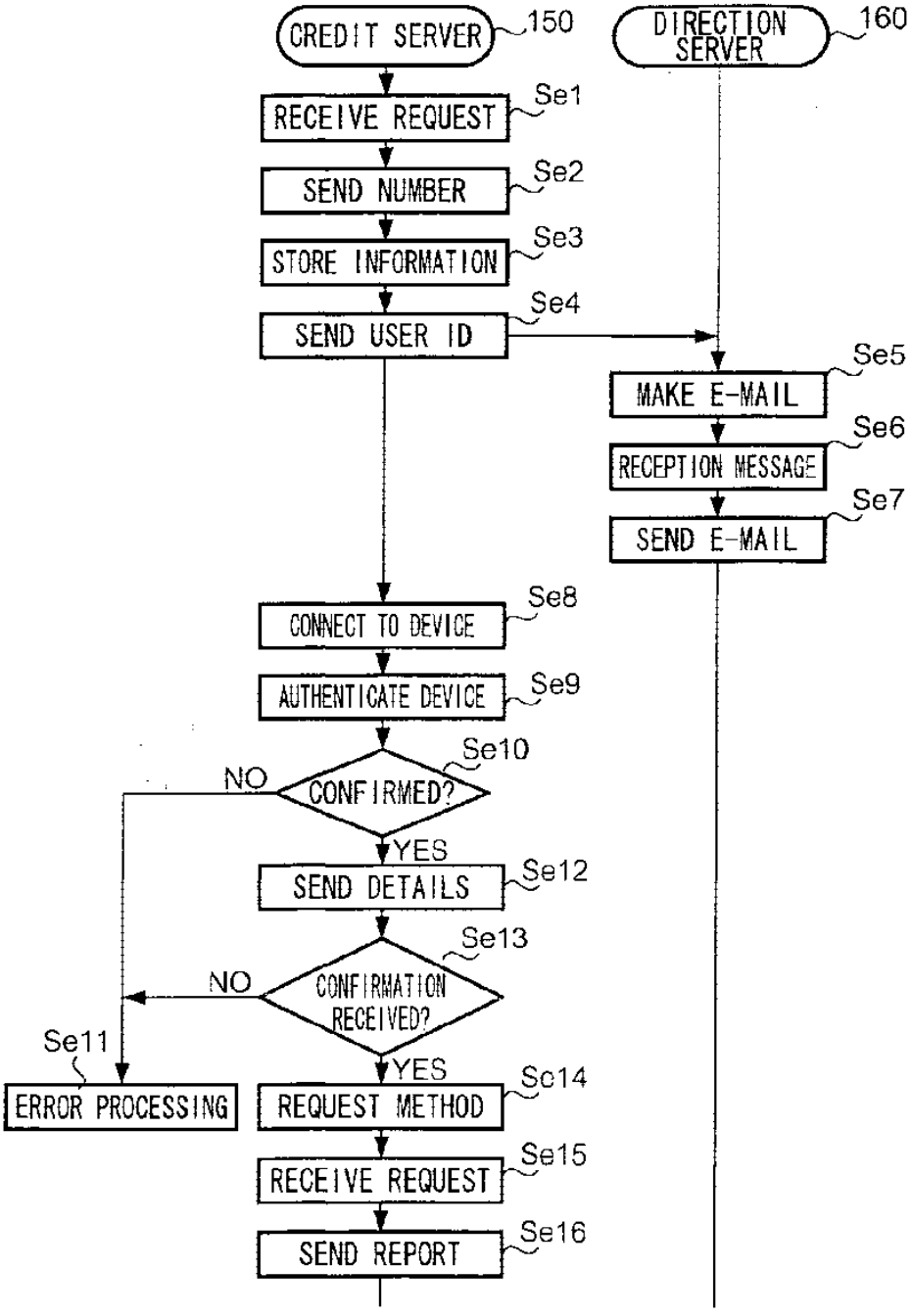
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 949 of 1360

FIG. 18



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 950 of 1360

FIG. 19



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 951 of 1360

FIG. 20

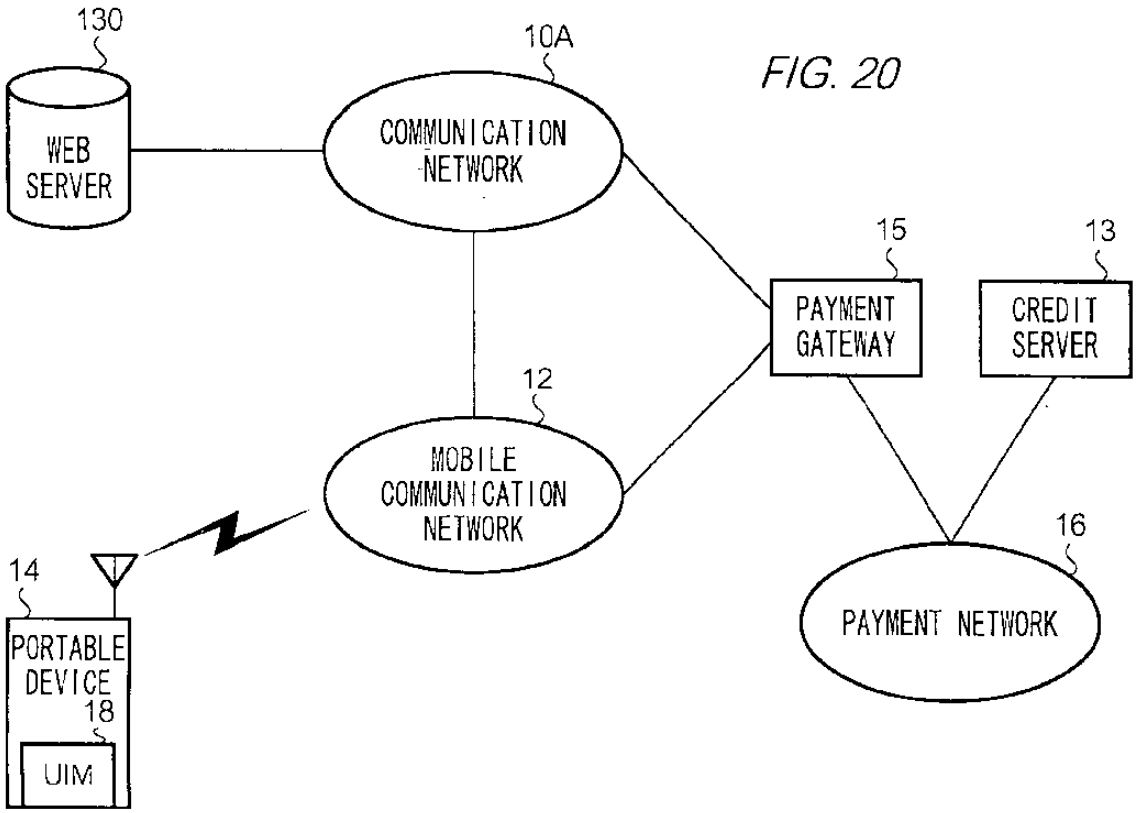
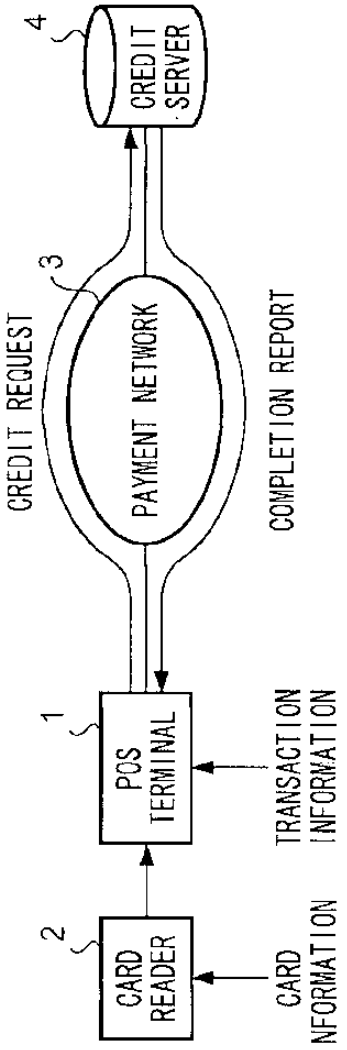
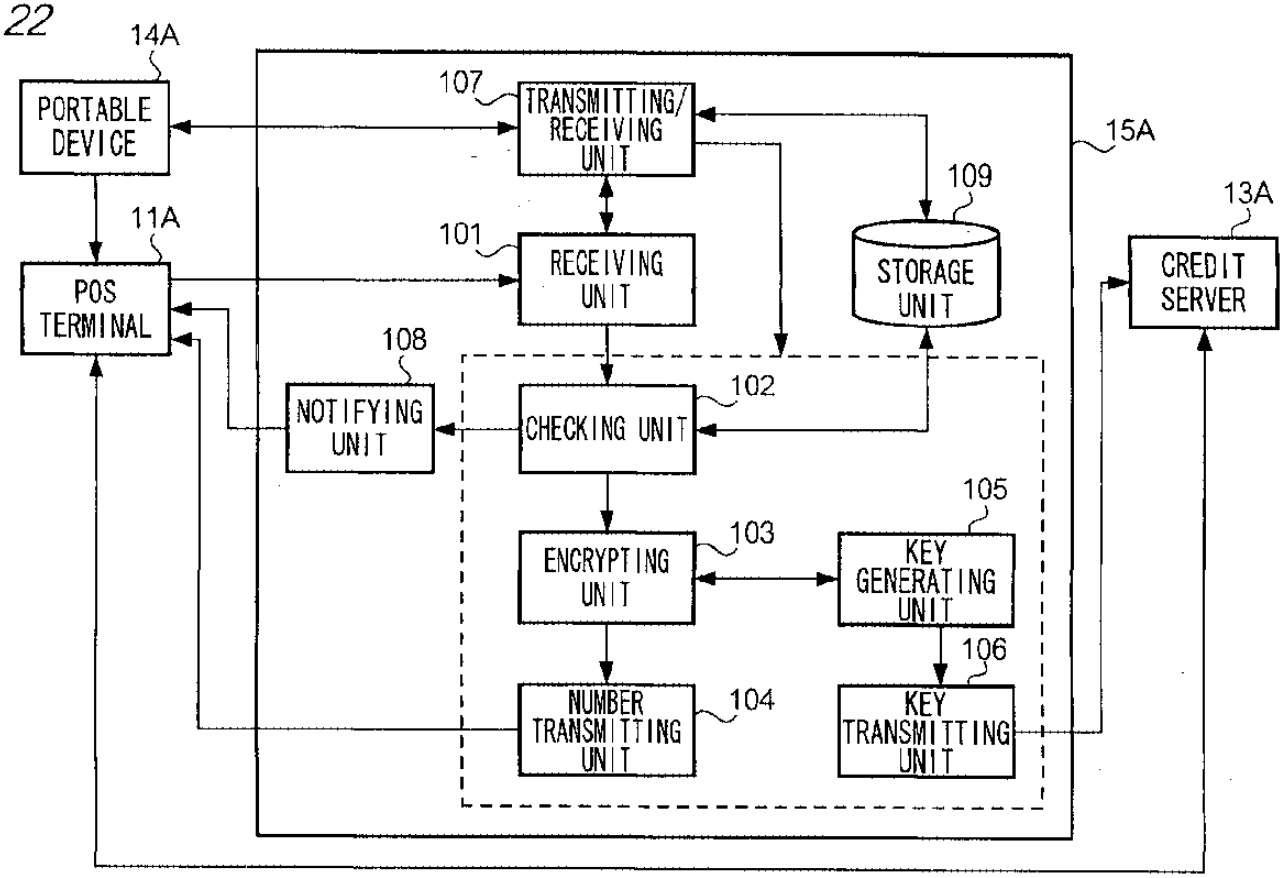

130
WEB SERVER
10A
COMMUNICATION NETWORK
15
PAYMENT GATEWAY
13
CREDIT SERVER
12
MOBILE COMMUNICATION NETWORK
16
PAYMENT NETWORK
14
PORTABLE DEVICE
18
UIM

FIG. 21



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 953 of 1360

FIG. 22



EP 1 280 115 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 954 of 1360

FIG. 23

ISSUER CODE	PAYMENT METHOD	MERCHANT CODE
.....	.....	.....
.....	.....	.....
.....	.....	.....
⋮	⋮	⋮

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 955 of 1360

FIG. 24A

MERCHANT CODE FOR CREDIT	PAYMENT METHOD	MERCHANT CODE
• • • •	• • • •	• • • •
• • • •	• • • •	• • • •
• • • •	• • • •	• • • •
⋮	⋮	⋮

FIG. 24B

USER NAME	ADDRESS	CARD NUMBER	EXPIRATION	LIMIT
• • • •	• • • •	• • • •	• • • •	• • • •
• • • •	• • • •	• • • •	• • • •	• • • •
• • • •	• • • •	• • • •	• • • •	• • • •
⋮	⋮	⋮	⋮	⋮

FIG. 24C

CARD NUMBER	KEY	TYPE	DATE	SERIAL NO.	MERCHANT NUMBER	AMOUNT NO.	PAYMENT METHOD	MERCHANDISE CODE
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

FIG. 24D

MERCHANT NUMBER	TYPE	DATE	SALES	CARD NUMBER	PAYMENT METHOD
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
	• • • •	• • • •	• • • •	• • • •	• • • •
	• • • •	• • • •	• • • •	• • • •	• • • •
⋮	⋮	⋮	⋮	⋮	⋮

EP 1 280 115 A2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 956 of 1360

FIG. 25A

MERCHANT CODE	MERCHANT NAME
• • • •	• • • •
• • • •	• • • •
• • • •	• • • •
⋮	⋮

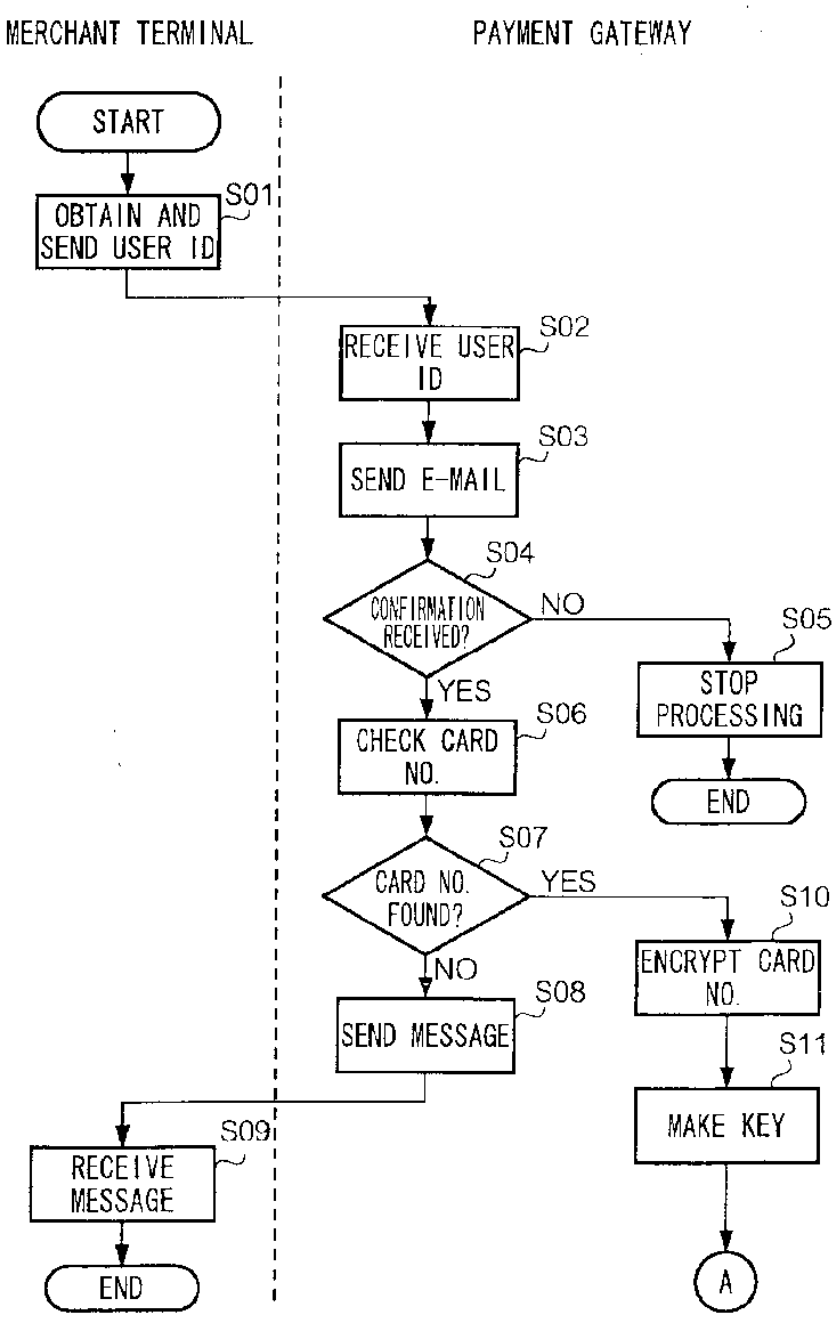
FIG. 25B

USER ID	PASSWORD	USER NAME	PHONE NUMBER	E-MAIL ADDRESS	DEVICE NO.	CARD NUMBER	ISSUER CODE	EXPIRATION
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

EP 1 280 115 A2

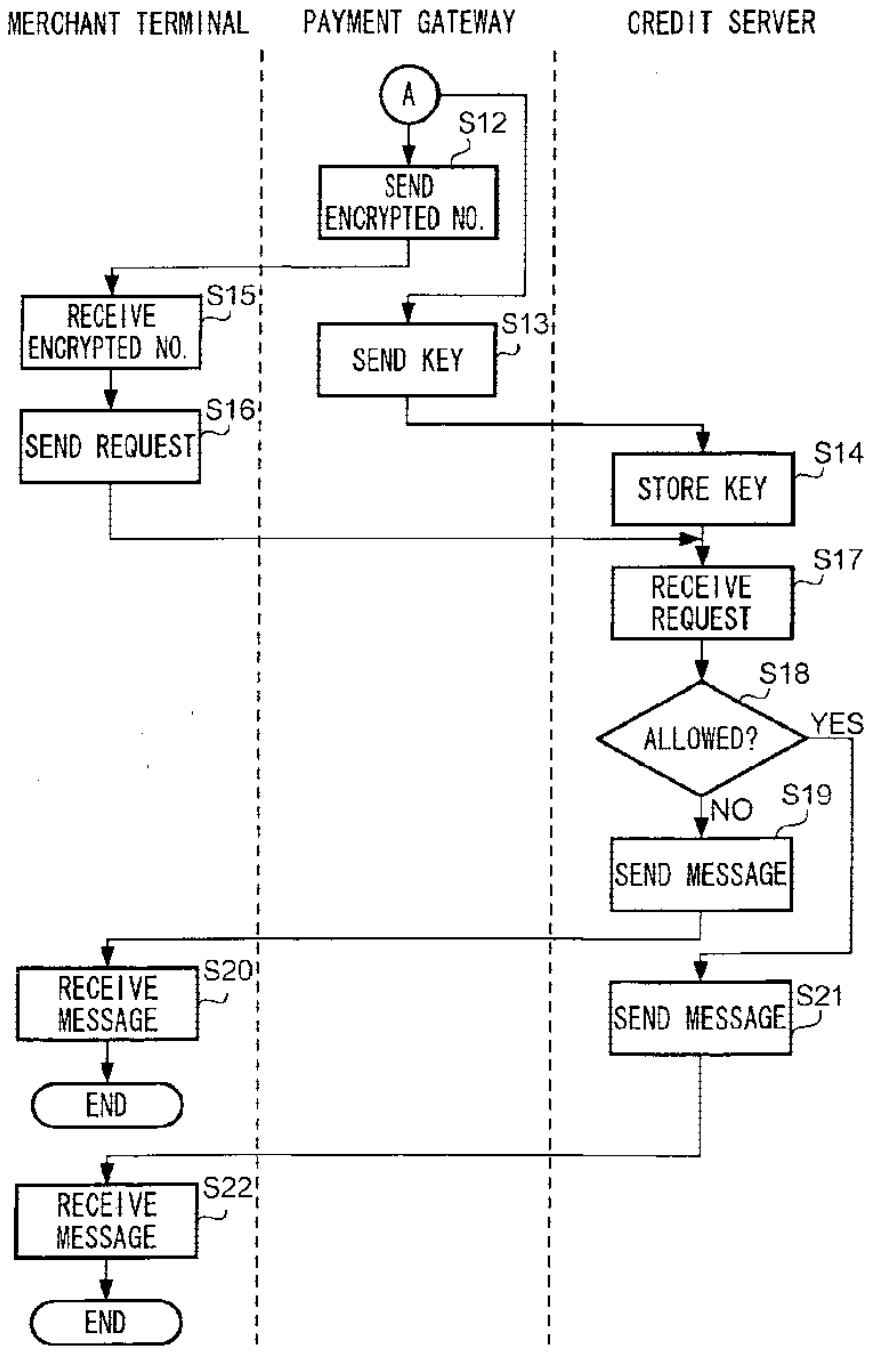
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 957 of 1360

FIG. 26



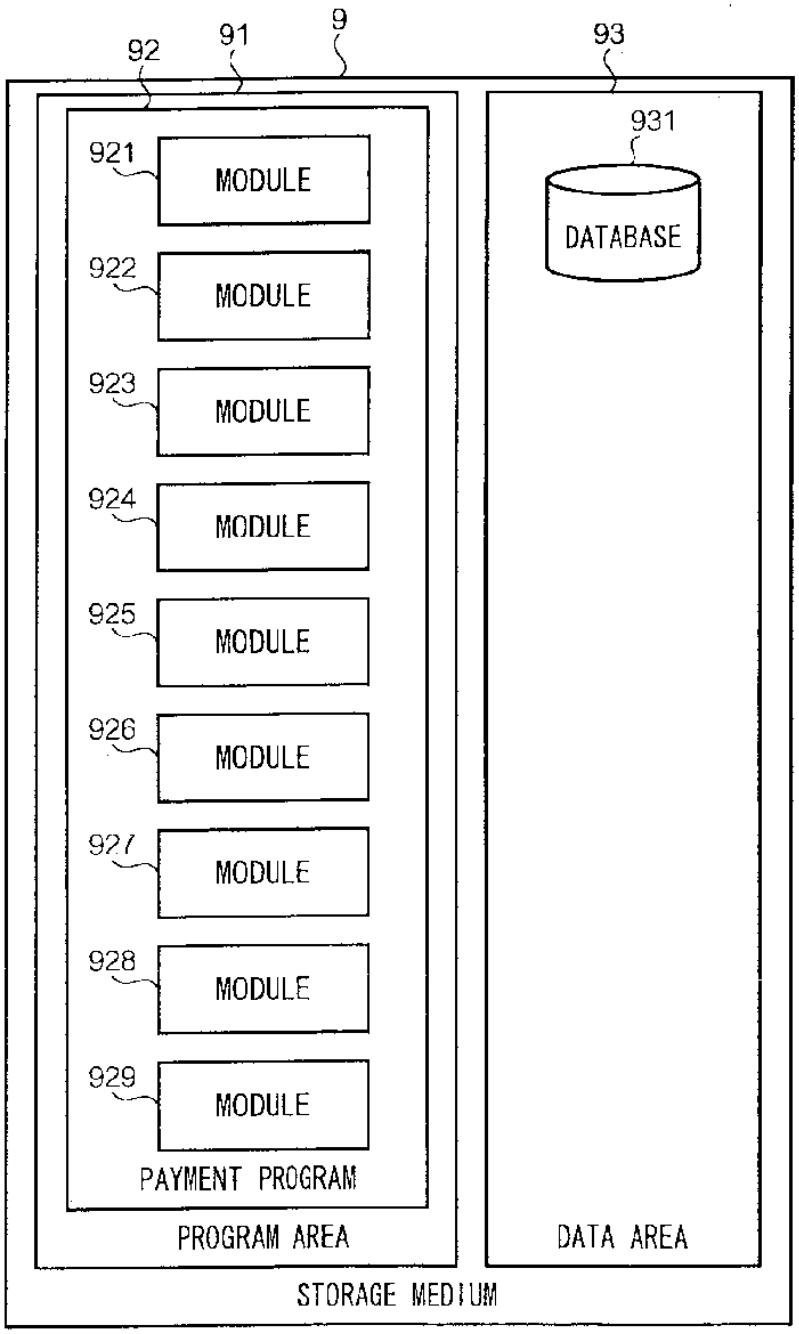
PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 958 of 1360

FIG. 27



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 959 of 1360

FIG. 28



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 960 of 1360

(19) **KOREAN INTELLECTUAL PROPERTY OFFICE**

KOREAN PATENT ABSTRACTS

(11)Publication number: **1020070092400 A**

(21)Application number: **1020060022464**
(22)Date of filing: **10.03.2006**
(30)Priority: ..
(51)Int. Cl **G06Q 20/00**

(71)Applicant: **SHIN HAN BANK**
(72)Inventor: **JUNG, JONG PIL**
KIM, KI JUNG

(54) **SYSTEM AND A METHOD FOR PROVIDING A CONVENIENT/SAFE ONE-STOP NON-FACIAL CHANNEL PAYMENT SERVICE BY USING A NICKNAME**

(57) Abstract:

PURPOSE: A system and a method for processing payment by using a nickname are provided to offer an one-stop non-facial channel payment service for online non-facial channel payment by replacing a payment account number for a non-facial channel with the nickname. CONSTITUTION: An information inputting part(115) receives nickname information set to a virtual account connected to a real account of a customer. An information storing part(120) stores the nickname to a storage medium(130) by linking with virtual/real account and customer information. An interface provider(110) transmits a payment form or window to a customer terminal when the customer performs the payment in the online network. A payment processor receives mobile number/nickname information from the customer terminal and transmits an authentication code to the mobile terminal by using the mobile number. If the authentication code is received from the customer terminal, the payment processor authenticates the customer and processes an approval for the payment by checking the virtual account.

copyright KIPO 2007

Legal Status
Date of request for an examination (20060310)
Notification date of refusal decision (00000000)
Final disposal of an application (registration)
Date of final disposal of an application (20080319)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 961 of 1360

Patent registration number (1008229850000)
Date of registration (20080410)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent (00000000)
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )
Date of extinction of right ( )

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 962 of 1360

(19) **KOREAN INTELLECTUAL PROPERTY OFFICE**

KOREAN PATENT ABSTRACTS

(11)Publication number: **1020030068603 A**

(21)Application number: **1020020008052**

(22)Date of filing: **15.02.2002**

(30)Priority: ..

(51)Int. Cl **G06F 17/60**

(71)Applicant: **NARU SYSTEM CO., LTD.**

(72)Inventor: **KIM, GYEONG SIK**

(54) **SYSTEM AND METHOD FOR SETTLING CHARGE USING CELLULAR PHONE**

(57) Abstract:

PURPOSE: A system and a method for settling charge using a cellular phone are provided to realize a micro remittance function and an accumulation function as well as a micro payment function by using the cellular phone of the wireless communication without the wired Internet environment. CONSTITUTION: A user section(52) is a buyer checking processor generated when a buyer starts transaction. An input server(54) stores a transaction request as a queue format. A customer information confirmation part(56) verifies a cellular phone number of the buyer and a seller by linking with a mobile communication companys data part(58). A mobile account(62) is a virtual account linked with a real account of a bank or a credit card company(64). A limit/remainder confirmation part (60) decides the transaction by checking the remainder or a credit limit of the mobile account(62). A certification number generating part(66) generates a number for the identification and the approval of the transaction. A transaction particulars server(68) changes the virtual account of the buyer and the seller after confirming the transaction particulars and the certification number from the buyer.

copyright KIPO 2003

Legal Status

Date of request for an examination (20020219)

Notification date of refusal decision (00000000)

Final disposal of an application (rejection)

Date of final disposal of an application (20040213)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 963 of 1360

Patent registration number ( )
Date of registration (00000000)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent (00000000)
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )
Date of extinction of right ( )

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 964 of 1360

(19) **KOREAN INTELLECTUAL PROPERTY OFFICE**

KOREAN PATENT ABSTRACTS

(11)Publication number: **1020020065989 A**

(21)Application number: **1020010006133**

(22)Date of filing: **08.02.2001**

(30)Priority: ..

(51)Int. Cl **G06F 17/60**

(71)Applicant: **STARBRIDGE COMMUNICATIONS CO., LTD.**

(72)Inventor: **CHOI, JONG HO**

(54) **PAYMENT METHOD USING PAYMENT CODE ON MOBILE TERMINAL**

(57) Abstract:

PURPOSE: A payment method is provided to make a payment on a mobile terminal by using an identifiable payment code downloaded at a mobile terminal via an online network or an offline media or given at every transaction. CONSTITUTION: The method comprises steps of a user requesting a payment on a mobile phone(S101), a mobile payment management company setting a monthly payment limit to the user by considering a vocation, an age or an income, and transmitting a payment code to the user(S102), the user downloading the payment code at the mobile phone(S103), in a case of buying a commodity or using a service by using a mobile payment, the user inputting a secret code at the mobile terminal for receiving a user approval(S104), the mobile phone displaying the payment code on a display(S105), a payment code reader, installed at an affiliated store, reading the payment code displayed on the mobile phone(S106), the payment code reader allowing an operator to input a transaction money or an installment month as well as the payment code, and transmitting a transaction approval request to the mobile payment management company(S107), the company transmitting a transaction approval code and specification to the reader and the mobile phone after checking if the requested transaction is normal(S110), and a mobile communication company calculating a total payment amount and sending a bill to the user(S111).

copyright KIPO 2003

Legal Status

Date of request for an examination (20010208)

Notification date of refusal decision ( )

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 965 of 1360

Final disposal of an application (rejection)
Date of final disposal of an application (20031209)
Patent registration number ( )
Date of registration ( )
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent ( )
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )
Date of extinction of right ( )

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 966 of 1360

Espacenet
Patent search
Deutsch English Français
Contact
Change country

About Espacenet Other EPO online services
Search | My patents list (0) | Query history | Settings | Help

DE10119808 (A1)

DE10119808 (A1)
Bibliographic data
Description
Claims
Mosaics
Original document
Cited documents
Citing documents
INPADOC legal status
INPADOC patent family

Quick help
- What does A1, A2, A3 and B stand for after a publication number?
- What happens if I click on "In my patents list"?
- What happens if I click on the "Register" button?
- Why are some similar options deactivated for certain documents?
- How can I bookmark this page?
- Why does a list of documents with the heading "Also published as" sometimes appear, and what are these documents?
- What is a cited document?
- What are citing documents?
- What information will I find if I click on the link "View all"?
- Why do I sometimes find the abstract of a corresponding document?
- What happens if I click on the button "Translate this text?"

Bibliographic data: DE10119808 (A1) — 2002-09-12

In my patents list | EP Register | Report data error | Print

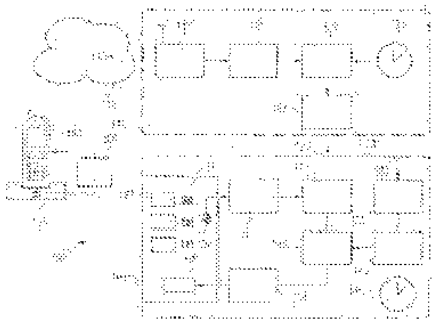
Transaction method for providing goods or services involves vending machine comparing transaction codes transmitted to it and to customer from terminal at chargeable connection

Page bookmark	DE10119808 (A1) - Transaction method for providing goods or services involves vending machine comparing transaction codes transmitted to it and to customer from terminal at chargeable connection
Inventor(s):	HOLLAND CHRIS [DE] ↑
Applicant(s):	HOLLAND CHRIS [DE] ↑
Classification:	- **international:** G06Q20/00; G07F5/18; (IPC1-7): G06F17/60
	- **European:** G06Q20/04; G06Q20/32; G07F5/18
Application number:	DE20011019808 20010423
Priority number(s):	DE20011019808 20010423, DE20011009821 20010301

Abstract of DE10119808 (A1)

Translate this text into

The method involves making a connection between a calling customer terminal or payment point and a called terminal or payment point at a chargeable connection, sending object and vending machine identification data to the called terminal, generating a transaction code and sending to the customer terminal and vending machine, storing a reference code in the vending machine, entering the code to the vending machine, comparing codes and dispensing. The method involves making a connection between a calling customer terminal or payment point and a called terminal or payment point at a chargeable connection, sending goods or service object identification data and vending machine identification data to the called terminal, generating a transaction code and sending to the customer terminal and to the vending machine, storing the transmitted or generated transaction code as a reference code in the vending machine, the customer entering the code to the vending machine, comparing codes and dispensing the goods or service. Independent claims are also included for (1) a transaction method for providing functionality (2) an arrangement for providing goods or services; and (3) an arrangement for providing functionality.



Sitemap Accessibility Legal notice Terms of use Last updated: 26.02.2012 Worldwide Database 5.7.28; 93p

IP.com Sign In | Register
Search | Publish | Resources | Research and Analytics | Blog | About Us | Contact Us

Electronic settlement system (05-Apr-2002)

Japanese Application Publication (Source: PAJ)
Publication No. JP 2002-99716 A *published on* 05-Apr-2002
Application No. JP 2000-289921 *filed on* 25-Sep-2000

Abstract (English)

PROBLEM TO BE SOLVED: To provide an electronic settlement system capable of preventing a user's privacy from being leaked to outside by preventing a payment code from being used illegally by another person.

SOLUTION: A user connects his/her portable telephone set with a settlement center and inputs the user's ID, password, etc., to request issuing of the payment code. When they are coincident with a user's ID and a password registered in advance, the settlement center issues the payment code. The user notes the payment code. The settlement center gives the information of confirmation to the portable telephone set. The payment code is validated by the user's answering to the information of confirmation. After then, the user does shopping at a store and presents the payment code to the store when paying for it. The store reports the payment code, a charging amount, etc., to the settlement center and after confirmation, the store regard the confirmation as the finish of payment and delivers merchandise. Hereafter, the payment code is invalidated and becomes unusable.

COPYRIGHT: (C)2002,JPO

RECRUIT AGENT
ｗｅｂ・インターネット業界の転職に強い。
エンジニア・プログラマー・デザイナー
IT転職エキスパートと一緒にあなたのキャリアを！
CLICK!

There's no image data available for this publication

Options
More Like This
Download PDF

Inventors
KUNINOBU MASANAO

Applicants
KUNINOBU MASANAO

Classifications
International: **G06F 17/60**

Supplemental Information (Source: DOCDB)

Inventors
KUNINOBU MASANAO

Applicants
KUNINOBU MASANAO

Priority
JP 2000-289921 A 25-Sep-2000

Classifications
International (2006.01): **G06Q 50/00**; G06Q 20/00; G06Q 40/00
International: G06F 17/60

Terms of Use | Privacy Policy | Contact us
Copyright © 2001-2012 IP.com. All Rights Reserved.

Espacenet

Bibliographic data: JP2001357164 (A) — 2001-12-26

METHOD AND CENTER FOR FUND MANAGEMENT

Inventor(s): SAKAMOTO HIROAKI; TAKAHASHI YOSHIO; TABUCHI EIJI; OGURO HIROAKI; HANIYUDA HIRONORI; HASEGAWA TAKESHI; IIJIMA MIKIMASA; SUDO MASANORI ± (SAKAMOTO HIROAKI, ; TAKAHASHI YOSHIO, ; TABUCHI EIJI, ; OGURO HIROAKI, ; HANIYUDA HIRONORI, ; HASEGAWA TAKESHI, ; IIJIMA MIKIMASA, ; SUDO MASANORI)

Applicant(s): NTT DATA CORP ± (NTT DATA CORP)

Classification: - **international:** ***G06Q50/00; G07C13/00;*** (IPC1-7): G06F17/60; G07C13/00

- **Euro:**

Application number: JP20000178134 20000614

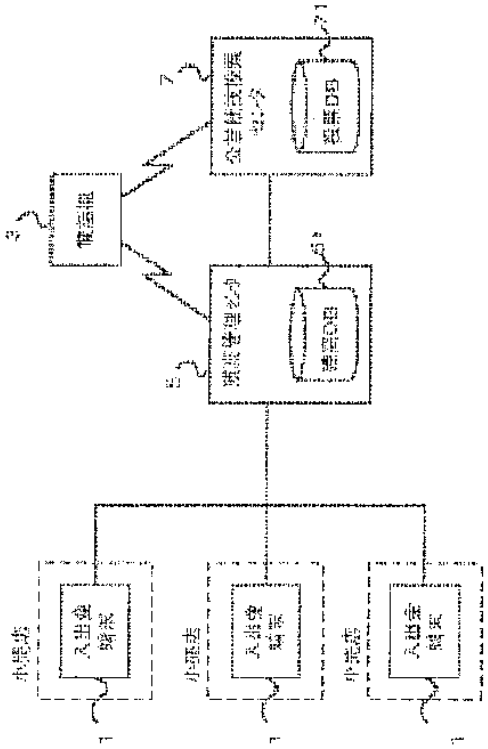
Priority number(s): JP20000178134 20000614

Abstract of JP2001357164 (A)

PROBLEM TO BE SOLVED: To provide a method and a center for fund management which is convenient for a betting system. SOLUTION: A balance management center 5 having a balance database 51 which stores balance data consisting of a telephone number for authentication, the balance, and a password code for each user adds a paid-back amount to the balance of the balance data of a winner according to winning data received from a municipally operated race betting center 7 and pays winning money back. Further, the balance management center 5 answers a payment request from a telephone set 3, specifies balance data corresponding to a specified telephone number for authentication in the balance database 51, and updates the balance according to an withdrawal amount and supplies a withdrawal reception number to the user after authenticating the user. The balance management center 5, after verifying the withdrawal reception number on a reception number verification request from a money paying and receiving terminal 1, allows money to be paid. In response, the store where the money paying and receiving terminal 1 is installed supplies the cash corresponding to the withdrawal amount to the user.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 969 of 1360

Last updated: 24.09.2012 Worldwide
Database 5.7.44.7.93p



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 970 of 1360

Espacenet

Bibliographic data: CN101606400 (A) — 2009-12-16

An interactive system and process

Inventor(s): ANH NGO DUC [AU] ± (NGO DUC ANH)

Applicant(s): DELOITTE SERVICES PTY LTD [AU] ± (DELOITTE SERVICES PTY LTD)

Classification: - international: ***H04W4/14; H04W4/18; H04W8/24***
- Euro: G06F8/65; H04M3/42E5; H04W8/24N

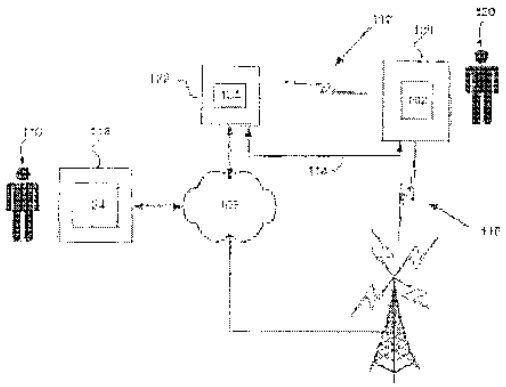
Application number: CN20078038721 20071019

Priority number (s): AU20060905829 20061019

Also published as: WO2008046161 (A1) US2010197326 (A1) EP2084921 (A1) CA2666616 (A1) AU2007312879 (A1) more

Abstract of CN101606400 (A)

A method of delivering an instruction (206) to a mobile user device (106) connected to a network (110) is disclosed. The method comprising the steps of receiving an interactive workflow (202), translating the interactive workflow into the instruction (206) in a form executable by the mobile user device (106), and sending a message (208) including the instruction (206) to the mobile user device (106).



PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 971 of 1360

(11) Application No. **AU 2007312879 A1**

(19) AUSTRALIAN PATENT OFFICE

(54) Title
An interactive system and process

(51)[6] International Patent Classification(s)
H04M 3/493 (2006.01) 4BHAU H04W 4/14 20090101ALI2009052
H04W 4/14 (2009.01) 9BHAU
H04M 3/493 PCT/AU2007/001599
20060101AFI2008042

(21) Application No: 2007312879 (22) Application Date: 2007.10.19

(87) WIPO No: WO08/046161

(30) Priority Data

(31) Number	(32) Date	(33) Country
2006905829	2006.10.19	AU

(43) Publication Date : 2008.04.24

(71) Applicant(s)
Fruitful Technologies Pty Ltd

(72) Inventor(s)
Ngo, Duc Anh

(74) Agent/Attorney
Blake Dawson Patent Attorneys, Level 36, Groevenor Place 225 George Street, Sydney, NSW, 2000

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 972 of 1360

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2008 (24.04.2008)

PCT

(10) International Publication Number
WO 2008/046161 A1

(51) International Patent Classification:
H04Q 7/22 (2006.01) *H04M 3/493* (2006.01)

(21) International Application Number:
PCT/AU2007/001599

(22) International Filing Date: 19 October 2007 (19.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2006905829 19 October 2006 (19.10.2006) AU

(71) Applicant *(for all designated States except US)*: **DELOITTE SERVICES PTY LTD** [AU/AU]; Level 1, 225 George Street, Sydney, NSW 2000 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **NGO, Duc, Anh** [/AU]; 2/9 Fabian Court, Maribyrnong, VIC 3032 (AU).

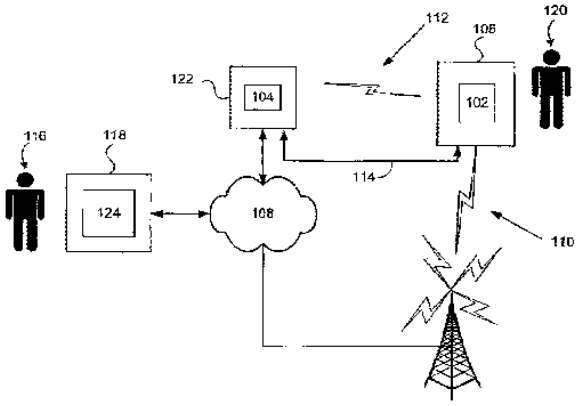
(74) Agent: **BLAKE DAWSON WALDRON PATENT SERVICES**; Level 35, Grosvenor Place, 225 George Street, Sydney, NSW 2000 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) Title: AN INTERACTIVE SYSTEM AND PROCESS



(57) Abstract: A method of delivering an instruction (206) to a mobile user device (106) connected to a network (110) is disclosed. The method comprising the steps of receiving an interactive workflow (202), translating the interactive workflow into the instruction (206) in a form executable by the mobile user device (106), and sending a message (208) including the instruction (206) to the mobile user device (106).

WO 2008/046161 A1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 973 of 1360

AN INTERACTIVE SYSTEM AND PROCESS

FIELD OF THE INVENTION

The present invention relates generally to a method of delivering an instruction to a mobile user device connected to a network.

BACKGROUND

Amongst the wide variety of portable electronic devices available today, mobile phones have become particularly pervasive, with more than double the penetration of the Internet. These devices have rapidly advanced in capability and can do far more than Voice and SMS. Using these capabilities to deliver and execute applications that provide customisable interactivity to mobile phones and other devices is highly desirable but continues to be a challenging endeavour due the varied types of largely incompatible devices and platforms on the market.

Most interactive applications for mobile phones involve either Short Message Service (SMS) or the development of dedicated applications that address specific business requirements. SMS interactivity suffers from poor usability (the user has to be familiar with idiosyncratic commands) and security issues (SMS source addresses can be faked), thus limiting their usage to simple, non-sensitive transactions. Furthermore, an organisation wishing to use SMS to interact with its customers needs to come to some commercial arrangement with the telecommunications provider in order to establish billing procedures and so on. This can be inconvenient for the organisation, and may also be quite expensive, both to set up and also to operate on an on-going basis.

The dedicated applications are an attempt to address these shortcomings by developing programming code that is executed by the mobile device to perform a specific task. This involves significant amounts of time, at least because mobile phones from different manufacturers are not usually binary compatible and cannot execute the same executable applications. Additionally, these applications are limited to the functionality required at the time of development, and thus may not support additions or modifications to that functionality. As can be appreciated, distributing changes to these applications is similarly quite a tedious process, typically requiring the user to manually download and install an updated version of the application on their telephone.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 974 of 1360

SUMMARY OF THE INVENTION

According to one aspect of the invention there is provided a method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

According to another aspect of the invention there is provided a method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

According to yet another aspect of the invention there is provided computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

Preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language. More preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

Preferably the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device. More preferably the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 975 of 1360

step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

Preferably the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

Preferably the step of translating the interactive workflow includes tailoring the instruction to the specification.

Preferably the step of translating the interactive workflow includes tailoring the instruction to a device operating system.

Preferably the step of sending the message includes the step of sending a unique message identifier. More preferably the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

Preferably the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network. More preferably the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS. Alternatively, the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

Preferably the method further comprises the step of the mobile user device receiving the set of instructions and the unique message identifier. More preferably the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

Preferably the method further comprises the step of receiving a response to the instruction from the mobile user device. More preferably the step of receiving a response includes the step of receiving a response identifier from the device. Even more preferably the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 976 of 1360

Preferably the method includes the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow from the external or third party. More preferably the method includes the step of sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow from the external or third party.

Preferably the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface from the external or third party. More preferably the step of receiving a request for an Application Programming Interface is received from the external or third party. Even more preferably the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

Preferably the method also comprises the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

In accordance with the present invention, there is also provided an interactive process executed by a computer system or device, the process including:

receiving one or more SMS messages including instruction data representing one or more instructions for execution on said system or device to determine information;

executing said one or more instructions to determine said information; and

sending one or more SMS messages including response data representing said information.

Advantageously, said information may include system information determined from said system or device and/or user information determined from a user of said system or device.

Preferably, said execution causes generation of an interactive user interface on a display of said system or device, and the process includes receiving response data representing said information from a user of said system or device in response to said interactive display.

Preferably, said one or more instructions are executed by a virtual machine of said system or device.

The present invention also provides an application component for a system or device, the applicationcomponent including:

a message receiver for processing one or more received SMS messages to generate one or more instructions for execution on said device to determine information;

an execution component for executing said one or more instructions of said application data to determine said information; and

a message sender for generating one or more SMS messages including response data representing said information.

Preferably, the application component further includes a data management component for storing sets of instructions on non-volatile storage means and for retrieving a selected one of the stored sets of instructions for execution.

Preferably, said execution component is adapted to generate an interactive display for a user of said system or device, and to receive response data representing said information from a user of said system or device in response to said interactive display.

The present invention also provides an interactive process for execution by a system or device, including:

receiving message data including header data and encrypted payload data;

selecting one of a plurality of encryption keys on the basis of said header data; and

decrypting said payload data using the selected encryption key.

Preferably, said header data includes index data representing an index for said plurality of encryption keys.

Advantageously, said payload data may represent one or more instructions for execution on said system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions on a remote system or device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 978 of 1360

The present invention also provides an interactive process for execution by a system or device, including:

generating payload data for sending to a remote system or device;

selecting one of a plurality of encryption keys;

encrypting said payload data using the selected encryption key;

generating message data for sending to said remote system or device, said message data including header data and the encrypted payload data, wherein said header data includes data representing an index for said plurality of encryption keys to allow said remote system or device to determine the selected encryption key and thereby to decrypt said payload data.

Advantageously, said payload data may represent one or more instructions for execution on said remote system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions.

Preferably, the process includes generating said plurality of encryption keys and sending said plurality of encryption keys to said remote system or device.

Preferably, the process includes associating said plurality of encryption keys with an identifier of said remote system or device.

The present invention also provides an interactive process, including:

receiving programming instructions for generating an interactive display on a remote system or device;

compiling said programming instructions to generate compiled instruction data;

sending said compiled instruction data to said remote system or device to generate an interactive display on said second remote system or device;

receiving response data representing at least one user response to said interactive display; and

sending response data representing said at least one user response.

The present invention also provides an interactive process, including:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 979 of 1360

receiving workflow instructions from a plurality of entities;

processing said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

sending said interactive applications to said user devices for execution.

Preferably, said interactive applications are sent to said user devices using short message service (SMS).

Preferably, said user devices include mobile telephones.

The present invention also provides an interactive system for managing interaction with users of remote systems and/or devices, the interactive system being adapted to:

receive workflow instructions from a plurality of entities;

process said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

send said interactive applications to said user devices for execution.

The present invention also provides a system having components for executing any one of the above processes.

The present invention also provides a computer-readable storage medium having stored thereon program instructions for executing any one of the above processes.

The present invention also provides an interactive system, including:

a gateway component for processing received workflow data to generate instructions for generating an interactive display on a user device, the gateway component being adapted to send said instructions to said user device for execution; and

an execution component of said user device to receive and execute said instructions to generate said interactive display, to receive response data representing at least one response of said user to said interactive display; and to send said response data to said gateway component.

Preferably, said user device is a mobile telephone.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 980 of 1360

Advantageously, the instructions may be sent to said gateway component in one or more SMS messages.

Advantageously, said user response data may be sent to said user device in one or more SMS messages.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a schematic diagram of a preferred embodiment of an interactive system;

Figure 2 is a schematic diagram of the high level process and data flow of an interactive process of the interactive system;

Figure 3 is a block diagram of a mobile telephone on which a client application of the interactive system is installed;

Figure 4 is a block diagram of the client application of the interactive system;

Figure 5 is a flow diagram of the life cycle of an interactive application generated by the interactive process and system;

Figure 6 is a block diagram of an application gateway of the interactive system;

Figure 7 is a block diagram of a computer system on which the application gateway is installed;

Figure 8 is a schematic diagram of the process and data flow of an opt-in process of the interactive system;

Figure 9 is a schematic diagram illustrating the use of encryption key sets to establish an encrypted communications channel between the client application and the application gateway;

Figure 10 is a schematic diagram of the process and data flow involved in conducting secure communications between the client application and the application gateway;

Figure 11 is a schematic diagram illustrating the default behaviour of the interactive system and process whereby a particular application gateway transmits instructions to a particular client application, and the resulting response data is returned to the same application gateway that sent the instructions;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 981 of 1360

Figure 12 is a schematic diagram similar to that of Figure 11, but illustrating the redirection of response data to a different application gateway from the application gateway that sent the corresponding instructions;

Figure 13 is a schematic diagram illustrating the structure of messages exchanged between the application gateway and the client application;

Figure 14 is a schematic diagram illustrating the structure of payload data of the messages shown in Figure 13;

Figure 15 is a schematic diagram illustrating the structure of each data part of the payload data of Figure 14;

Figure 16 is a schematic diagram illustrating the fifteen different types of instructions supported by the interactive system and process;

Figure 17 is a schematic diagram illustrating the structure of an SMS message generated by the interactive system and process;

Figure 18 is a schematic diagram illustrating how the interactive system uses multiple SMS messages to transmit instructions constituting an application whose length is greater than 133 bytes;

Figure 19 is a flow diagram of an SMS transmission process of the system;

Figure 20 is a flow diagram of an SMS receiving process of the system;

Figure 21 is a flow diagram of an application execution process executed by the execution engine of the system;

Figure 22 is a schematic diagram illustrating the structure of response data sent from the client application to the application gateway;

Figure 23 is a schematic diagram illustrating how the system uses parameter names provided in instructions to label corresponding responses;

Figure 24 is a schematic diagram illustrating execution branching in the client application;

Figure 25 is a schematic diagram illustrating the use of branch domains to label responses having the same parameter name;

Figure 26 is a schematic diagram illustrating the use of a branch name stack to determine control flow;

Figure 27 is a schematic diagram illustrating the user interface components resulting from selecting different branches of an interactive application;

Figure 28 is a schematic diagram illustrating the inclusion of a 'back' button on each user interface display;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 982 of 1360

Figure 29 is a schematic diagram illustrating the use of an executed instruction stack to implement the 'back' button of Figure 28;

Figure 30 is a screen shot of a user interface of the application gateway for entering scripting language instructions and for submitting those instructions to an instruction compiler of the application gateway;

Figure 31 is a source code listing of a function illustrating how the system APIs can be used to send details of a booking to a mobile telephone for display to a user, and to receive the user's response indicating whether they user accepts or rejects the booking;

Figure 32 is a partial listing of a scripting language application, illustrating the use of control flow branches in the scripting language;

Figure 33 is a schematic diagram illustrating the user interface components generated from the scripting language example of Figure 32;

Figure 34 is a schematic diagram illustrating the use of nested user interface displays generated by the system;

Figures 35 and 36 are schematic diagrams illustrating the appearance and structure of general user interface displays generated by the system;

Figure 37 is a schematic illustration of a slider control display generated by the system;

Figure 38 is a schematic diagram illustrating the use of single and multiple selections in user interface displays generated by the system; and

Figure 39 is a schematic diagram illustrating how the branch names of nested menus are used to label parameter data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As shown in Figure 1, an interactive system includes at least one client application 102 and at least one application gateway 104. Each client application 102 is a component of a corresponding user device 106 that can communicate with the at least one application gateway 104 via one or more of a variety of communications means supported by the device 106, preferably including a combination of (i) an IP-based communications network 108 such as the Internet, (ii) a wireless wide-area communications network such as the global system for mobiles (GSM) telephone network, (iii) a local wireless network or link between the device 106 and the at least one application gateway 104, such as an infra-red link, Wi-Fi or Bluetooth network 112, and/or (v) a direct cable connection 114

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 983 of 1360

using a standard communications protocol such as RS-232, universal serial bus (USB), or FireWire (IEEE 1394). The interactive system allows an application developer 116 using a standard computer system 118 to rapidly develop and deploy an interactive workflow or application for execution on one or more user devices 106 in order to interact with the users 120 of those devices 106, and to receive response data representing at least one response of each user 120 to the interactive application.

The interactive workflow or application includes a set of instructions for presenting information to a user 120 of each mobile device 106 in an interactive display or user interface, and for retrieving each user's response(s) to that information. Typically, the information presented to a user 120 will include one or more questions displayed on a display screen of the user's device 106 (and possibly also audio played on a sound transducer of the device 106), and each of the user's responses is provided by the user interacting with one or more user-interface (UI) components or input controls of the interactive display. Each response can be in the form of freeform text typed into a textbox, or the result of the user interacting with another type of input control, such as radio buttons, check boxes, sliders, simple menus, nested menus, and so on. To some extent, these possibilities are determined by the capabilities of the device 106. However, because the workflow supported by the system also includes control flow features similar to those provided by high-level programming languages, the workflow instructions generated by the system are also considered to constitute an interactive software application that is executed on the user device 106.

In the described embodiment, the user device 106 is a mobile telephone, but alternatively could be some other type of portable or handheld device such as a personal data assistant (PDA), and hence is also referred to hereinafter as "the mobile device 106". However, even though the device 106 is described as being "mobile" or "portable", it will be appreciated by those skilled in the art that the systems and processes described herein could alternatively be used in conjunction with other types of devices and systems that need not even be portable. For example, the client application 102 could even be installed on a standard personal computer system (rather than the portable device 106) in order to rapidly develop and deliver interactive applications to a standard personal computer, for example.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 984 of 1360

In the described embodiment, the client application 102 is a software application that is stored on the mobile device 106, either as part of the device manufacturing or configuration prior to sale, or subsequently deployed as required via GPRS, Bluetooth, Infrared or a phone specific channel (*e.g.*, a data cable), allowing it to be installed on a wide variety of different types of device. However, it will be apparent to those skilled in the art that the client application 102 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

Similarly, the application gateway 104 is a software application that is installed on and executed by a standard computer system 122, such an Intel™ IA-32 computer server executing a Windows™ operating system. The computer system 122 includes standard hardware components 702, and software components 704. The hardware components 702 include at least one processor 706, a communications interface (*e.g.*, network interface card) 708, random access memory 710, non-volatile (*e.g.*, hard disk storage) 712, user input device (*e.g.*, keyboard, mouse or other pointing device) 714, and a display adapter and device 716, all interconnected by a system bus 720. The software components 704 include the application gateway 104, and a standard operating system 718 such as Microsoft Windows. Additionally, a third party application 124, shown as being installed on the developer's computer 118, may additionally or alternatively be installed on the same computer system 122 on which the application gateway itself is located 104, as shown. However, although the application gateway 104 is described as being a software application, it will be apparent to those skilled in the art that the application gateway 104 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

The client application 102:

(i) verifies a set of instructions sent by the application gateway 104;

(ii) interprets these instructions;

(iii) interacts with the user device 106 and/or the user 120 in accordance with the set of instructions; and

(iv) sends responses back to the gateway 104 or other computer system or device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 985 of 1360

The application gateway 104 is effectively a backend component that:

(i) maintains a database of user devices of the interactive system (*i.e.*, devices on which the client application 102 has been installed);

(ii) generates and delivers interactive applications to the mobile device 106 via any one of a wide range of communication channels;

(iii) ensures the integrity and authenticity of outgoing and inbound messages to and from the mobile device 106; and

(iv) provides application programming interfaces (APIs) to allow third-party applications 124 to deploy an interactive application to the mobile device 106 and to receive corresponding responses generated by the client application 102 on the mobile device 106.

Figure 2 is a schematic diagram illustrating the high level operation of the interactive process of the system in relation to the various components shown in Figure 1. At step 202, an external or third-party application 204 executing on the developer's computer system 118 (or, alternatively, on the gateway computer system 122) calls an API 616 of the application gateway 104 to describe the workflow that the developers of the device 106 want to deploy. In general, the workflow includes the steps of displaying information to a user, and then retrieving at least one response to that information. For example, a typical workflow might be to display a message on the mobile device 106, ask the user to enter their age, then display another message, and send the age back to the developer. These steps or instructions constitute an interactive application for execution on the mobile device 106.

The workflow defines:

(i) one or more addresses of respective user devices 106;

(ii) the steps to be performed on the one or more user devices 106;

(iii) the address of an alternate gateway server (if any) 104 to which responses are to be sent; if no address is given, then the responses will be sent to the same gateway server 104 that sent the application instructions;

(iv) how the response data returned to the application gateway should be processed (*e.g.*, returned to the developer's application 124, sent to the developer 116 by email, stored in a file, etc.); and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 986 of 1360

(v) the communication method(s) that are to be used to send the instructions to the user device 106 and to receive the corresponding response data.

At step 206, the application gateway 104 transforms the workflow described by the developer into a compressed, encoded, and encrypted format for transmission to the mobile device 106. The application gateway 104 also inserts a unique identifier or ID into the message and stores data associating that ID with the destination (*e.g.*, phone number, or network address) to which the workflow is to be sent.

The application gateway 104 transforms the message so that it can be transmitted via the appropriate communication means. For example, if the message is to be transmitted via SMS, the application gateway 106 splits a large message into smaller messages to comply with the GSM standard. All this is hidden from the developer. At step 208, the application gateway 104 then transmits the message to the device 106 specified by the developer.

At step 210, the client application 102 receives, un-compresses and decrypts the message(s), thereby verifying their integrity. If valid, at step 212 the client application 102 interrupts the user and requests that they complete the workflow. With the user's cooperation, the client application 102 interprets each instruction and performs a corresponding operation *e.g.*, display a message, collect the user's age, etc. that in most cases involves interacting with the user of the device 106.

At the end of the workflow, the client application 102 sends back to the application gateway 104 all the collected response data via the response channel specified in the workflow instructions by the application gateway 104. For example, if the response is to be returned via SMS, a response SMS is sent back to a phone number provided in the initial message(s). The client application 102 also encrypts the response message(s) and includes the unique message ID to ensure authenticity of the response.

When the application gateway 104 receives the response message at step 216, it decrypts the message and determines whether the ID of the message is valid for the phone number it was received from, using the destination and ID association stored previously. If the message is valid, then it is processed as specified by the developer *e.g.*, passes it on to a third-party application, emails the developer, stores it in a file, etc.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 987 of 1360

In addition to the above, the interactive system also provides capabilities for (i) storing (and subsequently updating) a set of instructions as a permanent or semi-permanent application stored on non-volatile storage of the user device 106 for execution at any time; *i.e.*, the application persists on the user's device; (ii) the distribution of encryption keys; and (iii) opt-in mechanisms to ensure that the mobile device 106 is not sent unsolicited applications, *e.g.*, if the application gateway 104 is shared by multiple vendors.

The interactive system and the interactive process executed by the interactive system are described in detail below.

As shown in Figure 3, the mobile device 106 is a standard mobile phone including hardware components 302 and software components 304. The hardware components 302 include a processor 306, read-only memory 308, random-access memory 310, flash memory 312, user interface components including user input components 314 (*e.g.*, microphone, keyboard, and, in some devices, touch-screen), output components 316 (*e.g.*, display screen, speaker), and one or more communications interfaces 318 allowing the device 106 to communicate with a mobile phone network 110, and, in some devices, also Bluetooth and/or Wi-Fi local wireless networks or an infrared link 112. In the preferred case of the mobile device 106 being a telephone, the device 106 also includes a SIM card 320. The software components include an operating system 322 such as the closed, proprietary operating systems installed on mobile telephones sold under brands such as Nokia and Motorola, Java platform Micro-edition (Java ME) 324, and the client application 102. However, if the operating system 322 is a more sophisticated operating system such as Symbian, Linux, Microsoft SmartPhone, PocketPC, Windows CE, or Windows Mobile, that provides sufficiently powerful application programming interfaces (APIs), then the J2ME component 324 can be omitted. As shown in Figure 4, the client application 102 includes a message sender component 402, a message receiver component 404, user interface (UI) widgets 406, a workflow execution engine 408, instant data storage 410, and permanent data storage 412. The client application 102 is a native application that is executed by the mobile device 106. The client application 102 can be installed by any one of a number of means, including WAP push, IP data packets (GPRS or 3G networks), Bluetooth, Infrared, or a phone-specific channel such as a data cable. The

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 988 of 1360

client application 102 can be provided as a preinstalled application on the mobile phone 106 when purchased.

The message sender 608 sends response messages to the application gateway 104 in a format understood by the application gateway 104. It encrypts the message and includes ID provided with the initial application to confirm its authenticity.

The message receiver 606 decrypts and uncompresses instruction sets received from the application gateway 104. It implements message reception via a number of channels, including Bluetooth, Infrared, IP networks (GPRS or 3G), and SMS. The message receiver 606 also invokes the workflow execution engine 408 to process the instruction set.

The UI Widgets 406 are pre-built user interface components that instructions sent by the application gateway 104 can use to interact with the user.

The workflow execution engine 408 is responsible for running and maintaining state for the instructions currently being processed. It associates instructions with UI widgets as well as storing input from the device 106 and its user. It is also responsible for invoking the message sender 402 once the workflow is completed to initiate sending the response to the application gateway 104. The workflow execution can also be invoked by a timer if an instruction asks to be run at a specific time.

The client application 102 can simultaneously receive multiple workflow applications at any one time, and the instant data store 410 is effectively a first-in, first-out queue that stores these applications and processes them one by one until the instant data store 410 is empty.

The interactive system has the ability to make a sequence of instructions persistent on the mobile device 106 as an application. These sequences are identified by a unique label and are stored in the permanent data store 412, being in this embodiment the non-volatile flash memory 312. The application gateway 104 can issue commands to update or delete applications in the permanent data store 412.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 989 of 1360

Figure 5 is a flow diagram illustrating the life cycle of an execution instance of the client application 102 following receipt of an instruction from an application gateway 104. However, the client application 102 can be invoked at step 502 by either a new data event or a timer event. A new data event occurs when the client application 102 is activated by the mobile device 106 when new payload data addressed to the client application 102 is received. Timer events are set by a specific instruction that suspends execution of the instruction to a later date/time. The workflow engine 408 is responsible for scheduling the client application 102 to start and process the instruction set at that date/time.

Once invoked, at step 504 the instruction sequence is retrieved either reading data from the instant data store 410, in the case of a Timer event, or from the input channel in the case of a new data event. If the instruction data is retrieved from the input channel and is encrypted, at step 506 the client application 102 decrypts and verifies it as described below. If the data is valid, the workflow execution begins at step 508.

The workflow execution 508 processes the instructions step by step. This may or may not involve user interactions (as some instructions described in the Appendix can be handled without user interaction). Upon execution of a timer instruction specifying that execution should be postponed to a later time, further execution of instructions of the workflow application is suspended and the instruction set is stored placed in the instant data store 410 pending resumption at the specified time.

Once the workflow execution 508 is complete, the workflow application is removed from the instant data store 410. If the application is marked as persistent, the instruction set is saved to the permanent data store 412. The user can then invoke the instruction set at any time.

At step 510, the information collected by the workflow execution 508 is sent back to the application gateway 104 as response data. The client application 102 encrypts the response data in addition to including the unique message ID that verifies the authenticity of the response data.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 990 of 1360

As shown in Figure 6, the application gateway 104 includes an instruction compiler 602, a key manager 604, a message receiver 606, a message sender 608, an opt-in manager 610, persistent storage 612, and an application programming interface (API) 616.

The instruction compiler 602 translates workflow descriptions received from the developer 116 into a format that is optimized for delivery to and execution by the client application 102. The workflow description is written in a scripting language that is compiled by the instruction compiler 602. The developer can enter the workflow description directly into a text box and submit its contents to the compiler 602. This is typically used to rapidly prototype the look and feel of a workflow application. Alternatively, the workflow description can be submitted by making an API call to the compiler 602 from a high-level programming language such as C#, Java, or TCL, thus providing end-to-end application integration.

The message sender 608 encrypts the workflow instruction set. The encryption relies on requesting the key manager 604 to provide a random index and an encryption key that is specific to a particular user device 106 on which the instructions are to be executed. The index is sent in cleartext to the client application 102, which uses the index to look up the appropriate encryption key to decipher the message. The message sender 608 also generates a unique random identifier for the workflow application. The random identifier is a combination of a random identifier and an identifier of the party who sent the workflow description.

The message sender 608 uses the transport adapter 614 to deliver the actual message(s) containing the workflow application. The message sender 608 first checks with the Opt-in manager 610 to ensure that the client application 102 does not receive unsolicited applications which it has not opted into, as described below.

The transport adapter 614 abstracts the various methods of delivering an instruction set to the client application 102 on the mobile device 106. It uses device capability information stored in the persistent storage 612 to determine the capabilities of the device 106 and hence the best communication channel to deliver the message(s).

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 991 of 1360

The transport adapter 614 provides plug-in support for new channel types dynamically by providing a set of messaging APIs and by allowing dynamic loading of compiled code that implements a new messaging interface. If required, the transport adapter 614 reformats the instruction payload so that it can be delivered via a particular channel. In particular, an application delivered by SMS may have to be divided into two or more smaller messages due to SMS message size limitations.

The key manager 604 is responsible for generating, distributing and managing the encryption keys issued to the portable device 106, as described below. It also provides encryption and decryption facilities for the message sender 608 and the message receiver 606.

The opt-in manager 610 provides an opt-in, opt-out process to allow client applications 102 select the entities they are willing to receive instruction sets from. This is desirable because the application gateway 104 may be shared by multiple parties and the client application 102 will otherwise execute any received instruction set as long as it is valid. The opt-in manager 610 maintains in the persistent data store 612 associations between parties and the phone numbers (or, in the case of devices other than telephones, other form of address or identifier of the destination device) they are allowed to send applications to. The process for creating these associations can be dynamic to allow users to selectively block or allow instructions from particular parties. For example, Figure 8 shows the message flow for an opt-in process.

At step 802, a party uses the external application 124 executing on the computer system 118 to send a workflow description to the application gateway 104, which at step 804 compiles and formats the instructions in preparation for sending them to a client application 102 that has not opted in. At step 806, the message sender 608 first checks whether the client application 102 has opted in. If not, at step 808 it asks the opt-in manager 610 to determine the opt-in status for this party and this user device. At step 810, the opt-in manager 610 sends an opt-in request message to the user, asking whether they agree to receive applications from this party. If the response is yes, at step 812 the opt-in manager 610 stores this information in the persistent data store 612 and then at step 814 instructs the message sender 608 to send the instruction set at step 816. Otherwise, if the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 992 of 1360

response is no, then the message sender 608 fails and notifies the party at step 818 that the user has not opted in.

Alternatively, the opt-in process could be performed manually, for example, by using a form that enables the user to directly add entries to the persistent data store 612. Alternatively, an analogous process could be used to opt-out of receiving applications from a particular party.

The message receiver 606 receives messages from the client application 102 and communicates with the transport adapter 614 to receive responses via any of the supported transport channels and protocols, including GPRS, IP network, Bluetooth, and SMS. For example, the instruction set of the interactive system allows instructions to be received by one physical channel/protocol (*e.g.*, SMS), and a corresponding response to be delivered by another (*e.g.*, Bluetooth).

When a message is received, the message receiver 606 first logs the message for audit purposes. Then it checks the authenticity of the message by deciphering the message using the key manager 604, and examining the unique message ID and the party ID to confirm that they match what was sent out.

Once the message authenticity is established, the message receipt is logged for billing and auditing purposes. Finally, the response message is processed as required by the party. This may include emailing the party; logging it to a file for the party to collect; and/or making a request to a third-party application to process the message. The actual method(s) used to process the response message can be specified when calling the API. If the API call does not specify a processing method, then the response is processed using the default method configured for the corresponding developer, determined when the developer establishes an account with the provider of the interactive system.

The persistent storage 612 is a non-volatile storage component that is used by:

(i) the key manager 604 to store the encryption keys for the various mobile devices;

(ii) the message sender 608 to store the addresses of user devices 106 (*e.g.*, phone numbers in the case of the device 106 being a telephone), together with the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 993 of 1360

delivery mechanisms that each user device 106 supports. It also stores the identifiers of the messages that have been sent out, for verification purposes;

(iii) the message receiver 606, to store received messages for audit and billing purposes; and

(iv) the opt-in manager 610, to store opt-in data representing each user device 106 and the third party applications that are authorised to send instructions to each user device 106.

Encryption keys

As described above, each installed instance of the client application 102 on a user device 106 is identified by a unique client identifier (also referred to herein as the client ID number) that is associated with its phone number. When a client application 102 is first installed on a mobile device 106, a number of private encryption keys are generated and associated with the client ID.

As shown schematically in Figure 9, these encryption keys are then used by the client application 102 to authenticate the payload data and to encrypt the response data. On each payload or response data packet or message, the index of the appropriate encryption key is indicated in the header of the payload.

Figure 10 is a schematic diagram illustrating the message and process flow for generating and updating encryption keys on a client application 102 and an application gateway or backend system 104. The process is initiated by the client application 102 making a secure communication activation request to the application gateway 104 at step 902. In response, the application gateway 104 generates and stores a set of private encryption keys, and associates these with the client ID at step 904. At step 906, the application gateway 104 sends these newly generated private keys to the client application 102. The client application 102 stores the received private keys on the persistent storage 412 at step 908, and returns an acknowledgement to the application gateway 104 at 910, confirming that the private keys have been stored (or updated if the keys had been previously stored). This completes the generation/update steps and secure communication is activated at step 912. This involves encrypting a message payload using one of the private encryption keys, which can be selected at random or on any other basis at step 914. At step 916, the secured payload encrypted with the selected key is sent to the client application 102, together with

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 994 of 1360

a message header specifying the index of the selected encryption key. At step 918, the client application uses the encryption key index indicated in the header to select the appropriate private key, and uses that key to decrypt the payload data at step 918. After performing the application instructions specified by the payload, the client application 102 then encrypts the response at step 920. The response can be encrypted using the same key, as shown in Figure 10, or any other of the stored keys. The secured response is sent to the application gateway 104 at step 922, and the response is decrypted using the appropriate response key at step 924. As will be understood by those skilled in the art, the use of private encryption keys greatly improves the security of communication, and the use of a set of encryption keys, rather than a single key, further increases this security.

When sending a response message, the client application 102 uses the source address of the corresponding payload data by default. This effectively provides multiple client-server communication channels in between the backend 104 and the client application 102. For example, Figure 11 shows an arrangement whereby two instances of the client application 102, a first instance 1002 and a second instance 1004, are in communication with two instances 1006, 1008 of the application gateway 104, via a wireless communications network 110. A message 1010 sent from the first backend system 1008 to the second client application 1004 includes an address 1012 of the first backend system 1008 in the header of the message 1010 so that when the client application 1004 sends the corresponding response 1014, it is addressed to the first backend system 1008.

In contrast, Figure 12 shows the same arrangement whereby a message 1102 also includes the address 1012 of the first backend system 1008. However, workflow instructions contained in the payload data can alter this default behaviour by redirecting the response to another backend server instead. This mechanism is activated by a DIVERT command in the payload data, described further in the Appendix. Specifically, in this message 1102 the payload 1104 includes a divert instruction with the address of the second backend system 1006. Consequently, after the second client application 1004 executes this instruction, the response 1106 is addressed to the second backend system 1006, rather than the first backend system 1008 that originated the message 1102 containing the instructions. Because the second backend system 1006 does not have direct access to the client ID and message ID pair, or the encryption keys for the client application 102, the second backend system 1006 calls an API of the first backend system 1008 to check the integrity and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 995 of 1360

authenticity of the response data. If the payload was encrypted, then the first backend system 1008 decrypts the payload and sends it back to the second backend system 1006 over a secured communications channel (using SSL, for example). In an alternative embodiment, the encryption keys are stored in a centralised component of the interactive system, and all encryptions and decryptions are performed in this manner.

Communication data payload

The payload exchanged between the client application 102 and the backend system 104 is binary data - a sequence of bytes. The communication channel for this payload can include SMS or Cell Broadcast Service (CBS) messages; IP/TCP data packets (over GPRS, 3G or other type of data networks); and/or Bluetooth data packets.

As shown in Figure 13, each data payload is prefixed with a header 1204 which indicates whether the payload is encrypted with an encryption key. The header data contains the index of the encryption key stored in the client application key-storage, thereby allowing the client application 102 to decrypt the payload data.

As shown in Figure 14, plain payload data (either unencrypted or after being decrypted) contains a series of variable-length data parts that instruct the dynamic workflow execution engine 508 of the client application 102 to construct the user UI workflow.

As shown in Figure 15, each data part includes type 1402 and length 1404 data fields, followed by the actual instruction data 1406. The type field is a single octet or byte that defines the type of workflow instruction that follows. The length indicates the number of octets or bytes of the instructor data 1406.

As described above, the interactive system is able to use one or more of a variety of different communication channels for sending and receiving messages and responses between the application gateway 104 and the client application 102. For most of these different communication channels, the communication itself is straightforward, using the standard methods and libraries available and known to those skilled in the art. However, the interactive system supports message and response delivery via the short message service, or SMS. SMS is defined in the GSM 03.40 specification, which defines an upper limit on the size of each SMS message. Specifically, each SMS message is capable of

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 996 of 1360

containing up to 140 bytes of data, equivalent to 160 ASCII characters when using 7-bit encoding, as shown in Figure 17. The interactive system sends SMS messages including 8-bit (binary) data and including a 7-byte user data header or UDH 1702, as described in the GSM 03.40 specification. The UDH 1702 consists of a length field or UDHL 1704, specifying the length of User Data Header in bytes as specified in GSM 03.40, and a 6-byte User Data Header field 1706 specifying the destination address of the payload data 1708.

The UDH data 1702 - specifying the destination of the binary message - is interpreted by the mobile device to deliver the payload data to the client application 102. Excluding UDH data 1702, each SMS message is capable of carrying 133 bytes of payload data 1708.

If the payload data exceeds this length, the payload data is sent in two or more SMS messages 1804, each message containing up to 127 bytes of payload data 1806, 1808, as shown in Figure 18. These SMS messages 1804 have a section of User Data Header indicating that they all belong to a concatenated message, as described in the GMS 03.40 specification. A byte padding mechanism is used by the backend system 104 and the client application 102 when the payload is sent in multiple SMS messages. In this mechanism, a padding or termination byte 1810 with value 0xFF is appended to the end of each payload data fragment 1806, 1808 when sent out from the backend system 104. The client application 102 removes these padding bytes 1810, which appear as stuffed bytes 1812 in the concatenated payload data before passing the payload data 1814 to the workflow execution engine 408. The byte padding mechanism is used to eliminate problems found in a number of mobile phone models that strip out the last byte of every concatenated data fragment.

The instruction compiler 602 creates the payload data from the compiler output to generate binary SMS messages. Construction of binary messages includes splitting the payload data 1802 into multiple SMS messages 1804 if the data length exceeds the single message capacity of 133 bytes. Figure 19 is a flow diagram showing the steps involved in this process.

As shown in Figure 19, when delivering a message or a response via SMS, at step 1902 a check is performed to determine whether the size of the payload data exceeds 133 bytes. If

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 997 of 1360

not, then at step 1904 a user data header is added, and a single SMS message is composed and sent at step 1906. Alternatively, if the payload length does exceed the maximum size that can be sent in a single SMS message, then at step 1908 a concatenated message identifier is generated, and at step 1910 the number of concatenated messages that are required to accommodate the payload data is determined. Then, a processing loop consisting of steps 1912 to 1920 composes the appropriate number of SMS messages as follows. At step 1912, the next payload portion is selected and copied to the payload of the current SMS message. At step 1914 a user data header is added, including the identifier indicating that the SMS message is part of this SMS message set. At step 1916, a padding or termination byte is appended to the payload data, as described above. Finally, at step 1918 the resulting SMS message is sent. These steps 1912 to 1918 are repeated until the test at step 1920 determines that the last part of the payload data has been sent, and the process then terminates.

Removal of stuffed bytes in the payload data is handled by the client application 102 by searching for the specific stuffed byte octet value (0xFF in this embodiment) and removing it from the payload data, as shown in Figure 20.

Figure 16 is a schematic diagram showing the fifteen different instructions supported by the interactive system, showing the respective type bytes identifying each instruction type, and the structure of the corresponding instruction parameters. Further details on the various instructions are provided in the Appendix.

Dynamic workflow execution engine

The client application 102 presents to the user a number of user interface (UI) widgets 406 as well as executing user-invisible routines. This allows the client application 102 to display information as well as capture device information and/or user inputs.

The UI widgets 406 typically include the following type of user interface components and controls:

(i) Message screen: to show textual information;

(ii) Selection menu: to ask for the user's selection of one of a number of defined choices (*i.e.*, radio buttons);

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 998 of 1360

(iii) Multiple choices: to ask for user's one or more choices (*i.e.*, check boxes);

(iv) Textual input: to retrieve free form text input from the user (textbox);

(v) Numeric or date inputs: to retrieve user input data, restricted by type; and

(vi) Widgets displayed when branching and jumping amongst execution steps.

However, this list of UI widgets 406 and their actual screen layouts can vary depending on the platform (*i.e.*, on each combination of device hardware and operating system software) on which the client application 102 is installed.

The client application 102 implements a workflow execution process 2100, as shown in Figure 21, on each invocation to execute a workflow application. The workflow execution process 2100 begins after the client application 102 is invoked at step 2102, and a test is performed at step 2104 to determine whether the invocation has resulted from the receipt of new payload data from the application gateway 104. If so, then at step 2105 the new payload instructions are retrieved, and then parsed at step 2110. Otherwise, if the invocation was not due to the receipt of new payload data, then a test is performed at step 2106 to determine whether instructions are contained in the instant data storage 410. If so, then the instructions are retrieved from the instant data storage 410 at step 2108, and then parsed at step 2110. Otherwise, another test is performed at step 2132 to determine whether any sets of instructions have been saved as applications in the permanent data storage 412. If not, then at step 2134 an information message is displayed to the user indicating that there are no applications (instant or permanent) in the queue. Once the user acknowledges this information message, or when a corresponding timeout period has elapsed, the client application 102 is terminated. Alternatively, if the permanent data storage 412 contains one or more permanently stored sets of instructions (*i.e.*, applications), then at step 2136 these are displayed to the user, and the process 400 pauses at step 2137, awaiting the user's selection of one of these, or selection of a quit option. If, at step 2138, it is determined that the user has selected the quit option, then the client application 102 terminates. Otherwise, the user has selected a permanently stored set of instructions, and these are retrieved at step 2140, and then parsed at step 2110.

Following parsing of the workflow instructions at step 2110, the first or next workflow instruction is read at step 2112, and executed at step 2114. If it is determined at step 2116 that the instruction is a UI instruction, then the process waits to receive user input at step 2118. Once the user's response has been received, at step 2120 the UI widget

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 999 of 1360

displayed on the screen of the device 106 is removed, and any user input is stored at step 2122. At step 2124, a test is performed to determine whether the instruction was the last in the workflow. If not, then the process loops back to step 2112. Otherwise, once all of the instructions have been executed, then a response message is composed at step 2126, and sent at step 2128. If the workflow instructions executed are stored in the instant data storage 410, then they are deleted at step 2130. This terminates the workflow execution process 2100.

Parsing workflow instructions and response data

The workflow execution engine 408 of the client application 102 interprets the payload data parts and generates the dynamic UI workflow accordingly.

The data parts from the payload data are indexed sequentially when read by the workflow execution engine 408, and, this is also the default order of workflow execution 508. As shown in Figure 22, the response data includes each response in the same order as the corresponding instructions were received and executed. When a workflow instruction is executed and response data is to be retrieved, a parameter name is included in the instruction data, and the user response or system response is associated with this parameter in the response. All the instruction responses are included in the response data when the workflow is completed, as shown in Figure 23.

Jumping and Branching in the workflow

The workflow execution engine 408 provides a mechanism to allow branching and jumping in the sequence of instructions.

Branching

Because an instruction might be involved in different branches through out the workflow, the workflow execution engine 408 differentiates the instruction response data for different branches using branch domains. A branch domain specifies the address of a workflow instruction in the workflow tree. When setting the instruction response data, the response parameter name is prefixed with the corresponding branch domain, separated by a period character. For example, an instruction to retrieve user input for a numeric-valued parameter with the parameter name "number" could be called from two different branch menus: one named "First branch", and the other named "Second branch". In both of these

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1000 of 1360

cases, the instruction returns the same parameter name "number" but with different values. The workflow execution engine 408 associates a branch domain with the parameter name to differentiate the two response values. Thus in this example, the first value is returned as "First branch.number = xxx" and the second value as "Second branch.number = yyy", where "xxx" and "yyy" represent the actual values entered by the user. Figure 25 shows a more complex example where menu selections are nested.

Additionally, the branch domain is appended with a branch name on selection of a branch menu. For example, in an application with two nested branch menus 3902 "Service Request" and 3904 "Water Service" as shown in Figure 39, when the user selects item 3910 "Water" in menu 3902, and then selects item 3912 "Pipe Burst" in the subsequent branch menu 3904 "Water Service", and then fills out 3914 with "John Doe" in the text input screen 3906 "Your name", the client application 102 will internally send the response as "Water.Pipe burst.name=John Doe". When the BRANCH_BACK command is executed, the previous branch name is removed. The workflow execution engine 408 uses a branch name stack to maintain the order of branch names as they are selected.

For usability reasons, when working with a multiple branch menu, it is important for the user to know whether or not a branch has already been visited by the user. To this end, the workflow execution engine 408 indicates visited branch menu items by displaying an image adjacent to those branches to indicate that they have already been visited by the user. For example, as shown in Figure 27.

When the user has visited user input screen 2702 to enter data 1, an image icon 2706 is displayed adjacent to the first branch menu item 2704 is marked with distinct. This allows user to visually distinguish those parts of the workflow that have been visited from those parts that have not been visited. Alternatively, the visited branches could be displayed in a different colour, as used by web browsers to indicate that a hyperlink has been visited.

Backward navigation

As shown in Figure 28, all of the user interface screens include a "Back" navigation button 2802 to allow the user to return to the previous screen within the workflow. The position of this back button can change depending on the specific mobile device platform executing

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1001 of 1360

the client application 102. As shown in Figure 29, the workflow execution engine 408 maintains an ordered list or stack of instructions that cause a change in the screen or display, and selection of the "Back" button causes the execution to return to the previous instruction.

Sending a workflow description to the Instruction Compiler

As described above, a developer 116 can send a workflow description to the instruction compiler 602 of the application gateway 104 by submitting programming instructions written in the programming language supported by the instruction compiler 602, using a hypertext transport protocol (HTTP) interface of the instruction compiler 602. For example, Figure 30 is a screenshot of an HTML webpage generated by the application gateway 104. The webpage includes a scrollable text box 3002 into which the developer 118 can directly enter commands in the scripting language, and a compile button 3004 which, when pressed, submits the text in the scrollable text box 3002 to the instruction compiler 602 for compilation.

The scripting language of the interactive systems is a high level language for describing the workflow of an interactive application. It is similar in vein to BASIC and can be learnt quickly by a programmer who has a basic knowledge in programming.

Alternatively, a workflow description can be sent to the instruction compiler 602 by invoking API calls to the application gateway API 616. For example, Figure 31 shows a source code listing of a J2ME function `SendWorkflowRequest` that is used to generate and send workflow instructions to the mobile telephone 106. In this example, the workflow instructions are to display booking details to the user 120 and then retrieve the user's response indicating whether the user 120 accepts or rejects the booking, together with the user's name and telephone number. The workflow API is first initialised by creating (at 3102) a new J2ME Command() object named `WorkflowCommand`. A workflow header, as described below, is then added at 3104. Workflow instructions are then added in the order of desired execution by calling APIs that are provided as methods of the `WorkflowCommand` object. Each type of workflow instruction is added by calling a corresponding API function with a set of parameters. For example, the object method `AddInfoMessage` is used (at 3106) to add an instruction that displays a screen of

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1002 of 1360

information to the user. The first argument to this method provides a title for the screen, and the second argument provides the actual text information that is displayed. Similarly, the method `AddSingleMenu` adds (at 3108) an instruction that displays a single-level menu (*i.e.*, radio buttons) to the user, allowing the user to select one item from a list of items provided as a parameter to the method. In this example, the two items are displayed as "Accept", and "Reject", and the user's response indicates whether the user 120 accepts or rejects the booking.

The method `AddUserInputCmd (at 3110 and 3112)` displays a text string to the user, together with a textbox, prompting the user to enter an appropriate input value. The first parameter to this function finds the name of the parameter that will be associated with the returned input value. The second argument provides a string that is displayed to the user, and a third argument allows the developer to restrict the type of input; for example, to a phone number, email address, and so on.

Finally, the `AddRedirectHeader` method (at 3114) defines a return address or phone number to which the response will be redirected, as described above. The communication channel to be used (*e.g.*, whether by SMS, IP network, Bluetooth, etc) is also specified in the header.

Once the workflow instructions are added, the workflow API is called again (at 3116) to compile the instructions and build the payload data to be sent to the client application. The workflow API is called as many times as needed (at 3118) to send multiple messages if required.

Scripting Language Overview

- Instructions are written line by line.
- Comment lines start with //
- Label lines start with #
- String parameters are delimited by double quote characters ""

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1003 of 1360

Workflow-programming Structure

Commands are processed sequentially line by line. Three instructions are provided to create tree structures of the workflow: BRANCH_TO, BRANCH_BACK, and GOTO. BRANCH_TO and BRANCH_BACK are used in combination to create a subroutine for the compiled program. GOTO is a jump instruction that allows program execution to jump to a specified line in the script. Comment and blank lines are ignored by the instruction compiler 602.

Command line syntax

A command is a line in the script which has the following structure:

<Command Name> <String Parameter> <String Parameter> <Label>

Where:

- <Command Name> is a command.
- <String Parameter> is a qualified string value, *i.e.*, delimited by double quote characters. For example, "User name" is a string parameter. There can be more than one string parameter in each command.
- <Label> is the name of the label that is associated with the command. Labels can only be used with the GOTO command and the ITEM command when used in conjunction with BRANCH_TO command.

Comment

There is no block comment in the language. Comment lines are lines that start with // (two forward slash characters followed by a space character).

Example:

// this is a comment line

Label

A label is a way to mark a line number so that it can be referred to in GOTO and BRANCH_TO 's ITEM commands. A label line starts with # (hash) character, followed by a space character. The label name is the next word from the # character.

Example:

For label START, the line looks like this:

START

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1004 of 1360

The label name is mapped to the index (*i.e.*, relative position in the script) of the command immediately following the label line.

Labels in a script must be unique, a compile error occurs if a duplicate label is detected. All labels are parsed in the first pass of the compiler, building a mapping of label and command index to be used in the second pass.

Backward navigation

As described above, a "Back" navigation button is attached to all displayed screens by default. This button allows backward navigation of the workflow executed on the user device 106. On most mobile phone platforms, this "Back" button is mapped to the right action key. However, this can change depending on the type of phone.

Tree navigation

A combination of the BRANCH_TO command, labels, and the BRANCH_BACK command allows the workflow to support a tree like execution structure, as shown in the source code listing of Figure 32 and the resulting display screens of Figure 33. A detailed description is provided below. When a user is navigating thought workflow screens, the state of each screen (item selection and user inputs) is not remembered.

Example

The following is a source code listing that is used to generate an interactive application for execution on a user device such as the mobile telephone 106. The source code defines a workflow that allows the user 120 of the mobile telephone 106 to generate a service request for water, electricity, and/or gas services. The listing is arranged in four groups of commands or paragraphs under respective labels. The first paragraph, labeled START, results in display of a main screen 3402, as shown in Figure 34. The BRANCH_TO command has two parameters. The first, "serv" defines a branch name for this branch, and the second parameter, "Service Request" defines the title that is displayed at the top of the main screen 3402. The subsequent three commands define items that can be selected by the user to invoke corresponding workflow branches. For example, the first ITEM command has two parameters. The first parameter, "Water", defines the text 3404 that is displayed on the main screen 3402, and that can be selected to invoke the corresponding workflow branch. The second parameter, in this case "WATER", is a label of the corresponding

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1005 of 1360

workflow branch, in this case referring to the second group or paragraph of commands grouped under that label. Thus if the user navigates the main screen 3402 to select the first item 3404, the workflow jumps to the SELECT ITEMS, causing display of a water service selection screen 3406. In this case, the three items are simply menu selections (rather than workflow branches), and thus selection of any one of these items causes the appropriate parameter, in this case named "water" to be assigned a value defined with the corresponding item. For example, if the user selects the second item, "Leaking" 3408, then the parameter "water" is assigned the value "Leaking". Once this item has been selected, the workflow proceeds to the following command, which in this case is the BRANCH_BACK command, which returns control to the main screen 3402.

In this manner, the user can select the Electricity item 3410 to branch to the ELECTRICITY workflow, resulting in display of a Electricity service screen 3412. Similarly, the user can select the "Gas" request item 3414 to cause a Gas service screen 3416 to be displayed. Once the user is satisfied with the service requests thus defined, selection of the Next button 3418, or the OK button 3420 causes execution to continue to execute in this example the command "GOTO CONTACTS", which causes the workflow to jump to the command following the CONTACTS label, being in this case an INPUT command displaying a name input screen 3422, and subsequently a Contact number screen 3424. Once the OK button 3426 on the Contact numbers screen 3424 has been selected, a MESSAGE command causes display of a Service Info screen 3428 providing informational feedback to the user, in this case confirming that the service request will or has been sent to an appropriate party for processing the user's request.

```
// Start of program
#START
BRANCH_TO    "serv" "Service Request"
ITEM         "Water" WATER
ITEM         "Electricity" ELECTRICITY
ITEM         "Gas" GAS
GOTO         CONTACTS

#WATER
SELECT       "water" "Water service"
```

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1006 of 1360

```
ITEM            "Pipe Burst"
ITEM            "Leaking"
ITEM            "New connection"
BRANCH_BACK

# ELECTRICITY
SELECT      "elect" "Electricity service"
ITEM            "Fire"
ITEM            "New connection"
ITEM            "Disconnection"
BRANCH_BACK

# GAS
SELECT      "gas" "Gas service"
ITEM            "Leaking"
ITEM            "New connection"
ITEM            "Fire"
BRANCH_BACK

// This is like a subroutine
# CONTACTS
INPUT           "name" "Your Name" ANY
INPUT           "phone" "Contact Number" NUMERIC
// message is sent here
//# END
MESSAGE     "Service Info" "Your request will be sent to XXXX"
```

Script commands and syntax

HEADER command

The HEADER command is used to include a specified piece of text at the beginning of the response message when the workflow has been executed. This command is invisible to the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1007 of 1360

user of the user device. This command is used as a context identifier for server-client conversation.

There can be multiple header commands in the script. When using the HEADER command in conjunction with the BRANCH_TO command, different response message prefixes can be set, based on the user's selection.

Syntax

HEADER <header>

- <header> is a string parameter to be prepended to the response text message.

Example

HEADER "timesheet"

Response

<header> is attached to the beginning of the response message. If there are multiple headers to be included in the response message, the response headers are prepended based on their execution order in the workflow.

DIVERT command

The DIVERT command is used to redirect a response message to a telephone number or address different from that of the source of the original instructions. Normally, the response message is sent back to the source address of the payload, but the response message can be sent back to another number instead by including a DIVERT command in the workflow. This command is invisible to the user. There can be multiple DIVERT commands in the script, but the last one that is executed in the workflow takes effect. When combining this command with the BRANCH_TO Command, the workflow can send a response message to a source number selected by the user.

Syntax

DIVERT <address>

- <address> is a string parameter representing the mobile number of the redirected address.

Example

DIVERT "+61418366896"

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1008 of 1360

MESSAGE command

MESSAGE command shows a message with a title and message content to the user.

Syntax

MESSAGE <title> <message content>

- <title> is a string parameter for of the title of the message to be displayed.
- <message content> is a string parameter.

The end result is display of a screen as shown in Figure 35.

Example

MESSAGE "Hello" "Hello world"

Response

This GUI screen does not collect any user input and no response data is associated with it.

INPUT command

This command displays a GUI screen with a text input box 3602 to the user to retrieve user inputs, as shown in Figure 36. A parameter name is provided in the command to set the name of the user input data when included in the response message. A default input value can be provided as an input parameter. If desired, the user input data can be restricted to a certain types such as numeric, decimal or a phone number. However, the implementation of user input restriction depends on the capability of the user device executing the client application 102.

Syntax

INPUT<return parameter> <label> <type> <default value>

- <return parameter> is a string parameter for the name of the entered value to be set in the return message.
- <label> is the title of the input text box
- <type> is the type of the input to be captured, these types are available:
  - ANY
  - EMAILADDR
  - NUMERIC

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1009 of 1360

- PHONENUMBER
- URL
- DECIMAL

- <default value> is an optional string parameter to be set to the input text box when the screen is visible to the user. If omitted, the default value of the input text box is left empty.

Response

User input data is included in a response message associated with a parameter name specified in the corresponding instruction. If the INPUT command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<return parameter>=<value> (without domain path)

<domain path>.<return parameter>=<value>

Where:

- <value> is a string value that user enters. This can be an empty value.
- <domain path> is the path of branches that lead to this INPUT command in the workflow.

GAUSS command

This command results in the display of an interactive screen having a slider or "gauss" control 3702 to prompt the user to provide corresponding response data, as shown in Figure 37. The user is able to slide the slider control from a minimum value to a maximum value specified on the command line. The resulting data is included in the response message associated with the parameter name given.

Syntax

GAUSS <parameter name> <minimum value> <maximum value> <default value>

- <parameter name> is a string parameter for the name of the gauss value to be set in the return message.
- <minimum value> is the minimum value the user can select.
- <maximum value> is the maximum value the user can select

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1010 of 1360

- <default value> is the default value if the user does not select any value. This parameter is optional so if it is not present, the default value is empty.

Example

GAUSS "temper" "1" "10" "5"

Response

If this command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<parameter name>=<value> (without domain path)

<domain path>.<parameter name>=<value>

GOTO command

This command allows the workflow execution engine 406 to jump to a specific workflow instruction, rather than proceed to the next instruction in sequence. A parameter of this command is the label of the instruction for the workflow execution to be directed to. There is no user screen or response data associated with this instruction.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1011 of 1360

Syntax

GOTO <label>

- <label> is the label name indicating the index the command that the workflow execution jumps to after executing this command.

Example

....

GOTO Hello // The program jumps to message hello world after executing this command.

...

...

Hello

MESSAGE "Hello" "Hello world"

...

SELECT, SELECT_MULTI command

As shown in Figure 38, these commands display a screen with a list of items to select from. The SELECT command allows single item selection, and the SELECT_MULTI command allows multiple item selection screen. The user selection is included in the response message identified by the parameter name. In case of multiple selection list, the selected values are separated by a delimiter character in the response value data.

Syntax

SELECT or SELECT_MULTI command is followed by ITEM definitions (one per line).

SELECT <parameter name> <title>
ITEM <item name>
ITEM <item name>
ITEM <item name>

SELECT_MULTI < parameter name> <title>
ITEM <item name>

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1012 of 1360

ITEM <item name>
ITEM <item name>

Where:

- < parameter name > is a string parameter specifying the return parameter id for the SELECT screen.
- <title> is a string parameter specifying the title of the screen.
- <item name> is a string parameter specifying the item to be displayed on the screen.

Example

```
// This example allows the mobile user to select one of the option listed
SELECT "tsk" "Select task"
ITEM "Administration"
ITEM "Service desk"
ITEM "Client meeting"

// This example allows mobile user to select one or many of user names in the list
SELECT_MULTI "name" "Select users"
ITEM "User 1"
ITEM "User 2"
ITEM "User 3"
```

For multiple select command, each of the items in the select list is displayed adjacent to an icon that indicates whether or not the item has been selected by the user. On most mobile devices, a "Mark" button is displayed to allow user to mark the selection of the highlighted item. A "Next" button is also attached to this screen to allow the user to navigate to the next workflow instruction. On some mobile device platforms, the Next button is mapped directly to one of the mobile phone buttons.

Response

SELECT command:

<parameter name>=<item>

SELECT_MULTI command:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1013 of 1360

< parameter name >=<item>;<item>;<item>

Where:

- <item> is the item name as selected

The multiple select response can be empty.

BRANCH_TO command

This command provides users a list of items to select, and on selection of an item, execution of the workflow is branched to the specified command. The behavior of this screen is similar to the SELECT screen described above. Once the workflow execution starts executing from the new target instruction, it follows the default sequential order. When the BRANCH_BACK command is executed, the workflow execution engine returns to the previous BRANCH_TO command to execute. However, the BRANCH_TO command does not require a BRANCH_BACK command to operate. The workflow can consequently branch to the last command without returning to the branch menu.

To progress to the next screen from a BRANCH_TO command, a "Next" button is provided. On some phones, this button is mapped to one of the phone keys on the mobile device. On most phones however, this button is mapped to a soft-key named "Next" when the user select Options on the BRANCH_TO screen (similar to SELECT_MULTI command).

There is no specific user value attached to this screen in the response message. The selected branch item is however appended to the branch domain path. This domain path is then appended to the parameter name of any input screens being executed in the branch target.

Syntax

BRANCH_TO command is followed by ITEM definitions (one per line).

```
BRANCH_TO    <parameter name> <title>
ITEM         <item> <label>
ITEM         <item > <label>
ITEM         <item > <label>
```

Where:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1014 of 1360

- < parameter name > is a string parameter specifying the return parameter id for the BRANCH_TO screen.
- <title> is a string parameter specifying the title of the screen.
- <item > is a string parameter specifying the item to be displayed on the screen.
- <label> is a valid label name as specified in the workflow with "#" character.

Examples

```
...
# EnterBetAmount
INPUT "bet" "Enter bet amount" DECIMAL
BRANCH_BACK
....
# SelectBetAmount
SELECT "bet" "Select bet amount in dollars"
ITEM "100"
ITEM "200"
ITEM "300"
BRANCH_BACK
....
BRANCH_TO "b" "Select team to bet"
ITEM "Melbourne" EnterBetAmount
ITEM "Geelong" SelectBetAmount
GOTO END
...
# END
MESSAGE "Info" "Please select Yes to allow response message to be sent"
```

Response

- The domain path is appended with <item> selected in the branch menu.
- This domain path is then appended to the parameter name of any input screen executed in the branch target. In the example script, the "bet" amount parameter name when appearing in the response message is: Melbourne.bet=<bet value>.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1015 of 1360

BRANCH_BACK command

This command is invisible to the user, it provides the capability to navigate back from branching. A workflow could have multiple branches wired up and the result is a tree like structure. BRANCH_BACK command allows navigation upwards in this tree structure. Combination of label and BRANCH_BACK command allows combining a group of workflow commands in to a routine, which can be referred to multiple times during the workflow execution.

Syntax

BRANCH_BACK

STORE_PERMANENT command

This command instructs the workflow execution to store the whole payload data to persistent storage. A title is set in the parameter of this command allows the client application to display the stored payload data to the user. This command does not result in any user data in the response message.

Syntax

STORE_PERMANENT <title>

Where:

- <title> is a string parameter indicating the title of workflow payload data to be displayed in the persistent list. This persistent list is displayed to the user when the client application is started manually by the user and no instant payload data is waiting to be executed.

Example

STORE_PERMANENT "Message one"

CLEAR_PERMANENT command

This command clears all the persistent workflow payload data previously saved by STORE_PERMANENT command. Execution of this command does not result in any data in the response message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1016 of 1360

Syntax

CLEAR_PERMANENT

EXECUTE command

This command makes a request to the mobile device operating system to retrieve an URL address. The results could be making a phone call or launching the internet browser on the phone to the specified URL address. Behavior of this command might varies across different device models due to device capabilities.

Syntax

EXECUTE <url_address>

Where:

- <url_address> is a string parameter describing the URL address of the request to be sent to the J2ME platform.

Example

To make a mobile phone call to +61418366896 mobile number

EXECUTE "tel:+61418366896"

To launch the internet browser on the mobile phone to access ACME mobile website

EXECUTE "http://mobile.acme.com"

Response

If making a mobile phone call is required, the mobile device will ask user if a mobile phone call can be made. If launching of the internet browser is required, the application will ask for the user's permission to open the internet connection to the specified URL.

CONFIGURATION command

The response message is constructed from the user/system data. A number of default delimiter characters are used to separate the data parts as well as name-value separator. This command when included in the payload data can change the delimiter characters of the response message as well as specifying whether or not the name part is included in the response message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1017 of 1360

Syntax

CONFIGURATION <configuration_string>

Where <configuration_string> is composed of configuration characters:

- 1st character: Include parameter in the response, if set to '0', the response message only has values, set to '1', the response message has Name=Value
- 2nd character: Response part delimiter, the default is ','
- 3rd character: Equal character, the default is '='
- 4th character: Multiple selection options, the default is ';'
- 5th character: Screen path delimiter, the default is '.'

Example

CONFIGURATION "0,=;."

This configuration command instructs the workflow execution to exclude parameter names from the response message.

SYSTEM_PROPERTY command

This command instructs the workflow execution to read a system property and return the result in the response. The parameter name that is associated with the response data is the system property if parameter name is omitted.

Syntax

SYSTEM_PROPERTY <property_name> <parameter name>

Where:

- <property_name> is the system property to be read. On the J2ME platform, examples of these properties are:
  - microedition.profiles
  - microedition.configuration
- <parameter name> is an optional string parameter. If omitted, property name is used as parameter name in the response instead.

Examples

SYSTEM_PROPERTY "microedition.profiles"

SYSTEM_PROPERTY "microedition.profiles" "midp"

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1018 of 1360

Response

The value of the system property is included in the response message as name=value pair. All the rules applied to the name-value pairs are applied. These include changing of delimiter parameters and whether or not to include the name part in the response message.

<system property>=<value> (if parameter name is omitted)

<parameter name>=<value> (if parameter name is present)

NOP command

This is a no-operation command. It is useful when used in conjunction with labeling.

Syntax

NOP

SET_KEYS command

A command to set the encryption key specified by the index of the key on the mobile device.

Syntax

SET_KEYS <key_index> <key>

Where <key_index> is a string parameter indicating the index of the key to be set on the client application 102. <key> is a string parameter containing the actual key to be updated.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as hereinbefore described with reference to the accompanying drawings.

It will be apparent from the description above that the interactive system and process described herein allow a developer to dynamically send on demand customisable workflow instructions to one or more user devices 106 such as mobile telephones. The generation, secure delivery, execution, and secure return of response data to the developer are all handled transparently by the interactive system, thus hiding all the details of these aspects from the developer, greatly simplifying the provision of interactive applications and quasi-real-time interactions with one or more users. The provision of workflow instructions via

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1019 of 1360

SMS is particularly advantageous as it can be assumed to be supported by all mobile telephones available today. Moreover, since the SMS communications are all managed by the interactive system, any premium SMS services that may be required can be established by the operator of the interactive system, thus freeing the developer from needing to establish their own independent premium SMS services. This greatly simplifies the provision of new interactive applications, and also allows the operator of the interactive system to provide these services at a lower cost by leveraging the substantial volume of SMS traffic resulting from the aggregation of SMS traffic or all developers using the interactive system.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1020 of 1360

CLAIMS:

1. A method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

2. A method as defined by claim 1 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language.

3. A method as defined by either of claims 1 or 2 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

4. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device.

5. A method as defined by claim 4 wherein the step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

6. A method as defined by claim 5 wherein the step of sending the message includes the step of sending a unique message identifier.

7. A method as defined by claim 6 further comprising the step of the mobile user device receiving the set of instructions and the unique message identifier.

8. A method as defined by claim 7 wherein the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

9. A method as defined by either of the claims 7 or 8 further comprising the step of receiving a response to the instruction from the mobile user device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1021 of 1360

10. A method as defined by claim 9 wherein the step of receiving a response includes the step of receiving a response identifier from the device.

11. A method as defined by claim 10 wherein the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

12. A method as defined by any one of the preceding claims wherein the step of translating the instruction includes tailoring the instruction to a device operating system.

13. A method as defined by any one of the preceding claims wherein the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

14. A method as defined by claim 13 wherein the step of translating the interactive workflow includes tailoring the instruction to the specification.

15. A method as defined by any one of the preceding claims wherein the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

16. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network.

17. A method as defined by claim 16 wherein the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS.

18. A method as defined by any one of the claims 1-15 wherein the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1022 of 1360

19. A method as defined by any one of the preceding claims also including the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow.

20. A method as defined by claim 19 wherein the step of checking involves sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow.

21. A method as defined by claim 3 wherein the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface (API) from the external or third party.

22. A method as defined by claim 21 wherein the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

23. A method as defined by any one of the preceding claims also comprising the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

24. Computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

25. A method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1023 of 1360

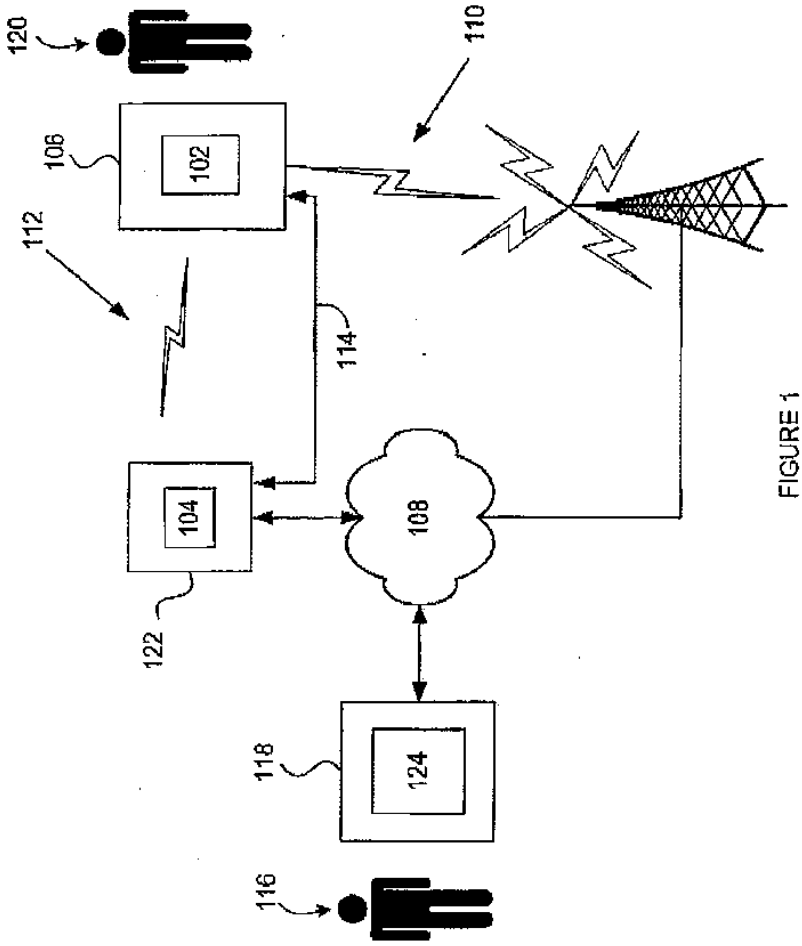


FIGURE 1

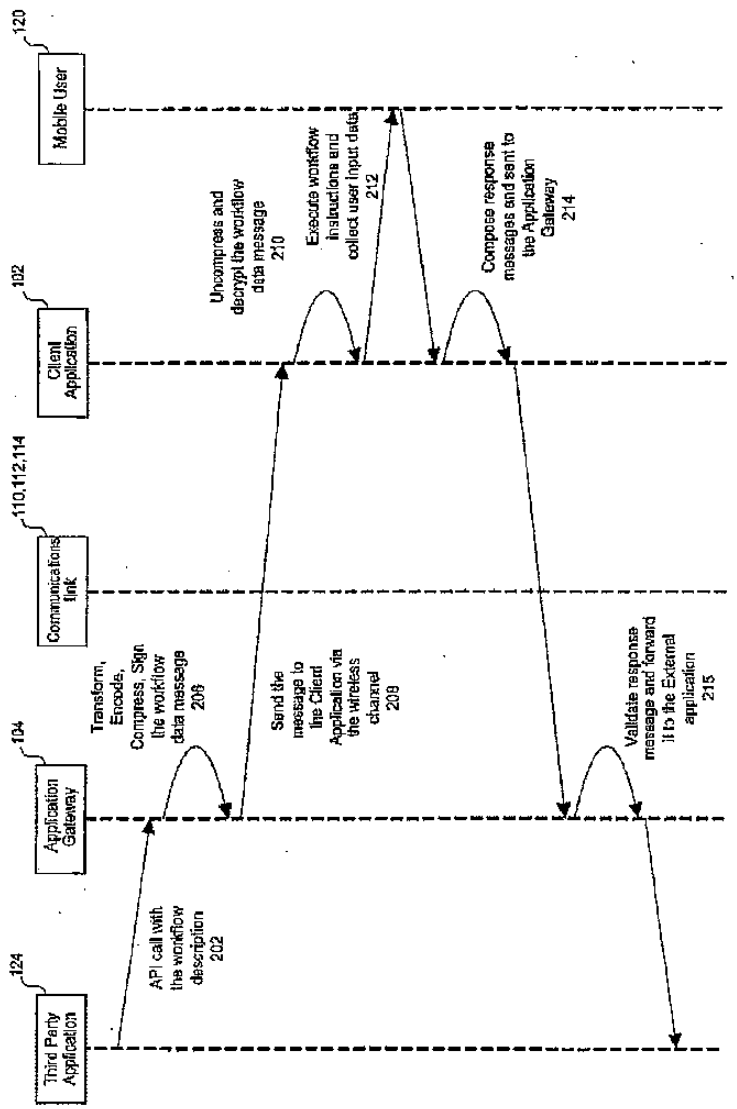


FIGURE 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1025 of 1360

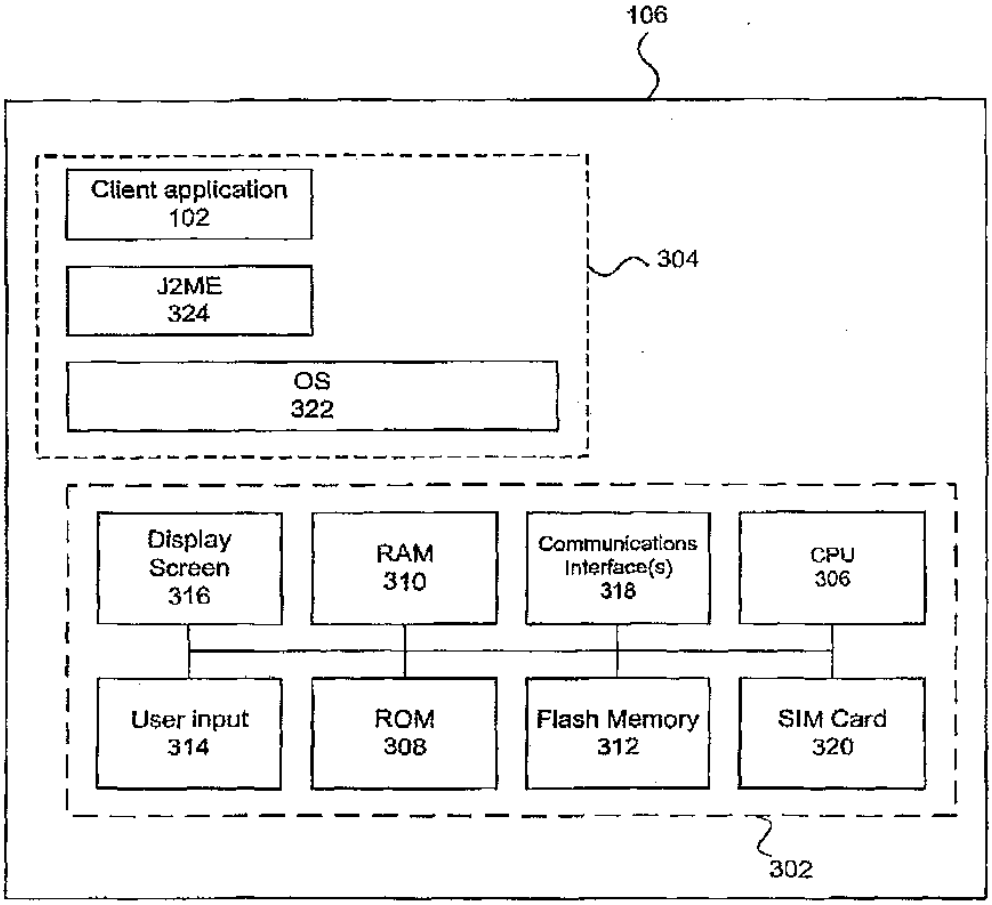

106
Client application
102
J2ME
324
OS
322
304
Display
Screen
316
RAM
310
Communications
Interface(s)
318
CPU
306
User input
314
ROM
308
Flash Memory
312
SIM Card
320
302

FIGURE 3

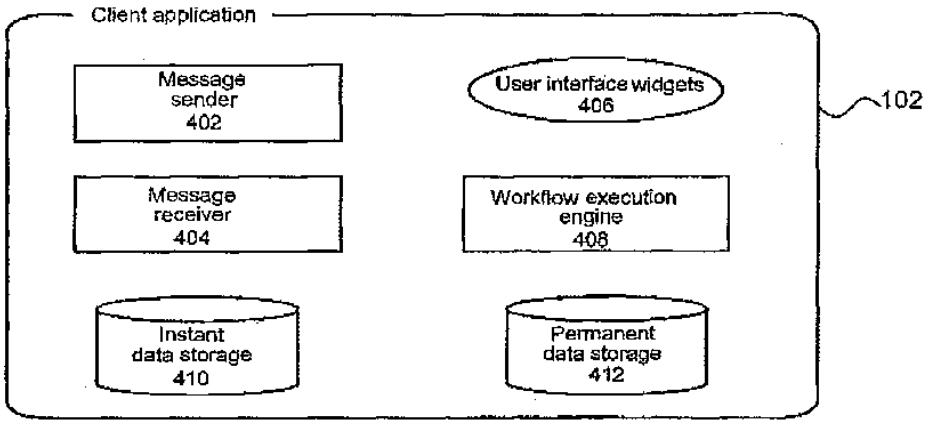


FIGURE 4

FIGURE 5

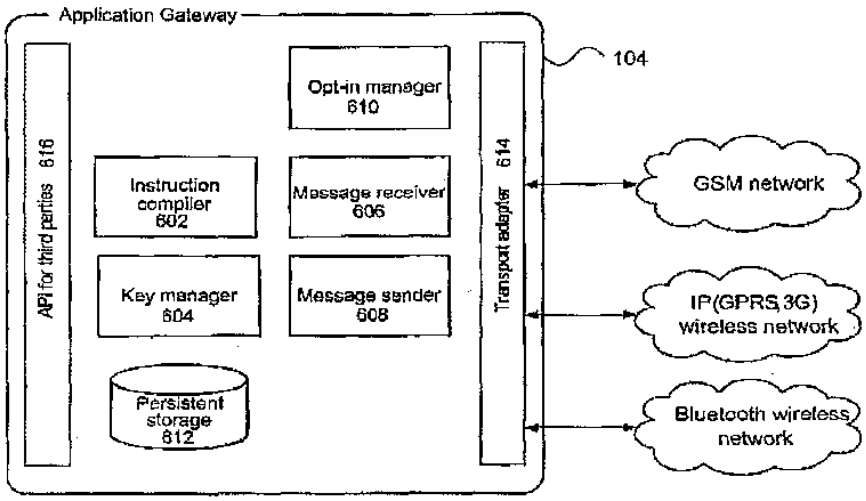

Application Gateway
104
API for third parties 616
Opt-in manager 610
Instruction compiler 602
Message receiver 606
Key manager 604
Message sender 608
Persistent storage 612
Transport adapter 614
GSM network
IP(GPRS,3G) wireless network
Bluetooth wireless network

FIGURE 6

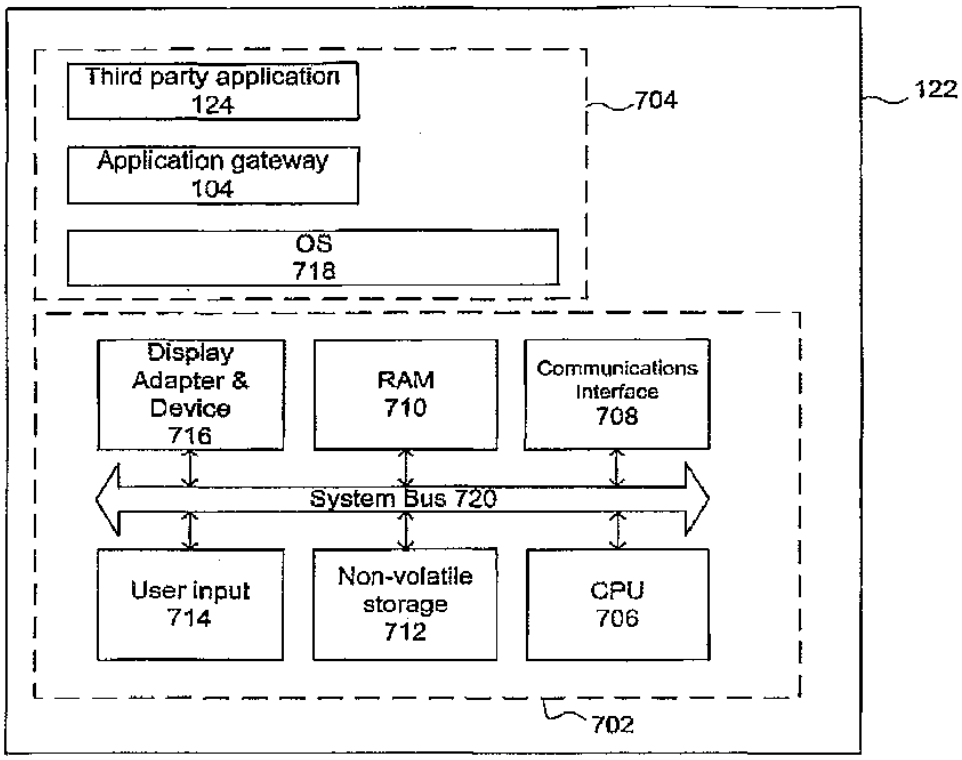

Third party application
124
Application gateway
104
OS
718
704
122
Display
Adapter &
Device
716
RAM
710
Communications
Interface
708
System Bus 720
User input
714
Non-volatile
storage
712
CPU
706
702

FIGURE 7

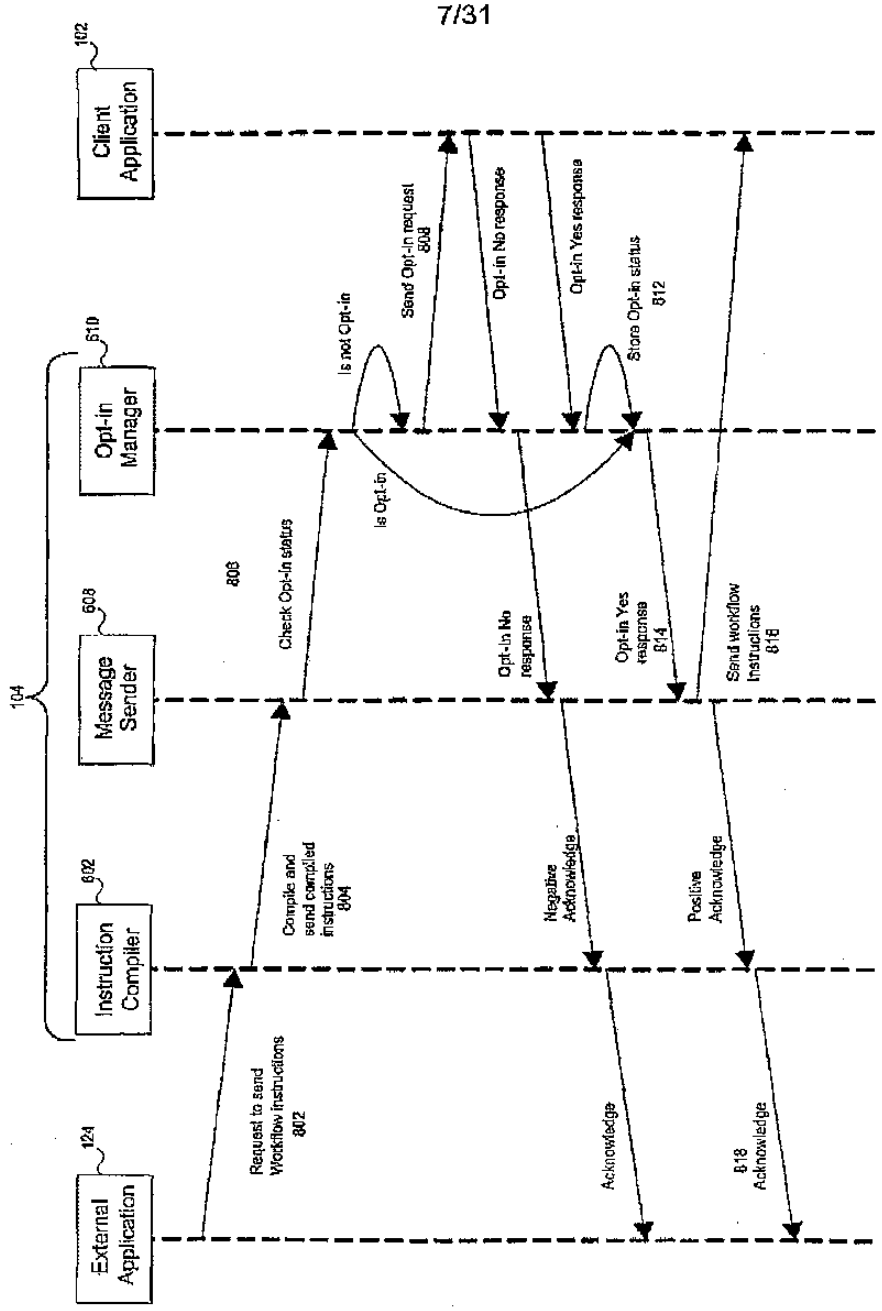


Figure 8

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1030 of 1360

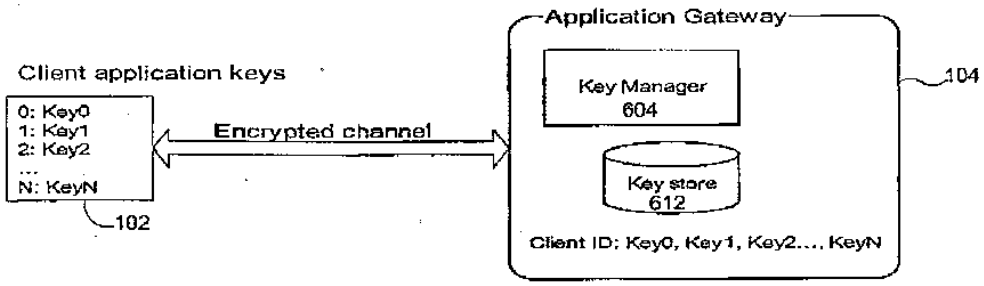

Application Gateway
Client application keys
0: Key0
1: Key1
2: Key2
...
N: KeyN
Encrypted channel
Key Manager
604
Key store
612
Client ID: Key0, Key1, Key2..., KeyN
102
104

FIGURE 9

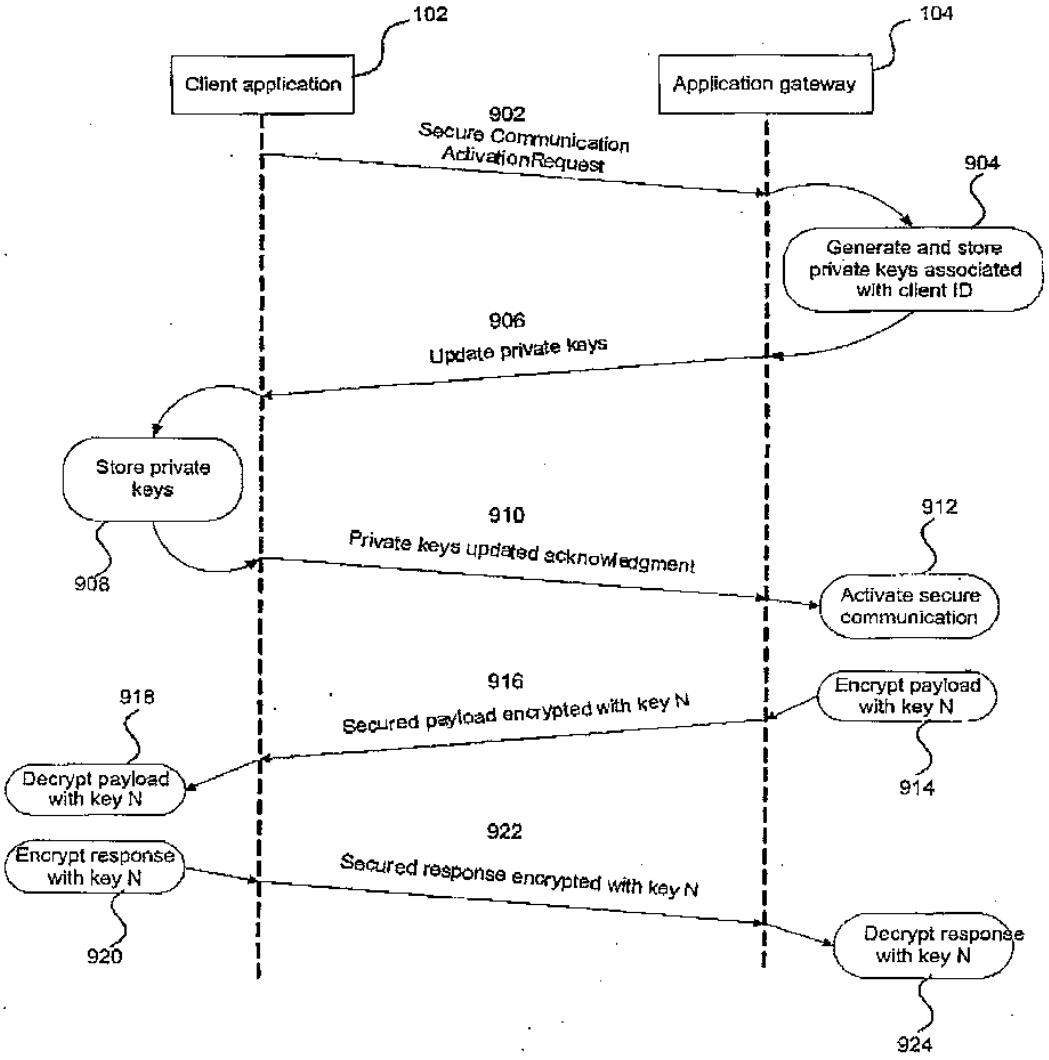


FIGURE 10

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1032 of 1360

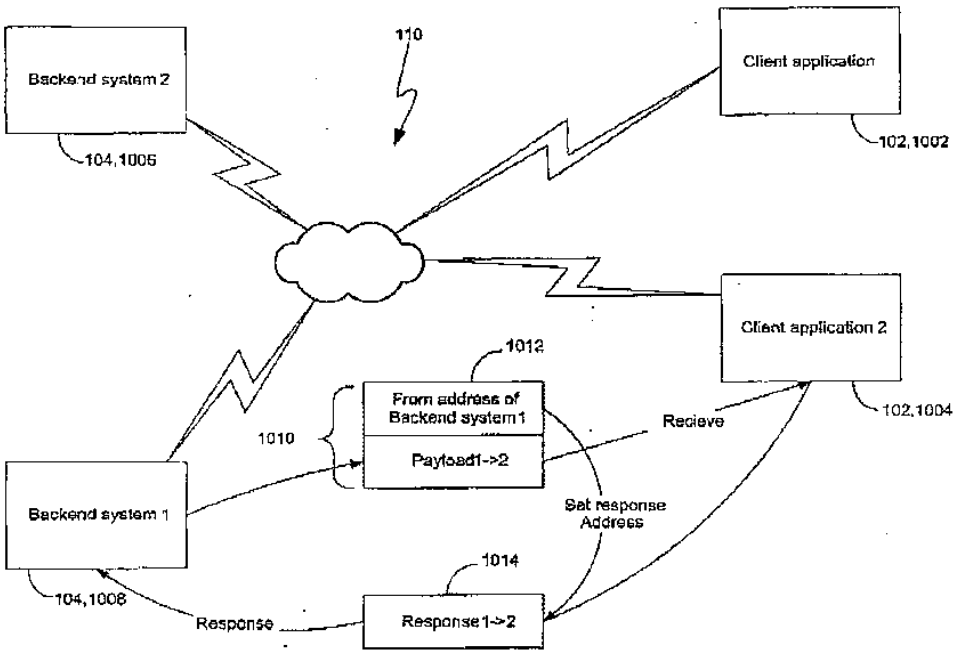

110
Backend system 2
104,1006
Client application
102,1002
Client application 2
102,1004
1012
From address of Backend system 1
Payload1->2
1010
Recieve
Backend system 1
Set response Address
1014
104,1008
Response
Response1->2

FIGURE 11

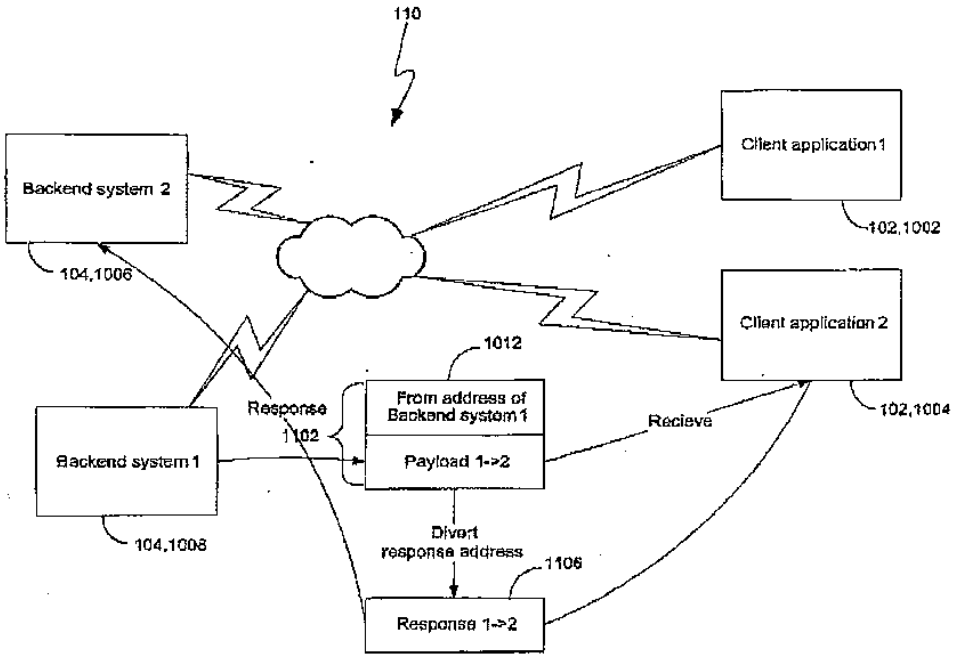

110
Backend system 2
104,1006
Client application1
102,1002
Client application 2
102,1004
1012
From address of Backend system1
Payload 1->2
Response 1102
Backend system1
104,1008
Recieve
Divert response address
1106
Response 1->2

FIGURE 12

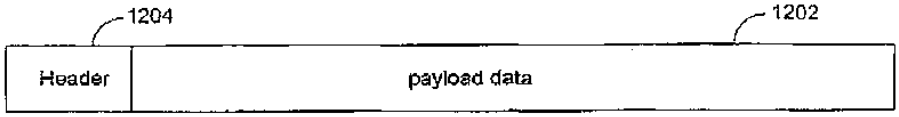


FIGURE 13

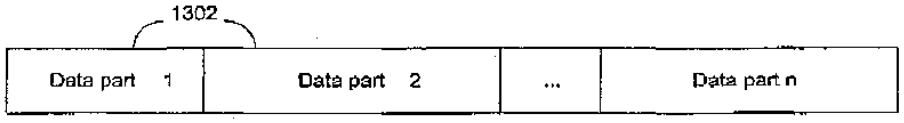


FIGURE 14

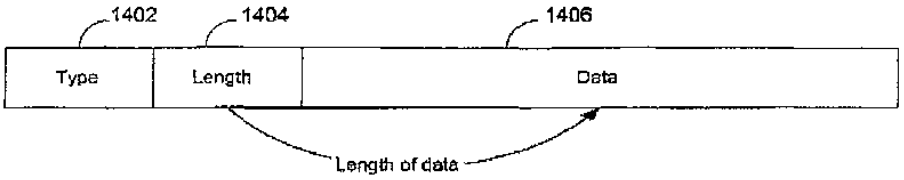


FIGURE 15

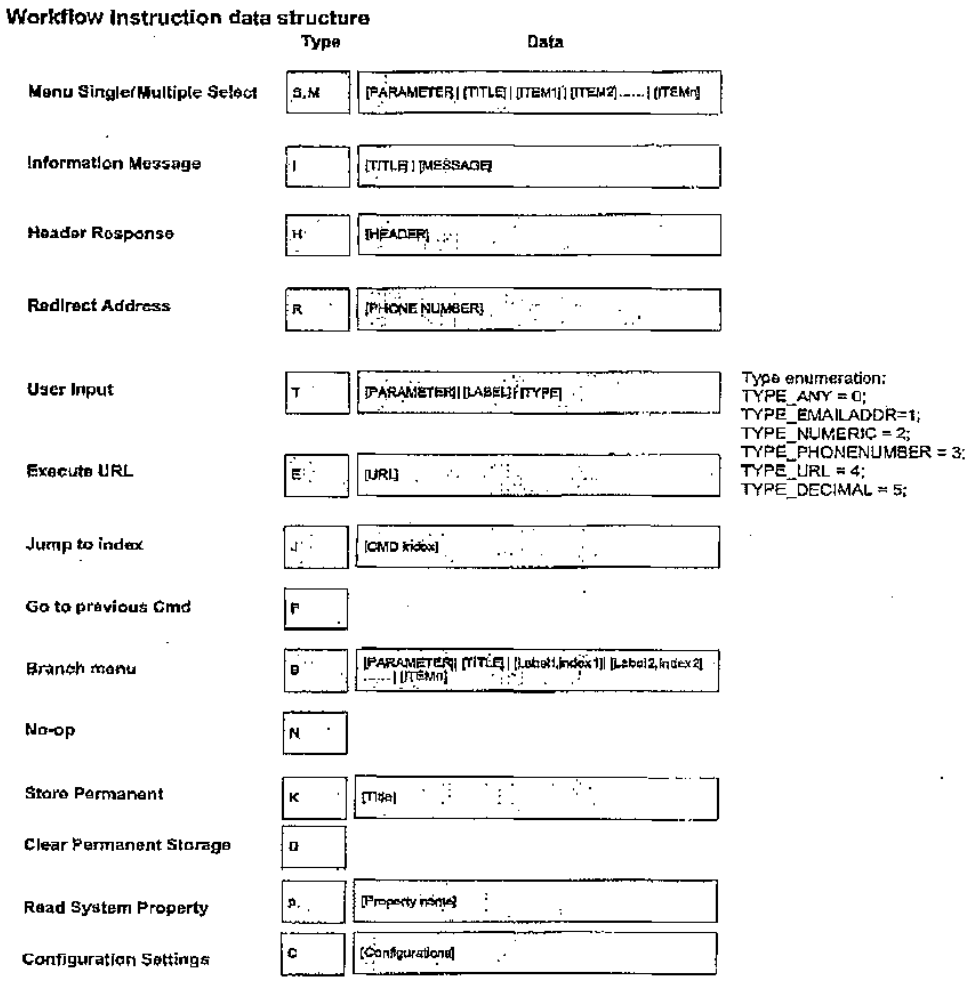


FIGURE 16

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1036 of 1360

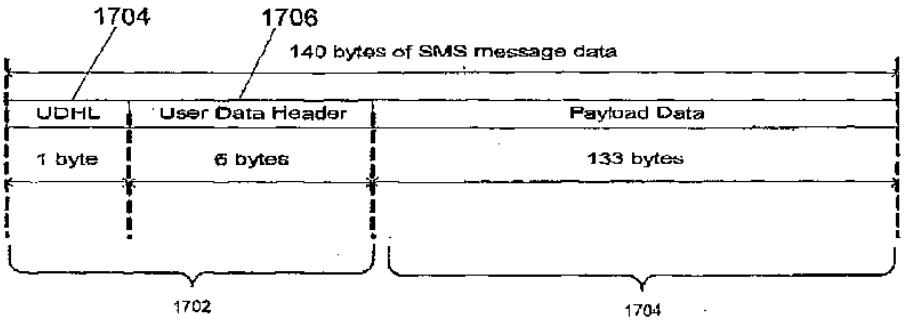

1704
1706
140 bytes of SMS message data
UDHL
User Data Header
Payload Data
1 byte
6 bytes
133 bytes
1702
1704

FIGURE 17

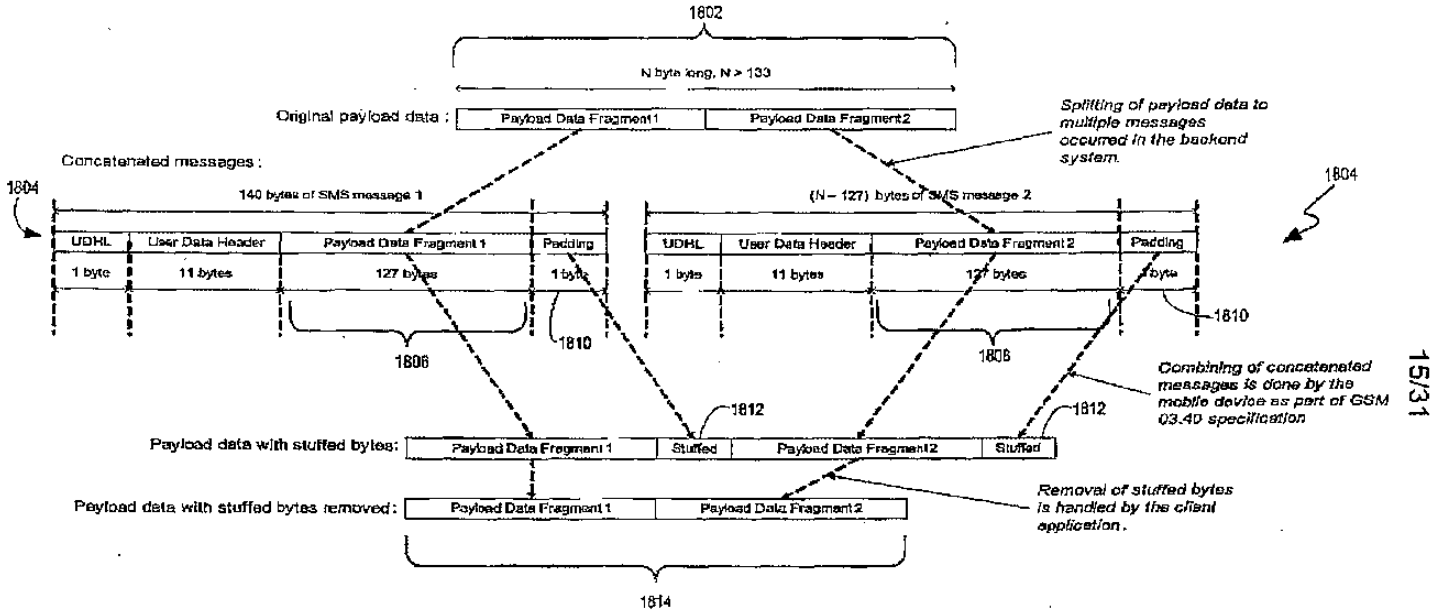


FIGURE 18

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1038 of 1360

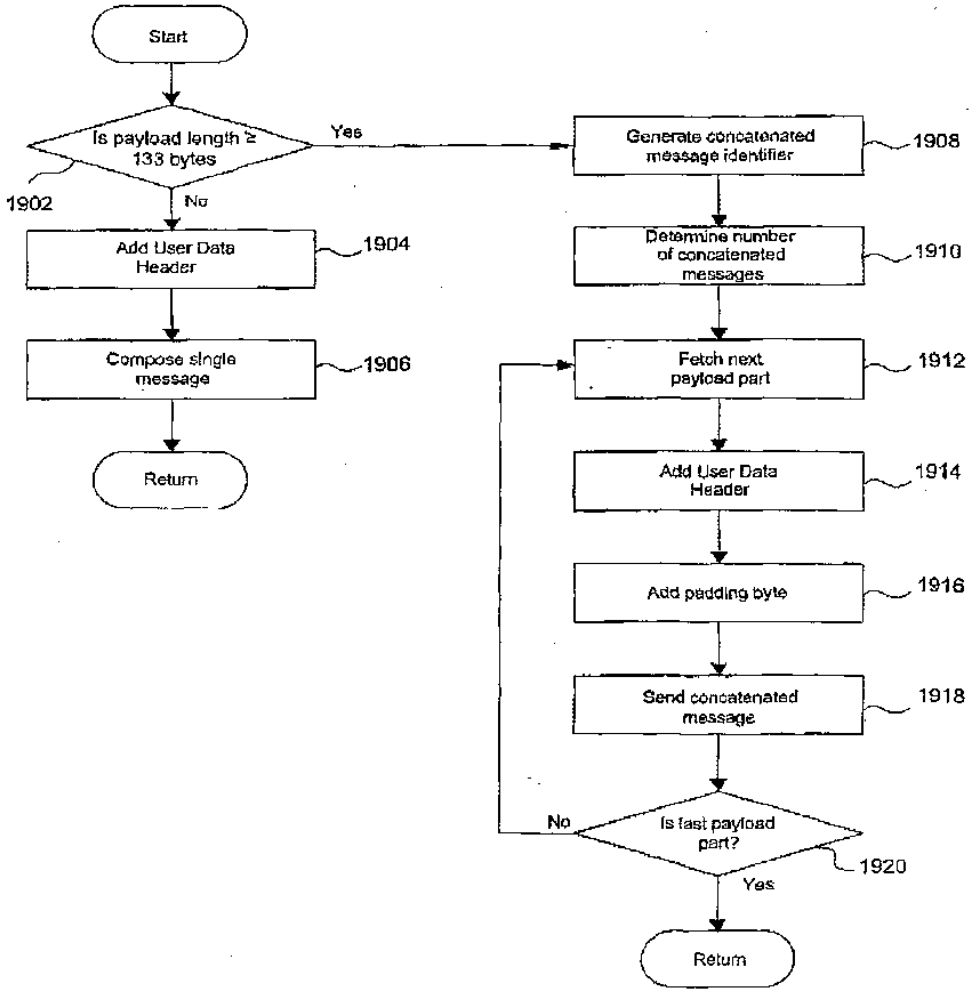

Start
Is payload length ≥ 133 bytes
Yes
No
1902
Add User Data Header
1904
Compose single message
1906
Return
Generate concatenated message identifier
1908
Determine number of concatenated messages
1910
Fetch next payload part
1912
Add User Data Header
1914
Add padding byte
1916
Send concatenated message
1918
Is last payload part?
No
Yes
1920
Return

FIGURE 19

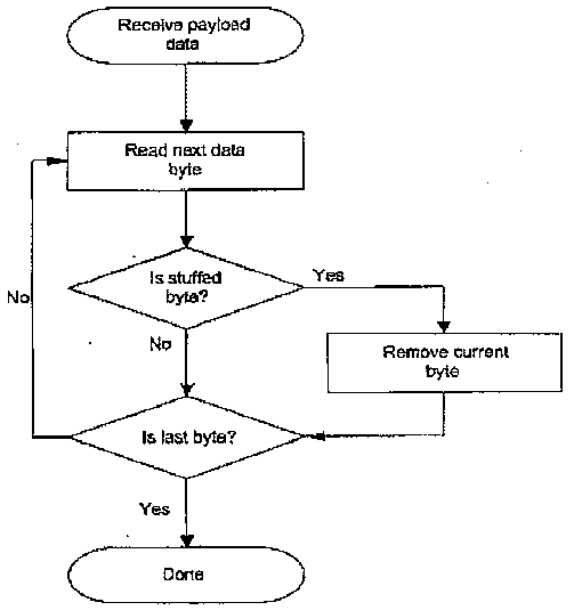

Receive payload data
Read next data byte
Is stuffed byte?
Yes
No
Remove current byte
Is last byte?
No
Yes
Done

FIGURE 20

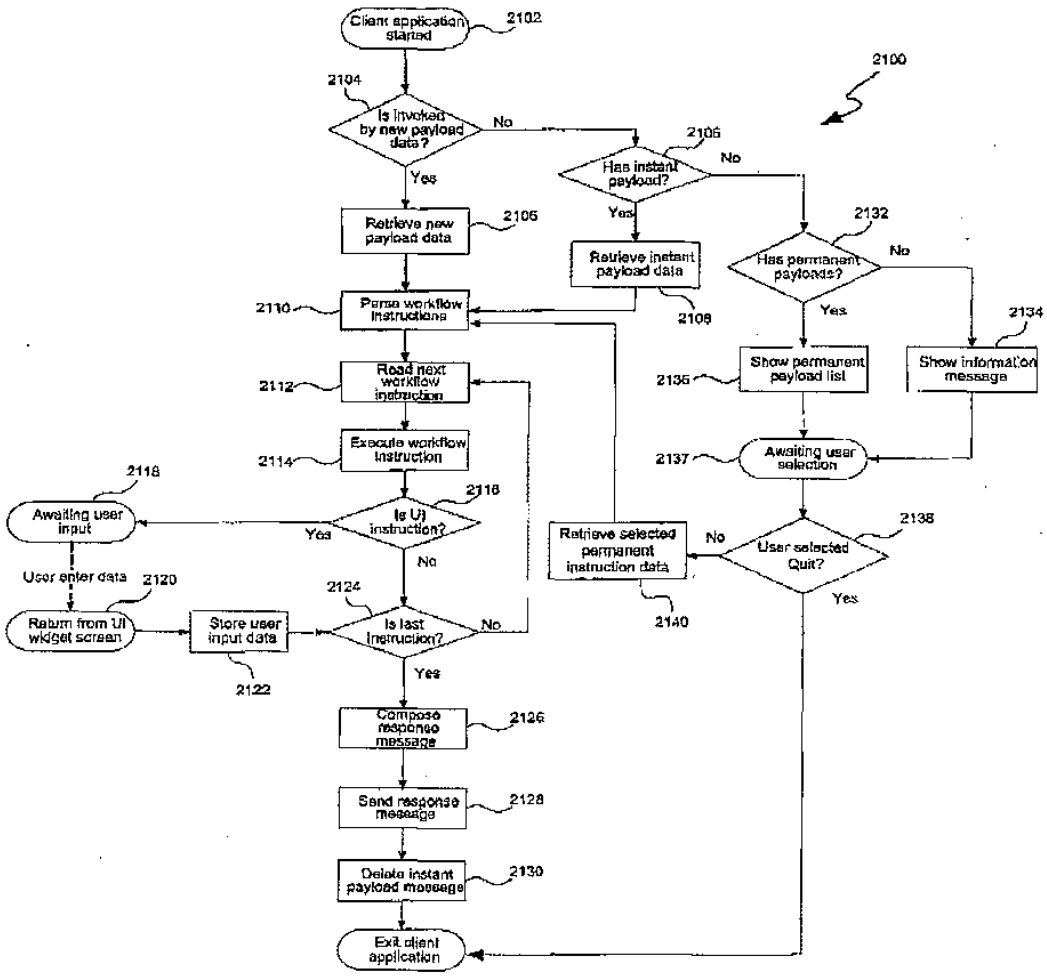

Client application started
2102
2100
2104
Is invoked by new payload data?
No
Yes
2105
Has instant payload?
No
Yes
Retrieve new payload data
2106
Retrieve instant payload data
2109
2132
Has permanent payloads?
No
Yes
2134
2110
Parse workflow instructions
Show permanent payload list
Show information message
2135
2112
Read next workflow instruction
2137
Awaiting user selection
2114
Execute workflow instruction
2118
Awaiting user input
2116
Is UI instruction?
Yes
No
Retrieve selected permanent instruction data
No
2138
User selected Quit?
Yes
2140
User enter data
2120
Return from UI widget screen
Store user input data
2122
2124
Is last instruction?
No
Yes
2126
Compose response message
2128
Send response message
2130
Delete instant payload message
Exit client application

FIGURE 21

0	Instruction 1 response
1	Instruction 2 response
n	Instruction n response

FIGURE 22

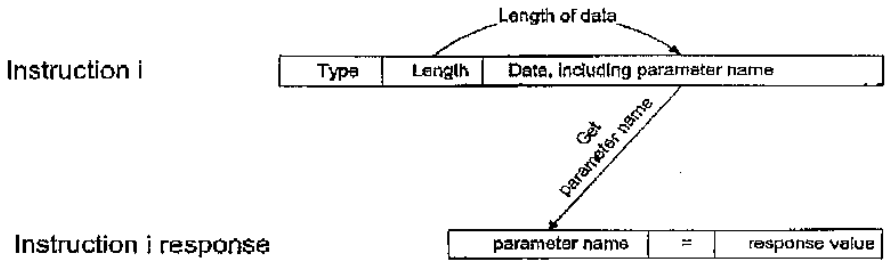


FIGURE 23

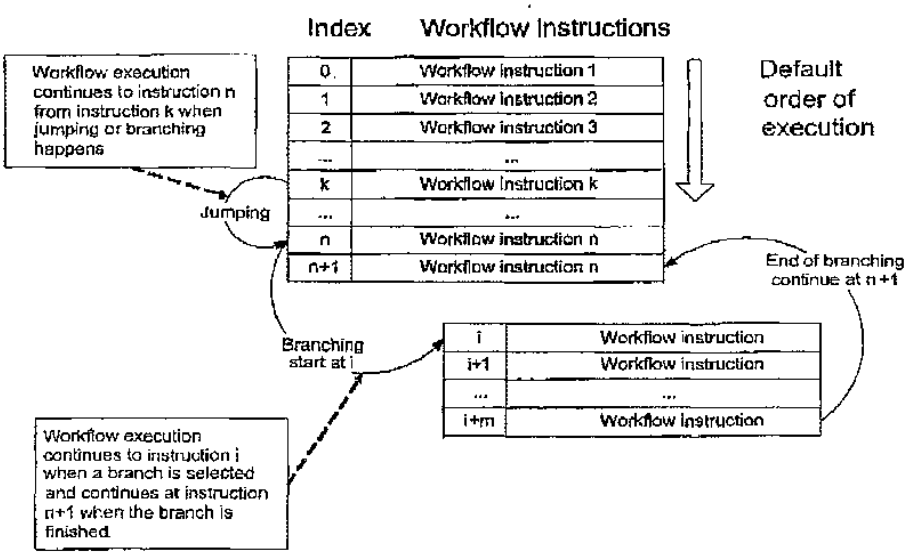

Index
Workflow Instructions
Workflow execution continues to instruction n from instruction k when jumping or branching happens
0
Workflow instruction 1
1
Workflow instruction 2
2
Workflow instruction 3
...
...
k
Workflow instruction k
...
...
n
Workflow instruction n
n+1
Workflow instruction n
Default order of execution
Jumping
End of branching continue at n+1
Branching start at i
i
Workflow instruction
i+1
Workflow instruction
...
...
i+m
Workflow instruction
Workflow execution continues to instruction i when a branch is selected and continues at instruction n+1 when the branch is finished

FIGURE 24

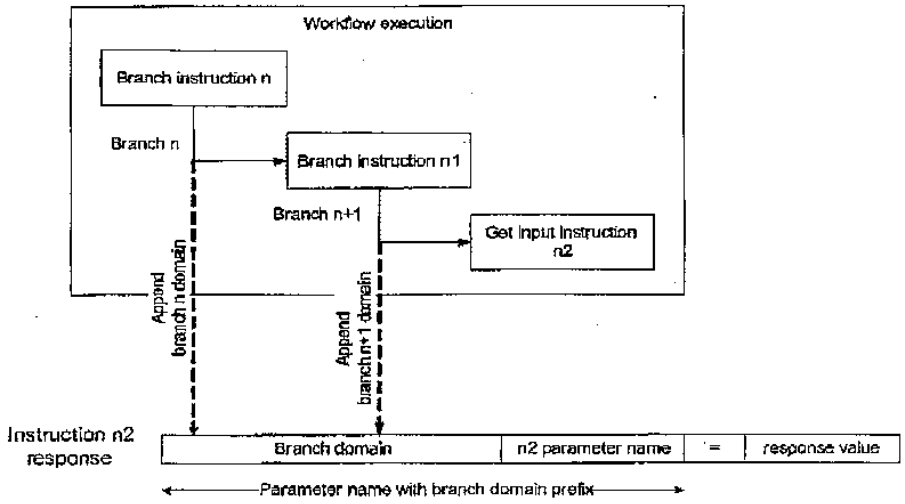

Workflow execution
Branch instruction n
Branch n
Branch instruction n1
Branch n+1
Get input instruction n2
Append branch n domain
Append branch n+1 domain
Instruction n2 response
Branch domain
n2 parameter name
=
response value
Parameter name with branch domain prefix

FIGURE 25

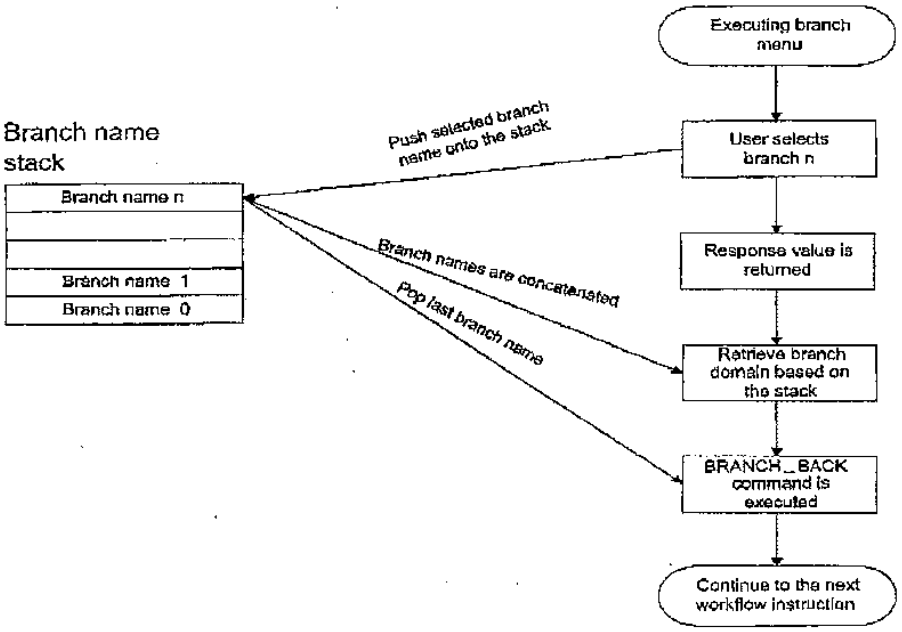

Executing branch menu
User selects branch n
Response value is returned
Retrieve branch domain based on the stack
BRANCH_BACK command is executed
Continue to the next workflow instruction
Push selected branch name onto the stack
Branch names are concatenated
Pop last branch name
Branch name stack
Branch name n
Branch name 1
Branch name 0

FIGURE 26

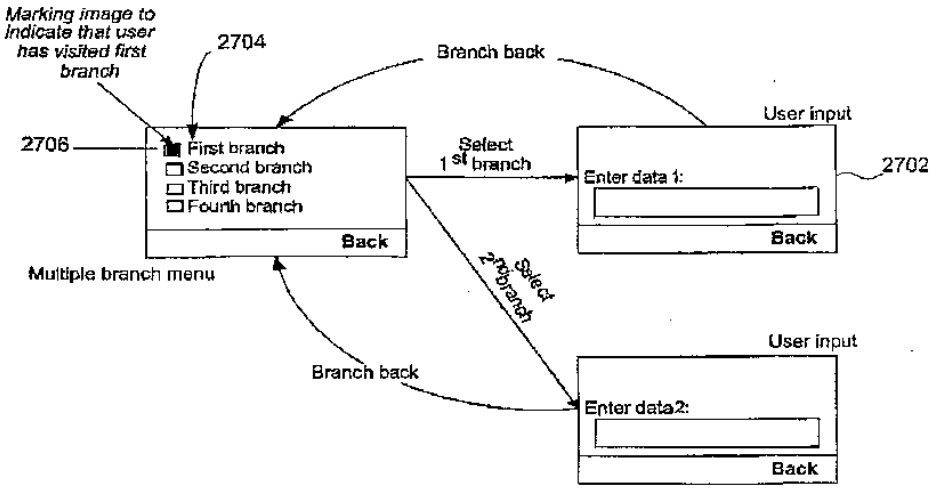


FIGURE 27

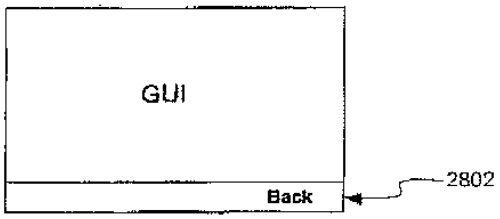


FIGURE 28

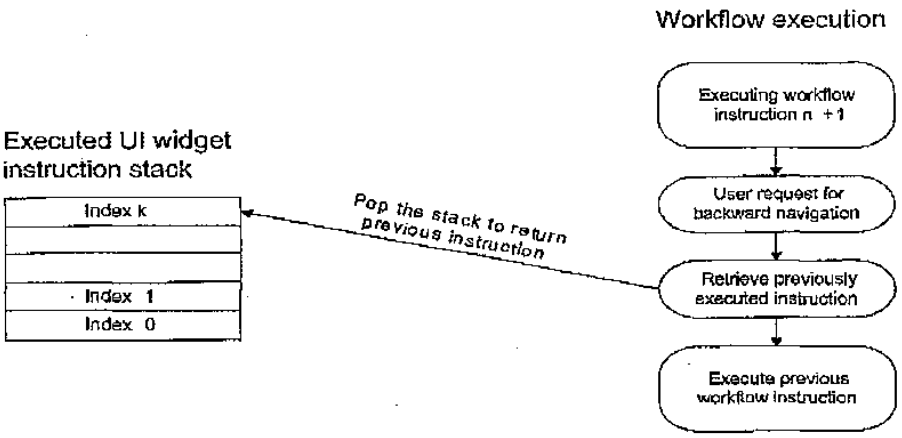

Workflow execution
Executing workflow instruction n +1
User request for backward navigation
Retrieve previously executed instruction
Execute previous workflow instruction
Pop the stack to return previous instruction
Executed UI widget instruction stack
Index k
Index 1
Index 0

FIGURE 29

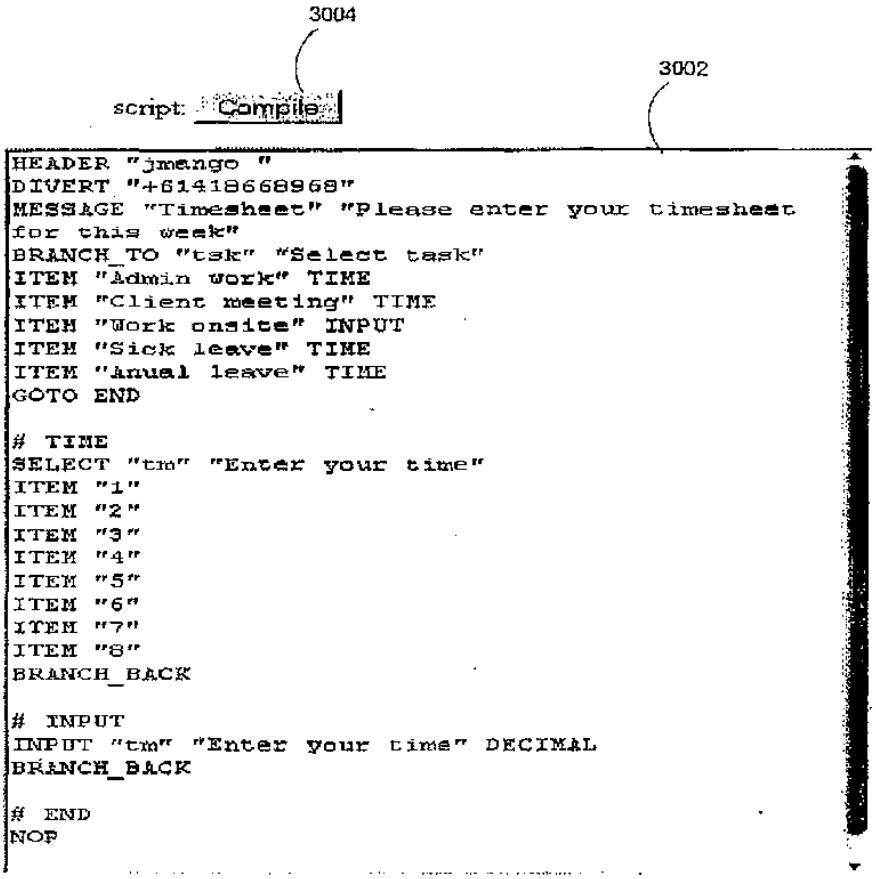


FIGURE 30

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1048 of 1360

```
private string SendWorkflowRequest(string sourceNumber,
    string destinationNumber, string bookingHeader,
    string bookingTitle, string bookingDetails)
{
3102 ---> J2MECommand workflowCommand = new J2MECommand();
3104 ---> if(bookingHeader != null)
        workflowCommand.AddCmdHeader(bookingHeader);

    // Add information message
3106 ---> workflowCommand.AddInfoMessage(bookingTitle, bookingDetails);
    // Add selection menu
3108 ---> workflowCommand.AddSingleMenu("action", "Select", new String[]{"Accept", "Reject"});
    // Add input text box to enter name
3110 ---> workflowCommand.AddUserInputCmd("name", "Enter your name", J2MECommand.InputType.ANY);
    // Add input text box to enter contact number
3112 ---> workflowCommand.AddUserInputCmd("contact", "Contact number", J2MECommand.InputType.PHONENUMBER);
    // Add redirection address where the response message is sent to
3114 ---> workflowCommand.AddRedirectHeader("sms://1991616");

    // Now send the command, in multiple messages if it is neede
3116 ---> IList messages = workflowCommand.BuildCommandMessages(1000);
    string sentIds = "";
    foreach(BinaryMessage binMessage in messages)
    {
3118    sentIds += _messageSender.SendBinaryMessage(sourceNumber, destinationNumber,
                                                    binMessage.UserData, binMessage.DataHeader);
        sentIds += ",";
    }
    return sentIds;
}
```

FIGURE 31

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1049 of 1360

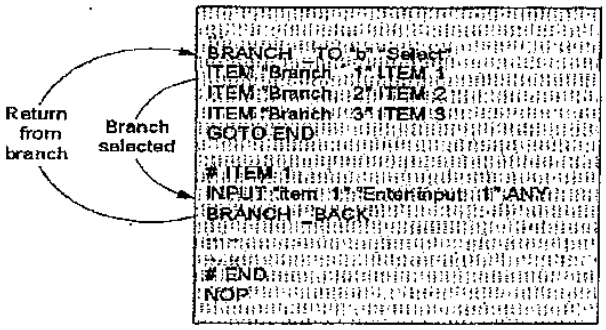


FIGURE 32

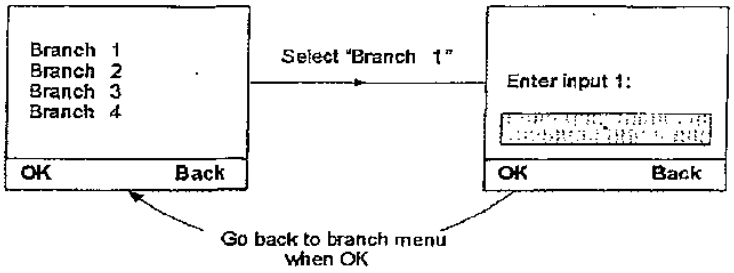


FIGURE 33

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1050 of 1360

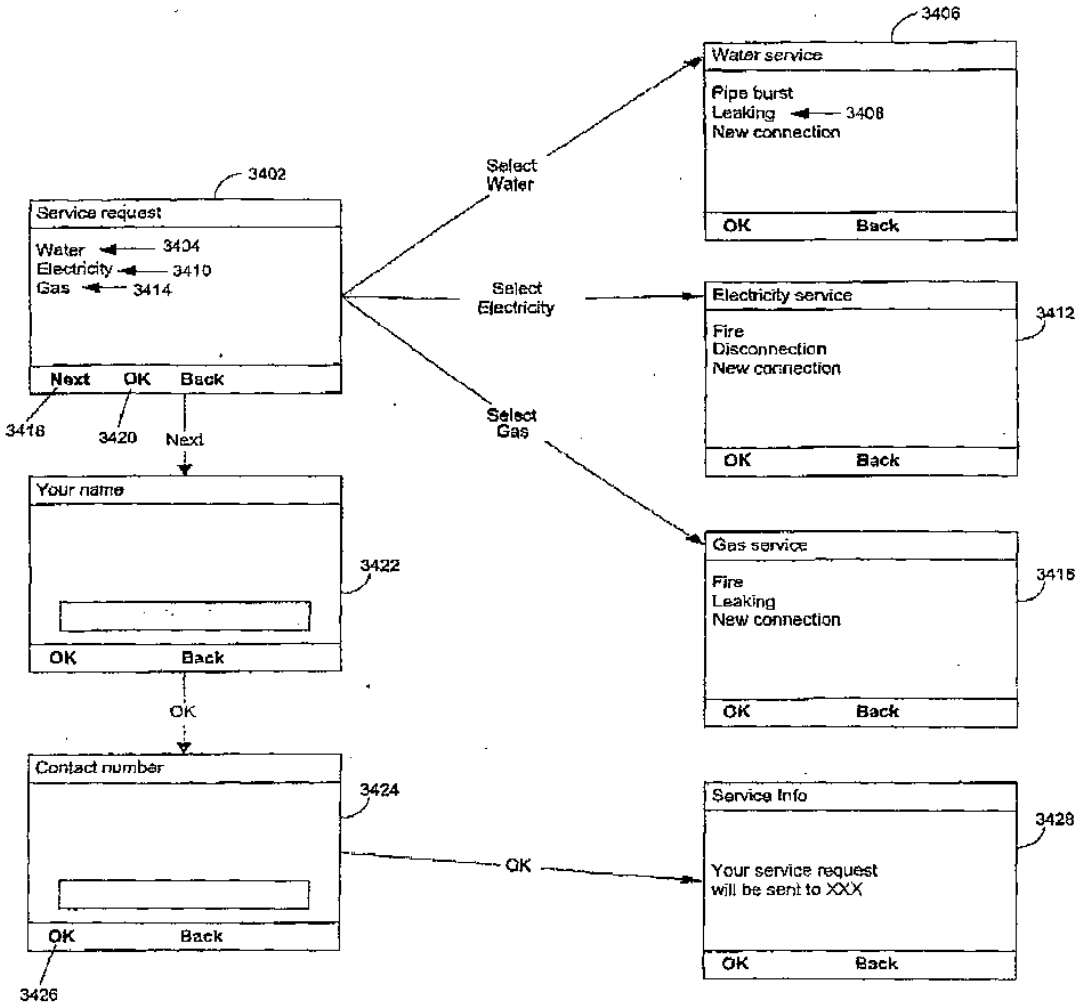

3406
Water service
Pipe burst
Leaking
3408
New connection
OK
Back
3402
Service request
Water
3404
Electricity
3410
Gas
3414
Next
OK
Back
3418
3420
Next
Select Water
Select Electricity
Select Gas
Electricity service
3412
Fire
Disconnection
New connection
OK
Back
Your name
3422
OK
Back
OK
Gas service
3416
Fire
Leaking
New connection
OK
Back
Contact number
3424
OK
Back
3426
OK
Service Info
3428
Your service request will be sent to XXX
OK
Back

FIGURE 34

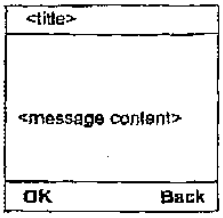


FIGURE 35

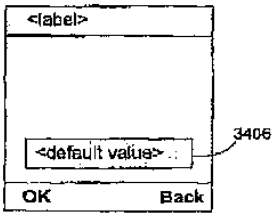


FIGURE 36

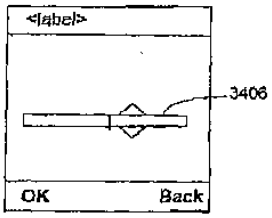


FIGURE 37

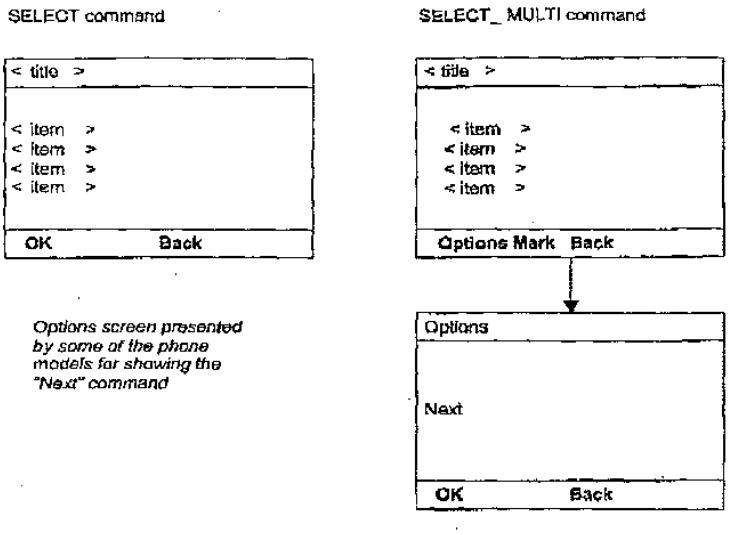

SELECT command
< title >
< item >
< item >
< item >
< item >
OK
Back
Options screen presented by some of the phone models for showing the "Next" command
SELECT_ MULTI command
< title >
< item >
< item >
< item >
< item >
Options Mark Back
Options
Next
OK
Back

FIGURE 38

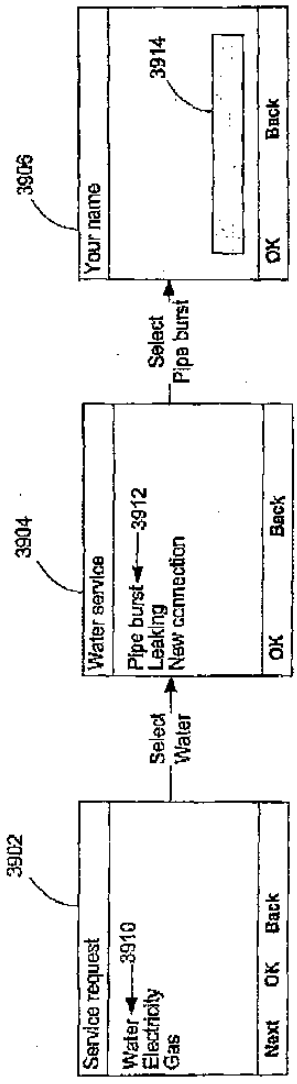


FIGURE 39

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1054 of 1360

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2007/001599

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04Q 7/22 (2006.01) ***H04M 3/493*** (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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)
DWPI & USPTO: Keywords: (interactive, SMS, encryption, compile, header, payload and like terms).

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/0095291 A1 (Cherney) 4 May 2006. See for example the title; abstract; fig 4A-4C, 5 and 7; paras [0013]-[0016], [0033]-[0041], [0057]-[0080] and [0089]-[0140].	1-25
X	EP 1509049 A1 (Accenture Global Services GMBH) 20 August 2003. See for example the abstract; paras [0033]-[0039]; and fig 2 and 5.	1-25
A	US 2002/0073023 A1 (Castro et al.) 13 June 2002.	

☐ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier 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
11 December 2007	20 DEC 2007
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **Malcolm Peh** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : (02) 6283 7914

Form PCT/ISA/210 (second sheet) (April 2007)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1055 of 1360

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU2007/001599

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	2006095291	EP	1836676	US	2006095290	WO	2006050413
EP	1509049	US	2007191032	WO	2005020609		
US	2002073023						

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1056 of 1360

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 2 084 921 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 2008/046161 (Art. 153(3) EPÜ).

International application published by the World Intellectual Property Organization under number:

WO 2008/046161 (Art. 153(3) EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété Intellectuelle sous le numéro:

WO 2008/046161 (art. 153(3) CBE).

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2008 (24.04.2008)

PCT

(10) International Publication Number
WO 2008/046161 A1

(51) International Patent Classification:
H04Q 7/22 (2006.01) *H04M 3/493* (2006.01)

(21) International Application Number:
PCT/AU2007/001599

(22) International Filing Date: 19 October 2007 (19.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2006905829 19 October 2006 (19.10.2006) AU

(71) Applicant *(for all designated States except US)*: **DELOITTE SERVICES PTY LTD** [AU/AU]; Level 1, 225 George Street, Sydney, NSW 2000 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **NGO, Duc, Anh** [/AU]; 2/9 Fabian Court, Maribyrnong, VIC 3032 (AU).

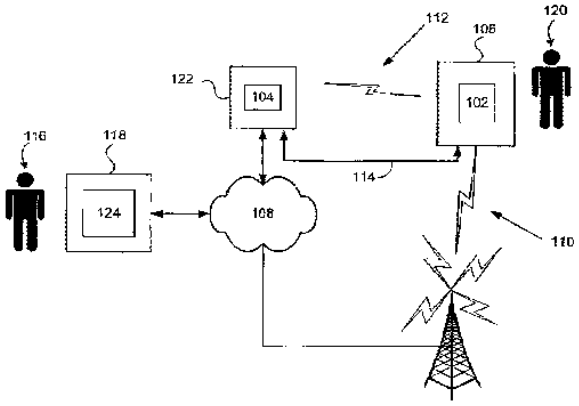
(74) Agent: **BLAKE DAWSON WALDRON PATENT SERVICES**; Level 35, Grosvenor Place, 225 George Street, Sydney, NSW 2000 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) Title: AN INTERACTIVE SYSTEM AND PROCESS



(57) Abstract: A method of delivering an instruction (206) to a mobile user device (106) connected to a network (110) is disclosed. The method comprising the steps of receiving an interactive workflow (202), translating the interactive workflow into the instruction (206) in a form executable by the mobile user device (106), and sending a message (208) including the instruction (206) to the mobile user device (106).

WO 2008/046161 A1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1058 of 1360

AN INTERACTIVE SYSTEM AND PROCESS

FIELD OF THE INVENTION

The present invention relates generally to a method of delivering an instruction to a mobile user device connected to a network.

BACKGROUND

Amongst the wide variety of portable electronic devices available today, mobile phones have become particularly pervasive, with more than double the penetration of the Internet. These devices have rapidly advanced in capability and can do far more than Voice and SMS. Using these capabilities to deliver and execute applications that provide customisable interactivity to mobile phones and other devices is highly desirable but continues to be a challenging endeavour due the varied types of largely incompatible devices and platforms on the market.

Most interactive applications for mobile phones involve either Short Message Service (SMS) or the development of dedicated applications that address specific business requirements. SMS interactivity suffers from poor usability (the user has to be familiar with idiosyncratic commands) and security issues (SMS source addresses can be faked), thus limiting their usage to simple, non-sensitive transactions. Furthermore, an organisation wishing to use SMS to interact with its customers needs to come to some commercial arrangement with the telecommunications provider in order to establish billing procedures and so on. This can be inconvenient for the organisation, and may also be quite expensive, both to set up and also to operate on an on-going basis.

The dedicated applications are an attempt to address these shortcomings by developing programming code that is executed by the mobile device to perform a specific task. This involves significant amounts of time, at least because mobile phones from different manufacturers are not usually binary compatible and cannot execute the same executable applications. Additionally, these applications are limited to the functionality required at the time of development, and thus may not support additions or modifications to that functionality. As can be appreciated, distributing changes to these applications is similarly quite a tedious process, typically requiring the user to manually download and install an updated version of the application on their telephone.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1059 of 1360

SUMMARY OF THE INVENTION

According to one aspect of the invention there is provided a method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

According to another aspect of the invention there is provided a method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

According to yet another aspect of the invention there is provided computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

Preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language. More preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

Preferably the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device. More preferably the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1060 of 1360

step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

Preferably the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

Preferably the step of translating the interactive workflow includes tailoring the instruction to the specification.

Preferably the step of translating the interactive workflow includes tailoring the instruction to a device operating system.

Preferably the step of sending the message includes the step of sending a unique message identifier. More preferably the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

Preferably the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network. More preferably the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS. Alternatively, the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

Preferably the method further comprises the step of the mobile user device receiving the set of instructions and the unique message identifier. More preferably the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

Preferably the method further comprises the step of receiving a response to the instruction from the mobile user device. More preferably the step of receiving a response includes the step of receiving a response identifier from the device. Even more preferably the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1061 of 1360

Preferably the method includes the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow from the external or third party. More preferably the method includes the step of sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow from the external or third party.

Preferably the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface from the external or third party. More preferably the step of receiving a request for an Application Programming Interface is received from the external or third party. Even more preferably the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

Preferably the method also comprises the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

In accordance with the present invention, there is also provided an interactive process executed by a computer system or device, the process including:

receiving one or more SMS messages including instruction data representing one or more instructions for execution on said system or device to determine information;

executing said one or more instructions to determine said information; and

sending one or more SMS messages including response data representing said information.

Advantageously, said information may include system information determined from said system or device and/or user information determined from a user of said system or device.

Preferably, said execution causes generation of an interactive user interface on a display of said system or device, and the process includes receiving response data representing said information from a user of said system or device in response to said interactive display.

Preferably, said one or more instructions are executed by a virtual machine of said system or device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1062 of 1360

The present invention also provides an application component for a system or device, the applicationcomponent including:

a message receiver for processing one or more received SMS messages to generate one or more instructions for execution on said device to determine information;

an execution component for executing said one or more instructions of said application data to determine said information; and

a message sender for generating one or more SMS messages including response data representing said information.

Preferably, the application component further includes a data management component for storing sets of instructions on non-volatile storage means and for retrieving a selected one of the stored sets of instructions for execution.

Preferably, said execution component is adapted to generate an interactive display for a user of said system or device, and to receive response data representing said information from a user of said system or device in response to said interactive display.

The present invention also provides an interactive process for execution by a system or device, including:

receiving message data including header data and encrypted payload data;

selecting one of a plurality of encryption keys on the basis of said header data; and

decrypting said payload data using the selected encryption key.

Preferably, said header data includes index data representing an index for said plurality of encryption keys.

Advantageously, said payload data may represent one or more instructions for execution on said system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions on a remote system or device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1063 of 1360

The present invention also provides an interactive process for execution by a system or device, including:

generating payload data for sending to a remote system or device;

selecting one of a plurality of encryption keys;

encrypting said payload data using the selected encryption key;

generating message data for sending to said remote system or device, said message data including header data and the encrypted payload data, wherein said header data includes data representing an index for said plurality of encryption keys to allow said remote system or device to determine the selected encryption key and thereby to decrypt said payload data.

Advantageously, said payload data may represent one or more instructions for execution on said remote system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions.

Preferably, the process includes generating said plurality of encryption keys and sending said plurality of encryption keys to said remote system or device.

Preferably, the process includes associating said plurality of encryption keys with an identifier of said remote system or device.

The present invention also provides an interactive process, including:

receiving programming instructions for generating an interactive display on a remote system or device;

compiling said programming instructions to generate compiled instruction data;

sending said compiled instruction data to said remote system or device to generate an interactive display on said second remote system or device;

receiving response data representing at least one user response to said interactive display; and

sending response data representing said at least one user response.

The present invention also provides an interactive process, including:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1064 of 1360

receiving workflow instructions from a plurality of entities;

processing said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

sending said interactive applications to said user devices for execution.

Preferably, said interactive applications are sent to said user devices using short message service (SMS).

Preferably, said user devices include mobile telephones.

The present invention also provides an interactive system for managing interaction with users of remote systems and/or devices, the interactive system being adapted to:

receive workflow instructions from a plurality of entities;

process said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

send said interactive applications to said user devices for execution.

The present invention also provides a system having components for executing any one of the above processes.

The present invention also provides a computer-readable storage medium having stored thereon program instructions for executing any one of the above processes.

The present invention also provides an interactive system, including:

a gateway component for processing received workflow data to generate instructions for generating an interactive display on a user device, the gateway component being adapted to send said instructions to said user device for execution; and

an execution component of said user device to receive and execute said instructions to generate said interactive display, to receive response data representing at least one response of said user to said interactive display; and to send said response data to said gateway component.

Preferably, said user device is a mobile telephone.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1065 of 1360

Advantageously, the instructions may be sent to said gateway component in one or more SMS messages.

Advantageously, said user response data may be sent to said user device in one or more SMS messages.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a schematic diagram of a preferred embodiment of an interactive system;

Figure 2 is a schematic diagram of the high level process and data flow of an interactive process of the interactive system;

Figure 3 is a block diagram of a mobile telephone on which a client application of the interactive system is installed;

Figure 4 is a block diagram of the client application of the interactive system;

Figure 5 is a flow diagram of the life cycle of an interactive application generated by the interactive process and system;

Figure 6 is a block diagram of an application gateway of the interactive system;

Figure 7 is a block diagram of a computer system on which the application gateway is installed;

Figure 8 is a schematic diagram of the process and data flow of an opt-in process of the interactive system;

Figure 9 is a schematic diagram illustrating the use of encryption key sets to establish an encrypted communications channel between the client application and the application gateway;

Figure 10 is a schematic diagram of the process and data flow involved in conducting secure communications between the client application and the application gateway;

Figure 11 is a schematic diagram illustrating the default behaviour of the interactive system and process whereby a particular application gateway transmits instructions to a particular client application, and the resulting response data is returned to the same application gateway that sent the instructions;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1066 of 1360

Figure 12 is a schematic diagram similar to that of Figure 11, but illustrating the redirection of response data to a different application gateway from the application gateway that sent the corresponding instructions;

Figure 13 is a schematic diagram illustrating the structure of messages exchanged between the application gateway and the client application;

Figure 14 is a schematic diagram illustrating the structure of payload data of the messages shown in Figure 13;

Figure 15 is a schematic diagram illustrating the structure of each data part of the payload data of Figure 14;

Figure 16 is a schematic diagram illustrating the fifteen different types of instructions supported by the interactive system and process;

Figure 17 is a schematic diagram illustrating the structure of an SMS message generated by the interactive system and process;

Figure 18 is a schematic diagram illustrating how the interactive system uses multiple SMS messages to transmit instructions constituting an application whose length is greater than 133 bytes;

Figure 19 is a flow diagram of an SMS transmission process of the system;

Figure 20 is a flow diagram of an SMS receiving process of the system;

Figure 21 is a flow diagram of an application execution process executed by the execution engine of the system;

Figure 22 is a schematic diagram illustrating the structure of response data sent from the client application to the application gateway;

Figure 23 is a schematic diagram illustrating how the system uses parameter names provided in instructions to label corresponding responses;

Figure 24 is a schematic diagram illustrating execution branching in the client application;

Figure 25 is a schematic diagram illustrating the use of branch domains to label responses having the same parameter name;

Figure 26 is a schematic diagram illustrating the use of a branch name stack to determine control flow;

Figure 27 is a schematic diagram illustrating the user interface components resulting from selecting different branches of an interactive application;

Figure 28 is a schematic diagram illustrating the inclusion of a 'back' button on each user interface display;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1067 of 1360

Figure 29 is a schematic diagram illustrating the use of an executed instruction stack to implement the 'back' button of Figure 28;

Figure 30 is a screen shot of a user interface of the application gateway for entering scripting language instructions and for submitting those instructions to an instruction compiler of the application gateway;

Figure 31 is a source code listing of a function illustrating how the system APIs can be used to send details of a booking to a mobile telephone for display to a user, and to receive the user's response indicating whether they user accepts or rejects the booking;

Figure 32 is a partial listing of a scripting language application, illustrating the use of control flow branches in the scripting language;

Figure 33 is a schematic diagram illustrating the user interface components generated from the scripting language example of Figure 32;

Figure 34 is a schematic diagram illustrating the use of nested user interface displays generated by the system;

Figures 35 and 36 are schematic diagrams illustrating the appearance and structure of general user interface displays generated by the system;

Figure 37 is a schematic illustration of a slider control display generated by the system;

Figure 38 is a schematic diagram illustrating the use of single and multiple selections in user interface displays generated by the system; and

Figure 39 is a schematic diagram illustrating how the branch names of nested menus are used to label parameter data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As shown in Figure 1, an interactive system includes at least one client application 102 and at least one application gateway 104. Each client application 102 is a component of a corresponding user device 106 that can communicate with the at least one application gateway 104 via one or more of a variety of communications means supported by the device 106, preferably including a combination of (i) an IP-based communications network 108 such as the Internet, (ii) a wireless wide-area communications network such as the global system for mobiles (GSM) telephone network, (iii) a local wireless network or link between the device 106 and the at least one application gateway 104, such as an infra-red link, Wi-Fi or Bluetooth network 112, and/or (v) a direct cable connection 114

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1068 of 1360

using a standard communications protocol such as RS-232, universal serial bus (USB), or FireWire (IEEE 1394). The interactive system allows an application developer 116 using a standard computer system 118 to rapidly develop and deploy an interactive workflow or application for execution on one or more user devices 106 in order to interact with the users 120 of those devices 106, and to receive response data representing at least one response of each user 120 to the interactive application.

The interactive workflow or application includes a set of instructions for presenting information to a user 120 of each mobile device 106 in an interactive display or user interface, and for retrieving each user's response(s) to that information. Typically, the information presented to a user 120 will include one or more questions displayed on a display screen of the user's device 106 (and possibly also audio played on a sound transducer of the device 106), and each of the user's responses is provided by the user interacting with one or more user-interface (UI) components or input controls of the interactive display. Each response can be in the form of freeform text typed into a textbox, or the result of the user interacting with another type of input control, such as radio buttons, check boxes, sliders, simple menus, nested menus, and so on. To some extent, these possibilities are determined by the capabilities of the device 106. However, because the workflow supported by the system also includes control flow features similar to those provided by high-level programming languages, the workflow instructions generated by the system are also considered to constitute an interactive software application that is executed on the user device 106.

In the described embodiment, the user device 106 is a mobile telephone, but alternatively could be some other type of portable or handheld device such as a personal data assistant (PDA), and hence is also referred to hereinafter as "the mobile device 106". However, even though the device 106 is described as being "mobile" or "portable", it will be appreciated by those skilled in the art that the systems and processes described herein could alternatively be used in conjunction with other types of devices and systems that need not even be portable. For example, the client application 102 could even be installed on a standard personal computer system (rather than the portable device 106) in order to rapidly develop and deliver interactive applications to a standard personal computer, for example.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1069 of 1360

In the described embodiment, the client application 102 is a software application that is stored on the mobile device 106, either as part of the device manufacturing or configuration prior to sale, or subsequently deployed as required via GPRS, Bluetooth, Infrared or a phone specific channel (*e.g.*, a data cable), allowing it to be installed on a wide variety of different types of device. However, it will be apparent to those skilled in the art that the client application 102 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

Similarly, the application gateway 104 is a software application that is installed on and executed by a standard computer system 122, such an Intel™ IA-32 computer server executing a Windows™ operating system. The computer system 122 includes standard hardware components 702, and software components 704. The hardware components 702 include at least one processor 706, a communications interface (*e.g.*, network interface card) 708, random access memory 710, non-volatile (*e.g.*, hard disk storage) 712, user input device (*e.g.*, keyboard, mouse or other pointing device) 714, and a display adapter and device 716, all interconnected by a system bus 720. The software components 704 include the application gateway 104, and a standard operating system 718 such as Microsoft Windows. Additionally, a third party application 124, shown as being installed on the developer's computer 118, may additionally or alternatively be installed on the same computer system 122 on which the application gateway itself is located 104, as shown. However, although the application gateway 104 is described as being a software application, it will be apparent to those skilled in the art that the application gateway 104 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

The client application 102:

(i) verifies a set of instructions sent by the application gateway 104;

(ii) interprets these instructions;

(iii) interacts with the user device 106 and/or the user 120 in accordance with the set of instructions; and

(iv) sends responses back to the gateway 104 or other computer system or device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1070 of 1360

The application gateway 104 is effectively a backend component that:

(i) maintains a database of user devices of the interactive system (*i.e.*, devices on which the client application 102 has been installed);

(ii) generates and delivers interactive applications to the mobile device 106 via any one of a wide range of communication channels;

(iii) ensures the integrity and authenticity of outgoing and inbound messages to and from the mobile device 106; and

(iv) provides application programming interfaces (APIs) to allow third-party applications 124 to deploy an interactive application to the mobile device 106 and to receive corresponding responses generated by the client application 102 on the mobile device 106.

Figure 2 is a schematic diagram illustrating the high level operation of the interactive process of the system in relation to the various components shown in Figure 1. At step 202, an external or third-party application 204 executing on the developer's computer system 118 (or, alternatively, on the gateway computer system 122) calls an API 616 of the application gateway 104 to describe the workflow that the developers of the device 106 want to deploy. In general, the workflow includes the steps of displaying information to a user, and then retrieving at least one response to that information. For example, a typical workflow might be to display a message on the mobile device 106, ask the user to enter their age, then display another message, and send the age back to the developer. These steps or instructions constitute an interactive application for execution on the mobile device 106.

The workflow defines:

(i) one or more addresses of respective user devices 106;

(ii) the steps to be performed on the one or more user devices 106;

(iii) the address of an alternate gateway server (if any) 104 to which responses are to be sent; if no address is given, then the responses will be sent to the same gateway server 104 that sent the application instructions;

(iv) how the response data returned to the application gateway should be processed (*e.g.*, returned to the developer's application 124, sent to the developer 116 by email, stored in a file, etc.); and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1071 of 1360

(v) the communication method(s) that are to be used to send the instructions to the user device 106 and to receive the corresponding response data.

At step 206, the application gateway 104 transforms the workflow described by the developer into a compressed, encoded, and encrypted format for transmission to the mobile device 106. The application gateway 104 also inserts a unique identifier or ID into the message and stores data associating that ID with the destination (*e.g.*, phone number, or network address) to which the workflow is to be sent.

The application gateway 104 transforms the message so that it can be transmitted via the appropriate communication means. For example, if the message is to be transmitted via SMS, the application gateway 106 splits a large message into smaller messages to comply with the GSM standard. All this is hidden from the developer. At step 208, the application gateway 104 then transmits the message to the device 106 specified by the developer.

At step 210, the client application 102 receives, un-compresses and decrypts the message(s), thereby verifying their integrity. If valid, at step 212 the client application 102 interrupts the user and requests that they complete the workflow. With the user's cooperation, the client application 102 interprets each instruction and performs a corresponding operation *e.g.*, display a message, collect the user's age, etc. that in most cases involves interacting with the user of the device 106.

At the end of the workflow, the client application 102 sends back to the application gateway 104 all the collected response data via the response channel specified in the workflow instructions by the application gateway 104. For example, if the response is to be returned via SMS, a response SMS is sent back to a phone number provided in the initial message(s). The client application 102 also encrypts the response message(s) and includes the unique message ID to ensure authenticity of the response.

When the application gateway 104 receives the response message at step 216, it decrypts the message and determines whether the ID of the message is valid for the phone number it was received from, using the destination and ID association stored previously. If the message is valid, then it is processed as specified by the developer *e.g.*, passes it on to a third-party application, emails the developer, stores it in a file, etc.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1072 of 1360

In addition to the above, the interactive system also provides capabilities for (i) storing (and subsequently updating) a set of instructions as a permanent or semi-permanent application stored on non-volatile storage of the user device 106 for execution at any time; *i.e.*, the application persists on the user's device; (ii) the distribution of encryption keys; and (iii) opt-in mechanisms to ensure that the mobile device 106 is not sent unsolicited applications, *e.g.*, if the application gateway 104 is shared by multiple vendors.

The interactive system and the interactive process executed by the interactive system are described in detail below.

As shown in Figure 3, the mobile device 106 is a standard mobile phone including hardware components 302 and software components 304. The hardware components 302 include a processor 306, read-only memory 308, random-access memory 310, flash memory 312, user interface components including user input components 314 (*e.g.*, microphone, keyboard, and, in some devices, touch-screen), output components 316 (*e.g.*, display screen, speaker), and one or more communications interfaces 318 allowing the device 106 to communicate with a mobile phone network 110, and, in some devices, also Bluetooth and/or Wi-Fi local wireless networks or an infrared link 112. In the preferred case of the mobile device 106 being a telephone, the device 106 also includes a SIM card 320. The software components include an operating system 322 such as the closed, proprietary operating systems installed on mobile telephones sold under brands such as Nokia and Motorola, Java platform Micro-edition (Java ME) 324, and the client application 102. However, if the operating system 322 is a more sophisticated operating system such as Symbian, Linux, Microsoft SmartPhone, PocketPC, Windows CE, or Windows Mobile, that provides sufficiently powerful application programming interfaces (APIs), then the J2ME component 324 can be omitted. As shown in Figure 4, the client application 102 includes a message sender component 402, a message receiver component 404, user interface (UI) widgets 406, a workflow execution engine 408, instant data storage 410, and permanent data storage 412. The client application 102 is a native application that is executed by the mobile device 106. The client application 102 can be installed by any one of a number of means, including WAP push, IP data packets (GPRS or 3G networks), Bluetooth, Infrared, or a phone-specific channel such as a data cable. The

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1073 of 1360

client application 102 can be provided as a preinstalled application on the mobile phone 106 when purchased.

The message sender 608 sends response messages to the application gateway 104 in a format understood by the application gateway 104. It encrypts the message and includes ID provided with the initial application to confirm its authenticity.

The message receiver 606 decrypts and uncompresses instruction sets received from the application gateway 104. It implements message reception via a number of channels, including Bluetooth, Infrared, IP networks (GPRS or 3G), and SMS. The message receiver 606 also invokes the workflow execution engine 408 to process the instruction set.

The UI Widgets 406 are pre-built user interface components that instructions sent by the application gateway 104 can use to interact with the user.

The workflow execution engine 408 is responsible for running and maintaining state for the instructions currently being processed. It associates instructions with UI widgets as well as storing input from the device 106 and its user. It is also responsible for invoking the message sender 402 once the workflow is completed to initiate sending the response to the application gateway 104. The workflow execution can also be invoked by a timer if an instruction asks to be run at a specific time.

The client application 102 can simultaneously receive multiple workflow applications at any one time, and the instant data store 410 is effectively a first-in, first-out queue that stores these applications and processes them one by one until the instant data store 410 is empty.

The interactive system has the ability to make a sequence of instructions persistent on the mobile device 106 as an application. These sequences are identified by a unique label and are stored in the permanent data store 412, being in this embodiment the non-volatile flash memory 312. The application gateway 104 can issue commands to update or delete applications in the permanent data store 412.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1074 of 1360

Figure 5 is a flow diagram illustrating the life cycle of an execution instance of the client application 102 following receipt of an instruction from an application gateway 104. However, the client application 102 can be invoked at step 502 by either a new data event or a timer event. A new data event occurs when the client application 102 is activated by the mobile device 106 when new payload data addressed to the client application 102 is received. Timer events are set by a specific instruction that suspends execution of the instruction to a later date/time. The workflow engine 408 is responsible for scheduling the client application 102 to start and process the instruction set at that date/time.

Once invoked, at step 504 the instruction sequence is retrieved either reading data from the instant data store 410, in the case of a Timer event, or from the input channel in the case of a new data event. If the instruction data is retrieved from the input channel and is encrypted, at step 506 the client application 102 decrypts and verifies it as described below. If the data is valid, the workflow execution begins at step 508.

The workflow execution 508 processes the instructions step by step. This may or may not involve user interactions (as some instructions described in the Appendix can be handled without user interaction). Upon execution of a timer instruction specifying that execution should be postponed to a later time, further execution of instructions of the workflow application is suspended and the instruction set is stored placed in the instant data store 410 pending resumption at the specified time.

Once the workflow execution 508 is complete, the workflow application is removed from the instant data store 410. If the application is marked as persistent, the instruction set is saved to the permanent data store 412. The user can then invoke the instruction set at any time.

At step 510, the information collected by the workflow execution 508 is sent back to the application gateway 104 as response data. The client application 102 encrypts the response data in addition to including the unique message ID that verifies the authenticity of the response data.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1075 of 1360

As shown in Figure 6, the application gateway 104 includes an instruction compiler 602, a key manager 604, a message receiver 606, a message sender 608, an opt-in manager 610, persistent storage 612, and an application programming interface (API) 616.

The instruction compiler 602 translates workflow descriptions received from the developer 116 into a format that is optimized for delivery to and execution by the client application 102. The workflow description is written in a scripting language that is compiled by the instruction compiler 602. The developer can enter the workflow description directly into a text box and submit its contents to the compiler 602. This is typically used to rapidly prototype the look and feel of a workflow application. Alternatively, the workflow description can be submitted by making an API call to the compiler 602 from a high-level programming language such as C#, Java, or TCL, thus providing end-to-end application integration.

The message sender 608 encrypts the workflow instruction set. The encryption relies on requesting the key manager 604 to provide a random index and an encryption key that is specific to a particular user device 106 on which the instructions are to be executed. The index is sent in cleartext to the client application 102, which uses the index to look up the appropriate encryption key to decipher the message. The message sender 608 also generates a unique random identifier for the workflow application. The random identifier is a combination of a random identifier and an identifier of the party who sent the workflow description.

The message sender 608 uses the transport adapter 614 to deliver the actual message(s) containing the workflow application. The message sender 608 first checks with the Opt-in manager 610 to ensure that the client application 102 does not receive unsolicited applications which it has not opted into, as described below.

The transport adapter 614 abstracts the various methods of delivering an instruction set to the client application 102 on the mobile device 106. It uses device capability information stored in the persistent storage 612 to determine the capabilities of the device 106 and hence the best communication channel to deliver the message(s).

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1076 of 1360

The transport adapter 614 provides plug-in support for new channel types dynamically by providing a set of messaging APIs and by allowing dynamic loading of compiled code that implements a new messaging interface. If required, the transport adapter 614 reformats the instruction payload so that it can be delivered via a particular channel. In particular, an application delivered by SMS may have to be divided into two or more smaller messages due to SMS message size limitations.

The key manager 604 is responsible for generating, distributing and managing the encryption keys issued to the portable device 106, as described below. It also provides encryption and decryption facilities for the message sender 608 and the message receiver 606.

The opt-in manager 610 provides an opt-in, opt-out process to allow client applications 102 select the entities they are willing to receive instruction sets from. This is desirable because the application gateway 104 may be shared by multiple parties and the client application 102 will otherwise execute any received instruction set as long as it is valid. The opt-in manager 610 maintains in the persistent data store 612 associations between parties and the phone numbers (or, in the case of devices other than telephones, other form of address or identifier of the destination device) they are allowed to send applications to. The process for creating these associations can be dynamic to allow users to selectively block or allow instructions from particular parties. For example, Figure 8 shows the message flow for an opt-in process.

At step 802, a party uses the external application 124 executing on the computer system 118 to send a workflow description to the application gateway 104, which at step 804 compiles and formats the instructions in preparation for sending them to a client application 102 that has not opted in. At step 806, the message sender 608 first checks whether the client application 102 has opted in. If not, at step 808 it asks the opt-in manager 610 to determine the opt-in status for this party and this user device. At step 810, the opt-in manager 610 sends an opt-in request message to the user, asking whether they agree to receive applications from this party. If the response is yes, at step 812 the opt-in manager 610 stores this information in the persistent data store 612 and then at step 814 instructs the message sender 608 to send the instruction set at step 816. Otherwise, if the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1077 of 1360

response is no, then the message sender 608 fails and notifies the party at step 818 that the user has not opted in.

Alternatively, the opt-in process could be performed manually, for example, by using a form that enables the user to directly add entries to the persistent data store 612. Alternatively, an analogous process could be used to opt-out of receiving applications from a particular party.

The message receiver 606 receives messages from the client application 102 and communicates with the transport adapter 614 to receive responses via any of the supported transport channels and protocols, including GPRS, IP network, Bluetooth, and SMS. For example, the instruction set of the interactive system allows instructions to be received by one physical channel/protocol (*e.g.*, SMS), and a corresponding response to be delivered by another (*e.g.*, Bluetooth).

When a message is received, the message receiver 606 first logs the message for audit purposes. Then it checks the authenticity of the message by deciphering the message using the key manager 604, and examining the unique message ID and the party ID to confirm that they match what was sent out.

Once the message authenticity is established, the message receipt is logged for billing and auditing purposes. Finally, the response message is processed as required by the party. This may include emailing the party; logging it to a file for the party to collect; and/or making a request to a third-party application to process the message. The actual method(s) used to process the response message can be specified when calling the API. If the API call does not specify a processing method, then the response is processed using the default method configured for the corresponding developer, determined when the developer establishes an account with the provider of the interactive system.

The persistent storage 612 is a non-volatile storage component that is used by:

(i) the key manager 604 to store the encryption keys for the various mobile devices;

(ii) the message sender 608 to store the addresses of user devices 106 (*e.g.*, phone numbers in the case of the device 106 being a telephone), together with the

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1078 of 1360

delivery mechanisms that each user device 106 supports. It also stores the identifiers of the messages that have been sent out, for verification purposes;

(iii) the message receiver 606, to store received messages for audit and billing purposes; and

(iv) the opt-in manager 610, to store opt-in data representing each user device 106 and the third party applications that are authorised to send instructions to each user device 106.

Encryption keys

As described above, each installed instance of the client application 102 on a user device 106 is identified by a unique client identifier (also referred to herein as the client ID number) that is associated with its phone number. When a client application 102 is first installed on a mobile device 106, a number of private encryption keys are generated and associated with the client ID.

As shown schematically in Figure 9, these encryption keys are then used by the client application 102 to authenticate the payload data and to encrypt the response data. On each payload or response data packet or message, the index of the appropriate encryption key is indicated in the header of the payload.

Figure 10 is a schematic diagram illustrating the message and process flow for generating and updating encryption keys on a client application 102 and an application gateway or backend system 104. The process is initiated by the client application 102 making a secure communication activation request to the application gateway 104 at step 902. In response, the application gateway 104 generates and stores a set of private encryption keys, and associates these with the client ID at step 904. At step 906, the application gateway 104 sends these newly generated private keys to the client application 102. The client application 102 stores the received private keys on the persistent storage 412 at step 908, and returns an acknowledgement to the application gateway 104 at 910, confirming that the private keys have been stored (or updated if the keys had been previously stored). This completes the generation/update steps and secure communication is activated at step 912. This involves encrypting a message payload using one of the private encryption keys, which can be selected at random or on any other basis at step 914. At step 916, the secured payload encrypted with the selected key is sent to the client application 102, together with

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1079 of 1360

a message header specifying the index of the selected encryption key. At step 918, the client application uses the encryption key index indicated in the header to select the appropriate private key, and uses that key to decrypt the payload data at step 918. After performing the application instructions specified by the payload, the client application 102 then encrypts the response at step 920. The response can be encrypted using the same key, as shown in Figure 10, or any other of the stored keys. The secured response is sent to the application gateway 104 at step 922, and the response is decrypted using the appropriate response key at step 924. As will be understood by those skilled in the art, the use of private encryption keys greatly improves the security of communication, and the use of a set of encryption keys, rather than a single key, further increases this security.

When sending a response message, the client application 102 uses the source address of the corresponding payload data by default. This effectively provides multiple client-server communication channels in between the backend 104 and the client application 102. For example, Figure 11 shows an arrangement whereby two instances of the client application 102, a first instance 1002 and a second instance 1004, are in communication with two instances 1006, 1008 of the application gateway 104, via a wireless communications network 110. A message 1010 sent from the first backend system 1008 to the second client application 1004 includes an address 1012 of the first backend system 1008 in the header of the message 1010 so that when the client application 1004 sends the corresponding response 1014, it is addressed to the first backend system 1008.

In contrast, Figure 12 shows the same arrangement whereby a message 1102 also includes the address 1012 of the first backend system 1008. However, workflow instructions contained in the payload data can alter this default behaviour by redirecting the response to another backend server instead. This mechanism is activated by a DIVERT command in the payload data, described further in the Appendix. Specifically, in this message 1102 the payload 1104 includes a divert instruction with the address of the second backend system 1006. Consequently, after the second client application 1004 executes this instruction, the response 1106 is addressed to the second backend system 1006, rather than the first backend system 1008 that originated the message 1102 containing the instructions. Because the second backend system 1006 does not have direct access to the client ID and message ID pair, or the encryption keys for the client application 102, the second backend system 1006 calls an API of the first backend system 1008 to check the integrity and

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1080 of 1360

authenticity of the response data. If the payload was encrypted, then the first backend system 1008 decrypts the payload and sends it back to the second backend system 1006 over a secured communications channel (using SSL, for example). In an alternative embodiment, the encryption keys are stored in a centralised component of the interactive system, and all encryptions and decryptions are performed in this manner.

Communication data payload

The payload exchanged between the client application 102 and the backend system 104 is binary data - a sequence of bytes. The communication channel for this payload can include SMS or Cell Broadcast Service (CBS) messages; IP/TCP data packets (over GPRS, 3G or other type of data networks); and/or Bluetooth data packets.

As shown in Figure 13, each data payload is prefixed with a header 1204 which indicates whether the payload is encrypted with an encryption key. The header data contains the index of the encryption key stored in the client application key-storage, thereby allowing the client application 102 to decrypt the payload data.

As shown in Figure 14, plain payload data (either unencrypted or after being decrypted) contains a series of variable-length data parts that instruct the dynamic workflow execution engine 508 of the client application 102 to construct the user UI workflow.

As shown in Figure 15, each data part includes type 1402 and length 1404 data fields, followed by the actual instruction data 1406. The type field is a single octet or byte that defines the type of workflow instruction that follows. The length indicates the number of octets or bytes of the instructor data 1406.

As described above, the interactive system is able to use one or more of a variety of different communication channels for sending and receiving messages and responses between the application gateway 104 and the client application 102. For most of these different communication channels, the communication itself is straightforward, using the standard methods and libraries available and known to those skilled in the art. However, the interactive system supports message and response delivery via the short message service, or SMS. SMS is defined in the GSM 03.40 specification, which defines an upper limit on the size of each SMS message. Specifically, each SMS message is capable of

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1081 of 1360

containing up to 140 bytes of data, equivalent to 160 ASCII characters when using 7-bit encoding, as shown in Figure 17. The interactive system sends SMS messages including 8-bit (binary) data and including a 7-byte user data header or UDH 1702, as described in the GSM 03.40 specification. The UDH 1702 consists of a length field or UDHL 1704, specifying the length of User Data Header in bytes as specified in GSM 03.40, and a 6-byte User Data Header field 1706 specifying the destination address of the payload data 1708.

The UDH data 1702 - specifying the destination of the binary message - is interpreted by the mobile device to deliver the payload data to the client application 102. Excluding UDH data 1702, each SMS message is capable of carrying 133 bytes of payload data 1708.

If the payload data exceeds this length, the payload data is sent in two or more SMS messages 1804, each message containing up to 127 bytes of payload data 1806, 1808, as shown in Figure 18. These SMS messages 1804 have a section of User Data Header indicating that they all belong to a concatenated message, as described in the GMS 03.40 specification. A byte padding mechanism is used by the backend system 104 and the client application 102 when the payload is sent in multiple SMS messages. In this mechanism, a padding or termination byte 1810 with value 0xFF is appended to the end of each payload data fragment 1806, 1808 when sent out from the backend system 104. The client application 102 removes these padding bytes 1810, which appear as stuffed bytes 1812 in the concatenated payload data before passing the payload data 1814 to the workflow execution engine 408. The byte padding mechanism is used to eliminate problems found in a number of mobile phone models that strip out the last byte of every concatenated data fragment.

The instruction compiler 602 creates the payload data from the compiler output to generate binary SMS messages. Construction of binary messages includes splitting the payload data 1802 into multiple SMS messages 1804 if the data length exceeds the single message capacity of 133 bytes. Figure 19 is a flow diagram showing the steps involved in this process.

As shown in Figure 19, when delivering a message or a response via SMS, at step 1902 a check is performed to determine whether the size of the payload data exceeds 133 bytes. If

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1082 of 1360

not, then at step 1904 a user data header is added, and a single SMS message is composed and sent at step 1906. Alternatively, if the payload length does exceed the maximum size that can be sent in a single SMS message, then at step 1908 a concatenated message identifier is generated, and at step 1910 the number of concatenated messages that are required to accommodate the payload data is determined. Then, a processing loop consisting of steps 1912 to 1920 composes the appropriate number of SMS messages as follows. At step 1912, the next payload portion is selected and copied to the payload of the current SMS message. At step 1914 a user data header is added, including the identifier indicating that the SMS message is part of this SMS message set. At step 1916, a padding or termination byte is appended to the payload data, as described above. Finally, at step 1918 the resulting SMS message is sent. These steps 1912 to 1918 are repeated until the test at step 1920 determines that the last part of the payload data has been sent, and the process then terminates.

Removal of stuffed bytes in the payload data is handled by the client application 102 by searching for the specific stuffed byte octet value (0xFF in this embodiment) and removing it from the payload data, as shown in Figure 20.

Figure 16 is a schematic diagram showing the fifteen different instructions supported by the interactive system, showing the respective type bytes identifying each instruction type, and the structure of the corresponding instruction parameters. Further details on the various instructions are provided in the Appendix.

Dynamic workflow execution engine

The client application 102 presents to the user a number of user interface (UI) widgets 406 as well as executing user-invisible routines. This allows the client application 102 to display information as well as capture device information and/or user inputs.

The UI widgets 406 typically include the following type of user interface components and controls:

(i) Message screen: to show textual information;

(ii) Selection menu: to ask for the user's selection of one of a number of defined choices (*i.e.*, radio buttons);

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1083 of 1360

(iii) Multiple choices: to ask for user's one or more choices (*i.e.*, check boxes);

(iv) Textual input: to retrieve free form text input from the user (textbox);

(v) Numeric or date inputs: to retrieve user input data, restricted by type; and

(vi) Widgets displayed when branching and jumping amongst execution steps.

However, this list of UI widgets 406 and their actual screen layouts can vary depending on the platform (*i.e.*, on each combination of device hardware and operating system software) on which the client application 102 is installed.

The client application 102 implements a workflow execution process 2100, as shown in Figure 21, on each invocation to execute a workflow application. The workflow execution process 2100 begins after the client application 102 is invoked at step 2102, and a test is performed at step 2104 to determine whether the invocation has resulted from the receipt of new payload data from the application gateway 104. If so, then at step 2105 the new payload instructions are retrieved, and then parsed at step 2110. Otherwise, if the invocation was not due to the receipt of new payload data, then a test is performed at step 2106 to determine whether instructions are contained in the instant data storage 410. If so, then the instructions are retrieved from the instant data storage 410 at step 2108, and then parsed at step 2110. Otherwise, another test is performed at step 2132 to determine whether any sets of instructions have been saved as applications in the permanent data storage 412. If not, then at step 2134 an information message is displayed to the user indicating that there are no applications (instant or permanent) in the queue. Once the user acknowledges this information message, or when a corresponding timeout period has elapsed, the client application 102 is terminated. Alternatively, if the permanent data storage 412 contains one or more permanently stored sets of instructions (*i.e.*, applications), then at step 2136 these are displayed to the user, and the process 400 pauses at step 2137, awaiting the user's selection of one of these, or selection of a quit option. If, at step 2138, it is determined that the user has selected the quit option, then the client application 102 terminates. Otherwise, the user has selected a permanently stored set of instructions, and these are retrieved at step 2140, and then parsed at step 2110.

Following parsing of the workflow instructions at step 2110, the first or next workflow instruction is read at step 2112, and executed at step 2114. If it is determined at step 2116 that the instruction is a UI instruction, then the process waits to receive user input at step 2118. Once the user's response has been received, at step 2120 the UI widget

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1084 of 1360

displayed on the screen of the device 106 is removed, and any user input is stored at step 2122. At step 2124, a test is performed to determine whether the instruction was the last in the workflow. If not, then the process loops back to step 2112. Otherwise, once all of the instructions have been executed, then a response message is composed at step 2126, and sent at step 2128. If the workflow instructions executed are stored in the instant data storage 410, then they are deleted at step 2130. This terminates the workflow execution process 2100.

Parsing workflow instructions and response data

The workflow execution engine 408 of the client application 102 interprets the payload data parts and generates the dynamic UI workflow accordingly.

The data parts from the payload data are indexed sequentially when read by the workflow execution engine 408, and, this is also the default order of workflow execution 508. As shown in Figure 22, the response data includes each response in the same order as the corresponding instructions were received and executed. When a workflow instruction is executed and response data is to be retrieved, a parameter name is included in the instruction data, and the user response or system response is associated with this parameter in the response. All the instruction responses are included in the response data when the workflow is completed, as shown in Figure 23.

Jumping and Branching in the workflow

The workflow execution engine 408 provides a mechanism to allow branching and jumping in the sequence of instructions.

Branching

Because an instruction might be involved in different branches through out the workflow, the workflow execution engine 408 differentiates the instruction response data for different branches using branch domains. A branch domain specifies the address of a workflow instruction in the workflow tree. When setting the instruction response data, the response parameter name is prefixed with the corresponding branch domain, separated by a period character. For example, an instruction to retrieve user input for a numeric-valued parameter with the parameter name "number" could be called from two different branch menus: one named "First branch", and the other named "Second branch". In both of these

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1085 of 1360

cases, the instruction returns the same parameter name "number" but with different values. The workflow execution engine 408 associates a branch domain with the parameter name to differentiate the two response values. Thus in this example, the first value is returned as "First branch.number = xxx" and the second value as "Second branch.number = yyy", where "xxx" and "yyy" represent the actual values entered by the user. Figure 25 shows a more complex example where menu selections are nested.

Additionally, the branch domain is appended with a branch name on selection of a branch menu. For example, in an application with two nested branch menus 3902 "Service Request" and 3904 "Water Service" as shown in Figure 39, when the user selects item 3910 "Water" in menu 3902, and then selects item 3912 "Pipe Burst" in the subsequent branch menu 3904 "Water Service", and then fills out 3914 with "John Doe" in the text input screen 3906 "Your name", the client application 102 will internally send the response as "Water.Pipe burst.name=John Doe". When the BRANCH_BACK command is executed, the previous branch name is removed. The workflow execution engine 408 uses a branch name stack to maintain the order of branch names as they are selected.

For usability reasons, when working with a multiple branch menu, it is important for the user to know whether or not a branch has already been visited by the user. To this end, the workflow execution engine 408 indicates visited branch menu items by displaying an image adjacent to those branches to indicate that they have already been visited by the user. For example, as shown in Figure 27.

When the user has visited user input screen 2702 to enter data 1, an image icon 2706 is displayed adjacent to the first branch menu item 2704 is marked with distinct. This allows user to visually distinguish those parts of the workflow that have been visited from those parts that have not been visited. Alternatively, the visited branches could be displayed in a different colour, as used by web browsers to indicate that a hyperlink has been visited.

Backward navigation

As shown in Figure 28, all of the user interface screens include a "Back" navigation button 2802 to allow the user to return to the previous screen within the workflow. The position of this back button can change depending on the specific mobile device platform executing

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1086 of 1360

the client application 102. As shown in Figure 29, the workflow execution engine 408 maintains an ordered list or stack of instructions that cause a change in the screen or display, and selection of the "Back" button causes the execution to return to the previous instruction.

Sending a workflow description to the Instruction Compiler

As described above, a developer 116 can send a workflow description to the instruction compiler 602 of the application gateway 104 by submitting programming instructions written in the programming language supported by the instruction compiler 602, using a hypertext transport protocol (HTTP) interface of the instruction compiler 602. For example, Figure 30 is a screenshot of an HTML webpage generated by the application gateway 104. The webpage includes a scrollable text box 3002 into which the developer 118 can directly enter commands in the scripting language, and a compile button 3004 which, when pressed, submits the text in the scrollable text box 3002 to the instruction compiler 602 for compilation.

The scripting language of the interactive systems is a high level language for describing the workflow of an interactive application. It is similar in vein to BASIC and can be learnt quickly by a programmer who has a basic knowledge in programming.

Alternatively, a workflow description can be sent to the instruction compiler 602 by invoking API calls to the application gateway API 616. For example, Figure 31 shows a source code listing of a J2ME function `SendWorkflowRequest` that is used to generate and send workflow instructions to the mobile telephone 106. In this example, the workflow instructions are to display booking details to the user 120 and then retrieve the user's response indicating whether the user 120 accepts or rejects the booking, together with the user's name and telephone number. The workflow API is first initialised by creating (at 3102) a new J2ME Command() object named `WorkflowCommand`. A workflow header, as described below, is then added at 3104. Workflow instructions are then added in the order of desired execution by calling APIs that are provided as methods of the `WorkflowCommand` object. Each type of workflow instruction is added by calling a corresponding API function with a set of parameters. For example, the object method `AddInfoMessage` is used (at 3106) to add an instruction that displays a screen of

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1087 of 1360

information to the user. The first argument to this method provides a title for the screen, and the second argument provides the actual text information that is displayed. Similarly, the method `AddSingleMenu` adds (at 3108) an instruction that displays a single-level menu (*i.e.*, radio buttons) to the user, allowing the user to select one item from a list of items provided as a parameter to the method. In this example, the two items are displayed as "Accept", and "Reject", and the user's response indicates whether the user 120 accepts or rejects the booking.

The method `AddUserInputCmd (at 3110 and 3112)` displays a text string to the user, together with a textbox, prompting the user to enter an appropriate input value. The first parameter to this function finds the name of the parameter that will be associated with the returned input value. The second argument provides a string that is displayed to the user, and a third argument allows the developer to restrict the type of input; for example, to a phone number, email address, and so on.

Finally, the `AddRedirectHeader` method (at 3114) defines a return address or phone number to which the response will be redirected, as described above. The communication channel to be used (*e.g.*, whether by SMS, IP network, Bluetooth, etc) is also specified in the header.

Once the workflow instructions are added, the workflow API is called again (at 3116) to compile the instructions and build the payload data to be sent to the client application. The workflow API is called as many times as needed (at 3118) to send multiple messages if required.

Scripting Language Overview

- Instructions are written line by line.
- Comment lines start with //
- Label lines start with #
- String parameters are delimited by double quote characters ""

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1088 of 1360

Workflow-programming Structure

Commands are processed sequentially line by line. Three instructions are provided to create tree structures of the workflow: BRANCH_TO, BRANCH_BACK, and GOTO. BRANCH_TO and BRANCH_BACK are used in combination to create a subroutine for the compiled program. GOTO is a jump instruction that allows program execution to jump to a specified line in the script. Comment and blank lines are ignored by the instruction compiler 602.

Command line syntax

A command is a line in the script which has the following structure:

<Command Name> <String Parameter> <String Parameter> <Label>

Where:

- <Command Name> is a command.
- <String Parameter> is a qualified string value, *i.e.*, delimited by double quote characters. For example, "User name" is a string parameter. There can be more than one string parameter in each command.
- <Label> is the name of the label that is associated with the command. Labels can only be used with the GOTO command and the ITEM command when used in conjunction with BRANCH_TO command.

Comment

There is no block comment in the language. Comment lines are lines that start with // (two forward slash characters followed by a space character).

Example:

// this is a comment line

Label

A label is a way to mark a line number so that it can be referred to in GOTO and BRANCH_TO 's ITEM commands. A label line starts with # (hash) character, followed by a space character. The label name is the next word from the # character.

Example:

For label START, the line looks like this:

START

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1089 of 1360

The label name is mapped to the index (*i.e.*, relative position in the script) of the command immediately following the label line.

Labels in a script must be unique, a compile error occurs if a duplicate label is detected. All labels are parsed in the first pass of the compiler, building a mapping of label and command index to be used in the second pass.

Backward navigation

As described above, a "Back" navigation button is attached to all displayed screens by default. This button allows backward navigation of the workflow executed on the user device 106. On most mobile phone platforms, this "Back" button is mapped to the right action key. However, this can change depending on the type of phone.

Tree navigation

A combination of the BRANCH_TO command, labels, and the BRANCH_BACK command allows the workflow to support a tree like execution structure, as shown in the source code listing of Figure 32 and the resulting display screens of Figure 33. A detailed description is provided below. When a user is navigating thought workflow screens, the state of each screen (item selection and user inputs) is not remembered.

Example

The following is a source code listing that is used to generate an interactive application for execution on a user device such as the mobile telephone 106. The source code defines a workflow that allows the user 120 of the mobile telephone 106 to generate a service request for water, electricity, and/or gas services. The listing is arranged in four groups of commands or paragraphs under respective labels. The first paragraph, labeled START, results in display of a main screen 3402, as shown in Figure 34. The BRANCH_TO command has two parameters. The first, "serv" defines a branch name for this branch, and the second parameter, "Service Request" defines the title that is displayed at the top of the main screen 3402. The subsequent three commands define items that can be selected by the user to invoke corresponding workflow branches. For example, the first ITEM command has two parameters. The first parameter, "Water", defines the text 3404 that is displayed on the main screen 3402, and that can be selected to invoke the corresponding workflow branch. The second parameter, in this case "WATER", is a label of the corresponding

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1090 of 1360

workflow branch, in this case referring to the second group or paragraph of commands grouped under that label. Thus if the user navigates the main screen 3402 to select the first item 3404, the workflow jumps to the SELECT ITEMS, causing display of a water service selection screen 3406. In this case, the three items are simply menu selections (rather than workflow branches), and thus selection of any one of these items causes the appropriate parameter, in this case named "water" to be assigned a value defined with the corresponding item. For example, if the user selects the second item, "Leaking" 3408, then the parameter "water" is assigned the value "Leaking". Once this item has been selected, the workflow proceeds to the following command, which in this case is the BRANCH_BACK command, which returns control to the main screen 3402.

In this manner, the user can select the Electricity item 3410 to branch to the ELECTRICITY workflow, resulting in display of a Electricity service screen 3412. Similarly, the user can select the "Gas" request item 3414 to cause a Gas service screen 3416 to be displayed. Once the user is satisfied with the service requests thus defined, selection of the Next button 3418, or the OK button 3420 causes execution to continue to execute in this example the command "GOTO CONTACTS", which causes the workflow to jump to the command following the CONTACTS label, being in this case an INPUT command displaying a name input screen 3422, and subsequently a Contact number screen 3424. Once the OK button 3426 on the Contact numbers screen 3424 has been selected, a MESSAGE command causes display of a Service Info screen 3428 providing informational feedback to the user, in this case confirming that the service request will or has been sent to an appropriate party for processing the user's request.

```
// Start of program
#START
BRANCH_TO    "serv" "Service Request"
ITEM         "Water" WATER
ITEM         "Electricity" ELECTRICITY
ITEM         "Gas" GAS
GOTO         CONTACTS

#WATER
SELECT       "water" "Water service"
```

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1091 of 1360

```
ITEM            "Pipe Burst"
ITEM            "Leaking"
ITEM            "New connection"
BRANCH_BACK

# ELECTRICITY
SELECT      "elect" "Electricity service"
ITEM            "Fire"
ITEM            "New connection"
ITEM            "Disconnection"
BRANCH_BACK

# GAS
SELECT      "gas" "Gas service"
ITEM            "Leaking"
ITEM            "New connection"
ITEM            "Fire"
BRANCH_BACK

// This is like a subroutine
# CONTACTS
INPUT           "name" "Your Name" ANY
INPUT           "phone" "Contact Number" NUMERIC
// message is sent here
//# END
MESSAGE     "Service Info" "Your request will be sent to XXXX"
```

Script commands and syntax

HEADER command

The HEADER command is used to include a specified piece of text at the beginning of the response message when the workflow has been executed. This command is invisible to the

user of the user device. This command is used as a context identifier for server-client conversation.

There can be multiple header commands in the script. When using the HEADER command in conjunction with the BRANCH_TO command, different response message prefixes can be set, based on the user's selection.

Syntax

HEADER <header>

- <header> is a string parameter to be prepended to the response text message.

Example

HEADER "timesheet"

Response

<header> is attached to the beginning of the response message. If there are multiple headers to be included in the response message, the response headers are prepended based on their execution order in the workflow.

DIVERT command

The DIVERT command is used to redirect a response message to a telephone number or address different from that of the source of the original instructions. Normally, the response message is sent back to the source address of the payload, but the response message can be sent back to another number instead by including a DIVERT command in the workflow. This command is invisible to the user. There can be multiple DIVERT commands in the script, but the last one that is executed in the workflow takes effect. When combining this command with the BRANCH_TO Command, the workflow can send a response message to a source number selected by the user.

Syntax

DIVERT <address>

- <address> is a string parameter representing the mobile number of the redirected address.

Example

DIVERT "+61418366896"

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1093 of 1360

MESSAGE command

MESSAGE command shows a message with a title and message content to the user.

Syntax

MESSAGE <title> <message content>

- <title> is a string parameter for of the title of the message to be displayed.
- <message content> is a string parameter.

The end result is display of a screen as shown in Figure 35.

Example

MESSAGE "Hello" "Hello world"

Response

This GUI screen does not collect any user input and no response data is associated with it.

INPUT command

This command displays a GUI screen with a text input box 3602 to the user to retrieve user inputs, as shown in Figure 36. A parameter name is provided in the command to set the name of the user input data when included in the response message. A default input value can be provided as an input parameter. If desired, the user input data can be restricted to a certain types such as numeric, decimal or a phone number. However, the implementation of user input restriction depends on the capability of the user device executing the client application 102.

Syntax

INPUT<return parameter> <label> <type> <default value>

- <return parameter> is a string parameter for the name of the entered value to be set in the return message.
- <label> is the title of the input text box
- <type> is the type of the input to be captured, these types are available:
  - ANY
  - EMAILADDR
  - NUMERIC

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1094 of 1360

- PHONENUMBER
- URL
- DECIMAL

- <default value> is an optional string parameter to be set to the input text box when the screen is visible to the user. If omitted, the default value of the input text box is left empty.

Response

User input data is included in a response message associated with a parameter name specified in the corresponding instruction. If the INPUT command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<return parameter>=<value> (without domain path)

<domain path>.<return parameter>=<value>

Where:

- <value> is a string value that user enters. This can be an empty value.
- <domain path> is the path of branches that lead to this INPUT command in the workflow.

GAUSS command

This command results in the display of an interactive screen having a slider or "gauss" control 3702 to prompt the user to provide corresponding response data, as shown in Figure 37. The user is able to slide the slider control from a minimum value to a maximum value specified on the command line. The resulting data is included in the response message associated with the parameter name given.

Syntax

GAUSS <parameter name> <minimum value> <maximum value> <default value>

- <parameter name> is a string parameter for the name of the gauss value to be set in the return message.
- <minimum value> is the minimum value the user can select.
- <maximum value> is the maximum value the user can select

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1095 of 1360

- <default value> is the default value if the user does not select any value. This parameter is optional so if it is not present, the default value is empty.

Example

GAUSS "temper" "1" "10" "5"

Response

If this command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<parameter name>=<value> (without domain path)

<domain path>.<parameter name>=<value>

GOTO command

This command allows the workflow execution engine 406 to jump to a specific workflow instruction, rather than proceed to the next instruction in sequence. A parameter of this command is the label of the instruction for the workflow execution to be directed to. There is no user screen or response data associated with this instruction.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1096 of 1360

Syntax

GOTO <label>

- <label> is the label name indicating the index the command that the workflow execution jumps to after executing this command.

Example

....

GOTO Hello // The program jumps to message hello world after executing this command.

...

...

Hello

MESSAGE "Hello" "Hello world"

...

SELECT, SELECT_MULTI command

As shown in Figure 38, these commands display a screen with a list of items to select from. The SELECT command allows single item selection, and the SELECT_MULTI command allows multiple item selection screen. The user selection is included in the response message identified by the parameter name. In case of multiple selection list, the selected values are separated by a delimiter character in the response value data.

Syntax

SELECT or SELECT_MULTI command is followed by ITEM definitions (one per line).

SELECT <parameter name> <title>
ITEM <item name>
ITEM <item name>
ITEM <item name>

SELECT_MULTI < parameter name> <title>
ITEM <item name>

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1097 of 1360

ITEM <item name>
ITEM <item name>

Where:

- < parameter name > is a string parameter specifying the return parameter id for the SELECT screen.
- <title> is a string parameter specifying the title of the screen.
- <item name> is a string parameter specifying the item to be displayed on the screen.

Example

```
// This example allows the mobile user to select one of the option listed
SELECT "tsk" "Select task"
ITEM "Administration"
ITEM "Service desk"
ITEM "Client meeting"

// This example allows mobile user to select one or many of user names in the list
SELECT_MULTI "name" "Select users"
ITEM "User 1"
ITEM "User 2"
ITEM "User 3"
```

For multiple select command, each of the items in the select list is displayed adjacent to an icon that indicates whether or not the item has been selected by the user. On most mobile devices, a "Mark" button is displayed to allow user to mark the selection of the highlighted item. A "Next" button is also attached to this screen to allow the user to navigate to the next workflow instruction. On some mobile device platforms, the Next button is mapped directly to one of the mobile phone buttons.

Response

SELECT command:

<parameter name>=<item>

SELECT_MULTI command:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1098 of 1360

< parameter name >=<item>;<item>;<item>

Where:

- <item> is the item name as selected

The multiple select response can be empty.

BRANCH_TO command

This command provides users a list of items to select, and on selection of an item, execution of the workflow is branched to the specified command. The behavior of this screen is similar to the SELECT screen described above. Once the workflow execution starts executing from the new target instruction, it follows the default sequential order. When the BRANCH_BACK command is executed, the workflow execution engine returns to the previous BRANCH_TO command to execute. However, the BRANCH_TO command does not require a BRANCH_BACK command to operate. The workflow can consequently branch to the last command without returning to the branch menu.

To progress to the next screen from a BRANCH_TO command, a "Next" button is provided. On some phones, this button is mapped to one of the phone keys on the mobile device. On most phones however, this button is mapped to a soft-key named "Next" when the user select Options on the BRANCH_TO screen (similar to SELECT_MULTI command).

There is no specific user value attached to this screen in the response message. The selected branch item is however appended to the branch domain path. This domain path is then appended to the parameter name of any input screens being executed in the branch target.

Syntax

BRANCH_TO command is followed by ITEM definitions (one per line).

```
BRANCH_TO    <parameter name> <title>
ITEM         <item> <label>
ITEM         <item > <label>
ITEM         <item > <label>
```

Where:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1099 of 1360

- < parameter name > is a string parameter specifying the return parameter id for the BRANCH_TO screen.
- <title> is a string parameter specifying the title of the screen.
- <item > is a string parameter specifying the item to be displayed on the screen.
- <label> is a valid label name as specified in the workflow with "#" character.

Examples

```
...
# EnterBetAmount
INPUT "bet" "Enter bet amount" DECIMAL
BRANCH_BACK
....
# SelectBetAmount
SELECT "bet" "Select bet amount in dollars"
ITEM "100"
ITEM "200"
ITEM "300"
BRANCH_BACK
....
BRANCH_TO "b" "Select team to bet"
ITEM "Melbourne" EnterBetAmount
ITEM "Geelong" SelectBetAmount
GOTO END
...
# END
MESSAGE "Info" "Please select Yes to allow response message to be sent"
```

Response

- The domain path is appended with <item> selected in the branch menu.
- This domain path is then appended to the parameter name of any input screen executed in the branch target. In the example script, the "bet" amount parameter name when appearing in the response message is: Melbourne.bet=<bet value>.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1100 of 1360

BRANCH_BACK command

This command is invisible to the user, it provides the capability to navigate back from branching. A workflow could have multiple branches wired up and the result is a tree like structure. BRANCH_BACK command allows navigation upwards in this tree structure. Combination of label and BRANCH_BACK command allows combining a group of workflow commands in to a routine, which can be referred to multiple times during the workflow execution.

Syntax

BRANCH_BACK

STORE_PERMANENT command

This command instructs the workflow execution to store the whole payload data to persistent storage. A title is set in the parameter of this command allows the client application to display the stored payload data to the user. This command does not result in any user data in the response message.

Syntax

STORE_PERMANENT <title>

Where:

- <title> is a string parameter indicating the title of workflow payload data to be displayed in the persistent list. This persistent list is displayed to the user when the client application is started manually by the user and no instant payload data is waiting to be executed.

Example

STORE_PERMANENT "Message one"

CLEAR_PERMANENT command

This command clears all the persistent workflow payload data previously saved by STORE_PERMANENT command. Execution of this command does not result in any data in the response message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1101 of 1360

Syntax

CLEAR_PERMANENT

EXECUTE command

This command makes a request to the mobile device operating system to retrieve an URL address. The results could be making a phone call or launching the internet browser on the phone to the specified URL address. Behavior of this command might varies across different device models due to device capabilities.

Syntax

EXECUTE <url_address>

Where:

- <url_address> is a string parameter describing the URL address of the request to be sent to the J2ME platform.

Example

To make a mobile phone call to +61418366896 mobile number

EXECUTE "tel:+61418366896"

To launch the internet browser on the mobile phone to access ACME mobile website

EXECUTE "http://mobile.acme.com"

Response

If making a mobile phone call is required, the mobile device will ask user if a mobile phone call can be made. If launching of the internet browser is required, the application will ask for the user's permission to open the internet connection to the specified URL.

CONFIGURATION command

The response message is constructed from the user/system data. A number of default delimiter characters are used to separate the data parts as well as name-value separator. This command when included in the payload data can change the delimiter characters of the response message as well as specifying whether or not the name part is included in the response message.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1102 of 1360

Syntax

CONFIGURATION <configuration_string>

Where <configuration_string> is composed of configuration characters:

- 1st character: Include parameter in the response, if set to '0', the response message only has values, set to '1', the response message has Name=Value
- 2nd character: Response part delimiter, the default is ','
- 3rd character: Equal character, the default is '='
- 4th character: Multiple selection options, the default is ';'
- 5th character: Screen path delimiter, the default is '.'

Example

CONFIGURATION "0,=;."

This configuration command instructs the workflow execution to exclude parameter names from the response message.

SYSTEM_PROPERTY command

This command instructs the workflow execution to read a system property and return the result in the response. The parameter name that is associated with the response data is the system property if parameter name is omitted.

Syntax

SYSTEM_PROPERTY <property_name> <parameter name>

Where:

- <property_name> is the system property to be read. On the J2ME platform, examples of these properties are:
  - microedition.profiles
  - microedition.configuration
- <parameter name> is an optional string parameter. If omitted, property name is used as parameter name in the response instead.

Examples

SYSTEM_PROPERTY "microedition.profiles"

SYSTEM_PROPERTY "microedition.profiles" "midp"

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1103 of 1360

Response

The value of the system property is included in the response message as name=value pair. All the rules applied to the name-value pairs are applied. These include changing of delimiter parameters and whether or not to include the name part in the response message.

<system property>=<value> (if parameter name is omitted)

<parameter name>=<value> (if parameter name is present)

NOP command

This is a no-operation command. It is useful when used in conjunction with labeling.

Syntax

NOP

SET_KEYS command

A command to set the encryption key specified by the index of the key on the mobile device.

Syntax

SET_KEYS <key_index> <key>

Where <key_index> is a string parameter indicating the index of the key to be set on the client application 102. <key> is a string parameter containing the actual key to be updated.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as hereinbefore described with reference to the accompanying drawings.

It will be apparent from the description above that the interactive system and process described herein allow a developer to dynamically send on demand customisable workflow instructions to one or more user devices 106 such as mobile telephones. The generation, secure delivery, execution, and secure return of response data to the developer are all handled transparently by the interactive system, thus hiding all the details of these aspects from the developer, greatly simplifying the provision of interactive applications and quasi-real-time interactions with one or more users. The provision of workflow instructions via

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1104 of 1360

SMS is particularly advantageous as it can be assumed to be supported by all mobile telephones available today. Moreover, since the SMS communications are all managed by the interactive system, any premium SMS services that may be required can be established by the operator of the interactive system, thus freeing the developer from needing to establish their own independent premium SMS services. This greatly simplifies the provision of new interactive applications, and also allows the operator of the interactive system to provide these services at a lower cost by leveraging the substantial volume of SMS traffic resulting from the aggregation of SMS traffic or all developers using the interactive system.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1105 of 1360

CLAIMS:

1. A method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

2. A method as defined by claim 1 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language.

3. A method as defined by either of claims 1 or 2 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

4. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device.

5. A method as defined by claim 4 wherein the step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

6. A method as defined by claim 5 wherein the step of sending the message includes the step of sending a unique message identifier.

7. A method as defined by claim 6 further comprising the step of the mobile user device receiving the set of instructions and the unique message identifier.

8. A method as defined by claim 7 wherein the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

9. A method as defined by either of the claims 7 or 8 further comprising the step of receiving a response to the instruction from the mobile user device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1106 of 1360

10. A method as defined by claim 9 wherein the step of receiving a response includes the step of receiving a response identifier from the device.

11. A method as defined by claim 10 wherein the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

12. A method as defined by any one of the preceding claims wherein the step of translating the instruction includes tailoring the instruction to a device operating system.

13. A method as defined by any one of the preceding claims wherein the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

14. A method as defined by claim 13 wherein the step of translating the interactive workflow includes tailoring the instruction to the specification.

15. A method as defined by any one of the preceding claims wherein the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

16. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network.

17. A method as defined by claim 16 wherein the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS.

18. A method as defined by any one of the claims 1-15 wherein the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1107 of 1360

19. A method as defined by any one of the preceding claims also including the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow.

20. A method as defined by claim 19 wherein the step of checking involves sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow.

21. A method as defined by claim 3 wherein the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface (API) from the external or third party.

22. A method as defined by claim 21 wherein the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

23. A method as defined by any one of the preceding claims also comprising the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

24. Computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

25. A method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1108 of 1360

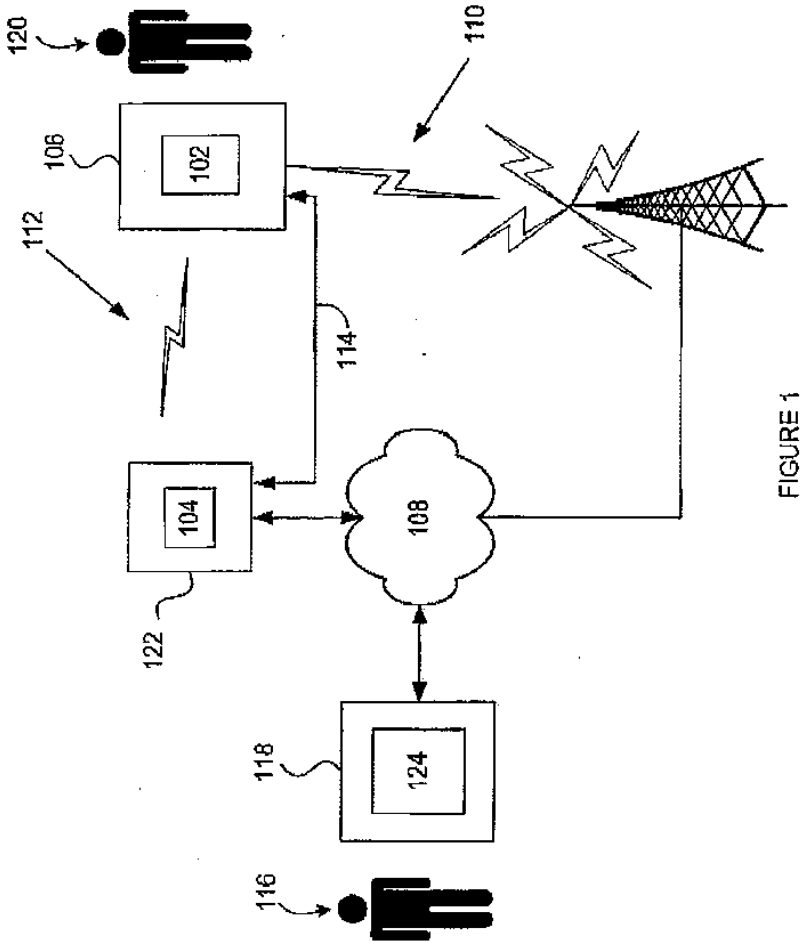


FIGURE 1

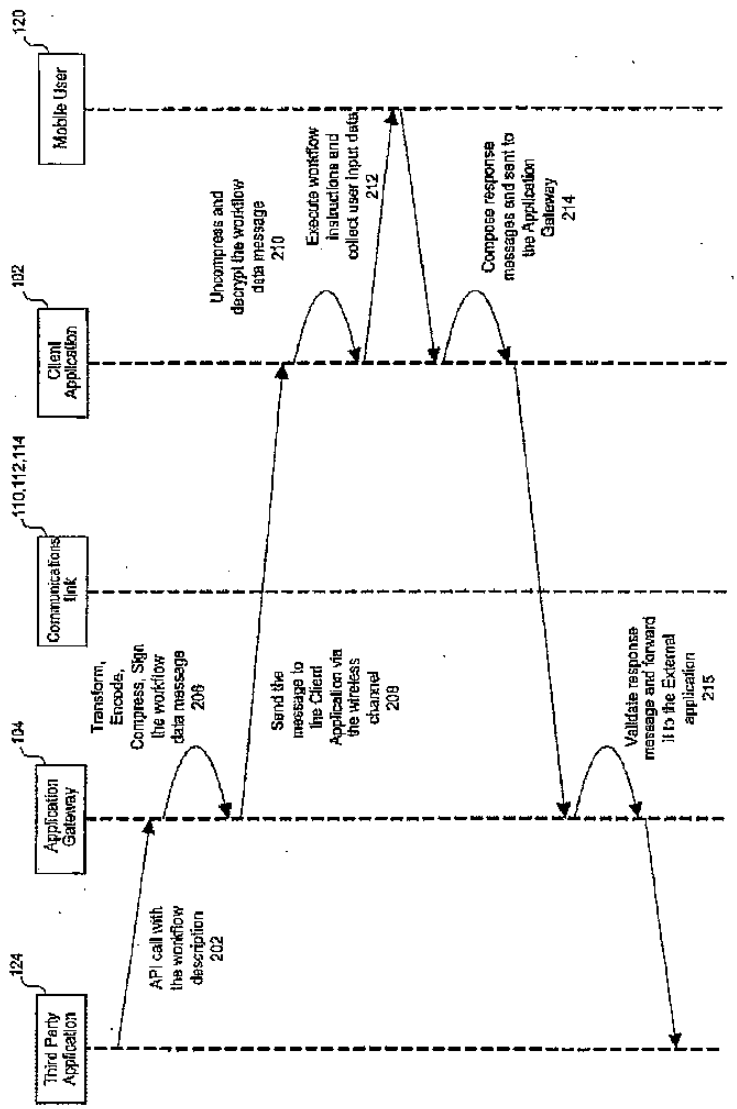


FIGURE 2

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1110 of 1360

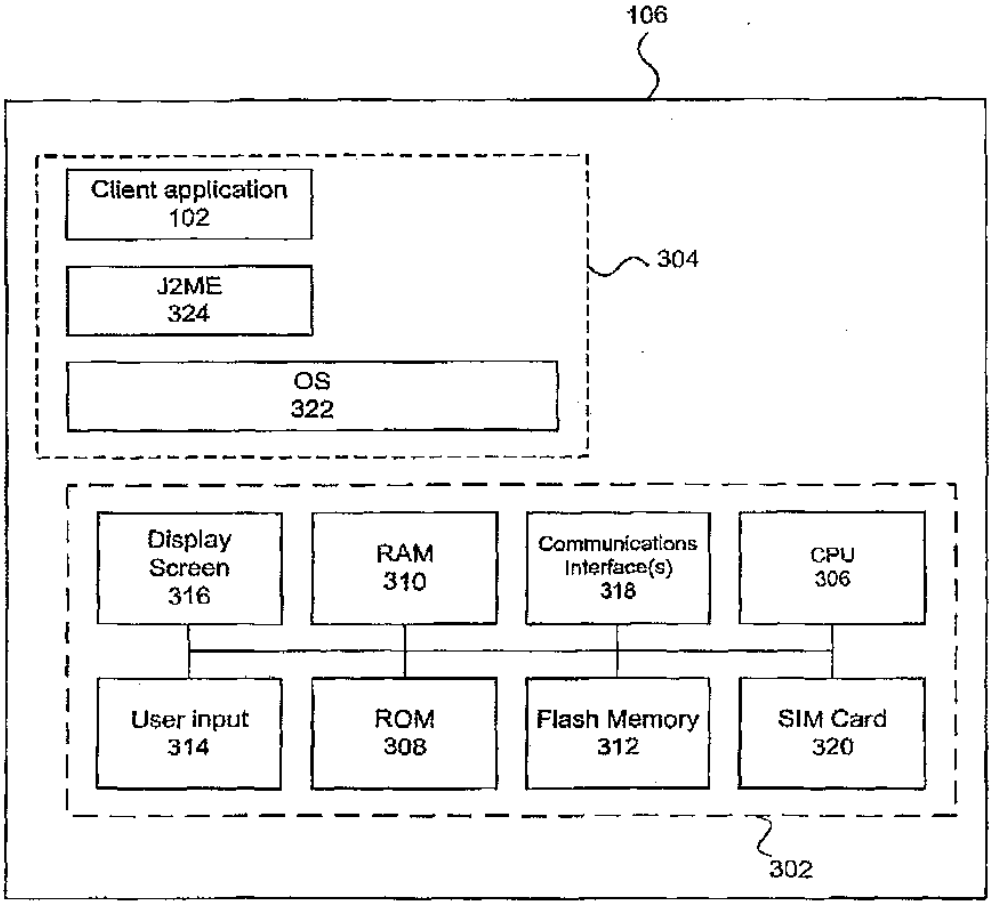

106
Client application
102
J2ME
324
OS
322
304
Display
Screen
316
RAM
310
Communications
Interface(s)
318
CPU
306
User input
314
ROM
308
Flash Memory
312
SIM Card
320
302

FIGURE 3

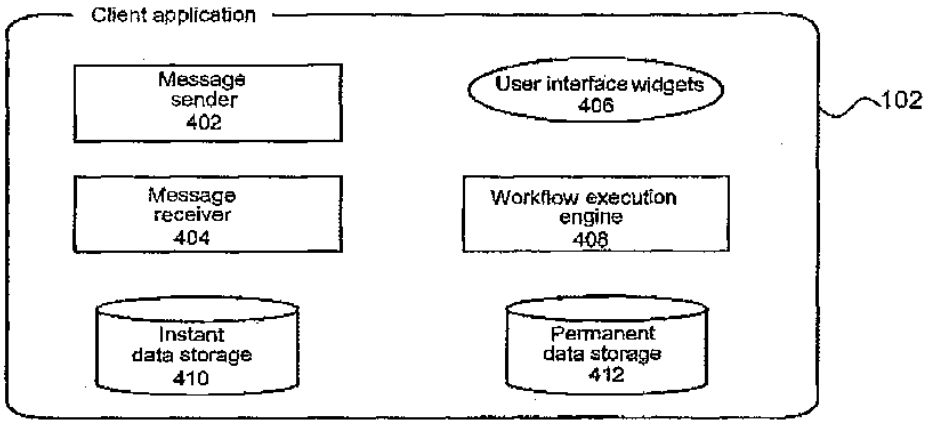


FIGURE 4

FIGURE 5

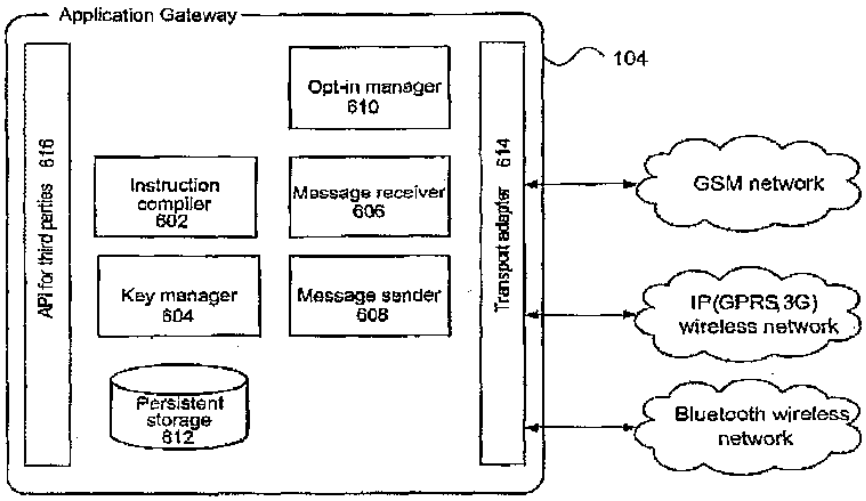

Application Gateway
104
API for third parties 616
Opt-in manager 610
Instruction compiler 602
Message receiver 606
Key manager 604
Message sender 608
Persistent storage 612
Transport adapter 614
GSM network
IP(GPRS,3G) wireless network
Bluetooth wireless network

FIGURE 6

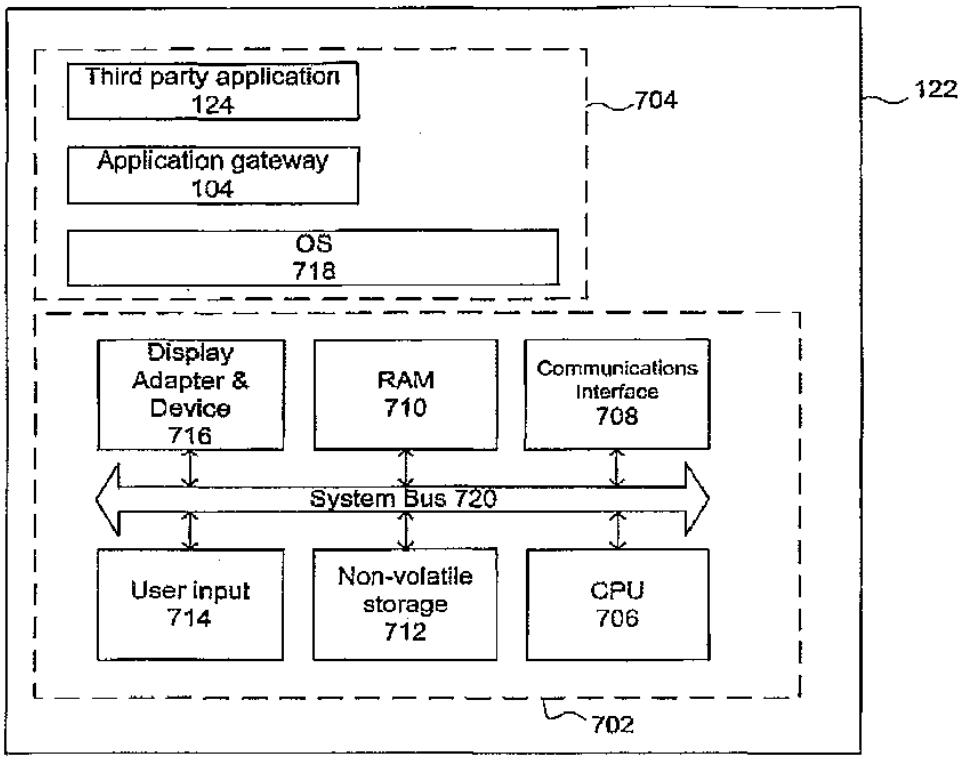

Third party application
124
Application gateway
104
OS
718
704
122
Display
Adapter &
Device
716
RAM
710
Communications
Interface
708
System Bus 720
User input
714
Non-volatile
storage
712
CPU
706
702

FIGURE 7

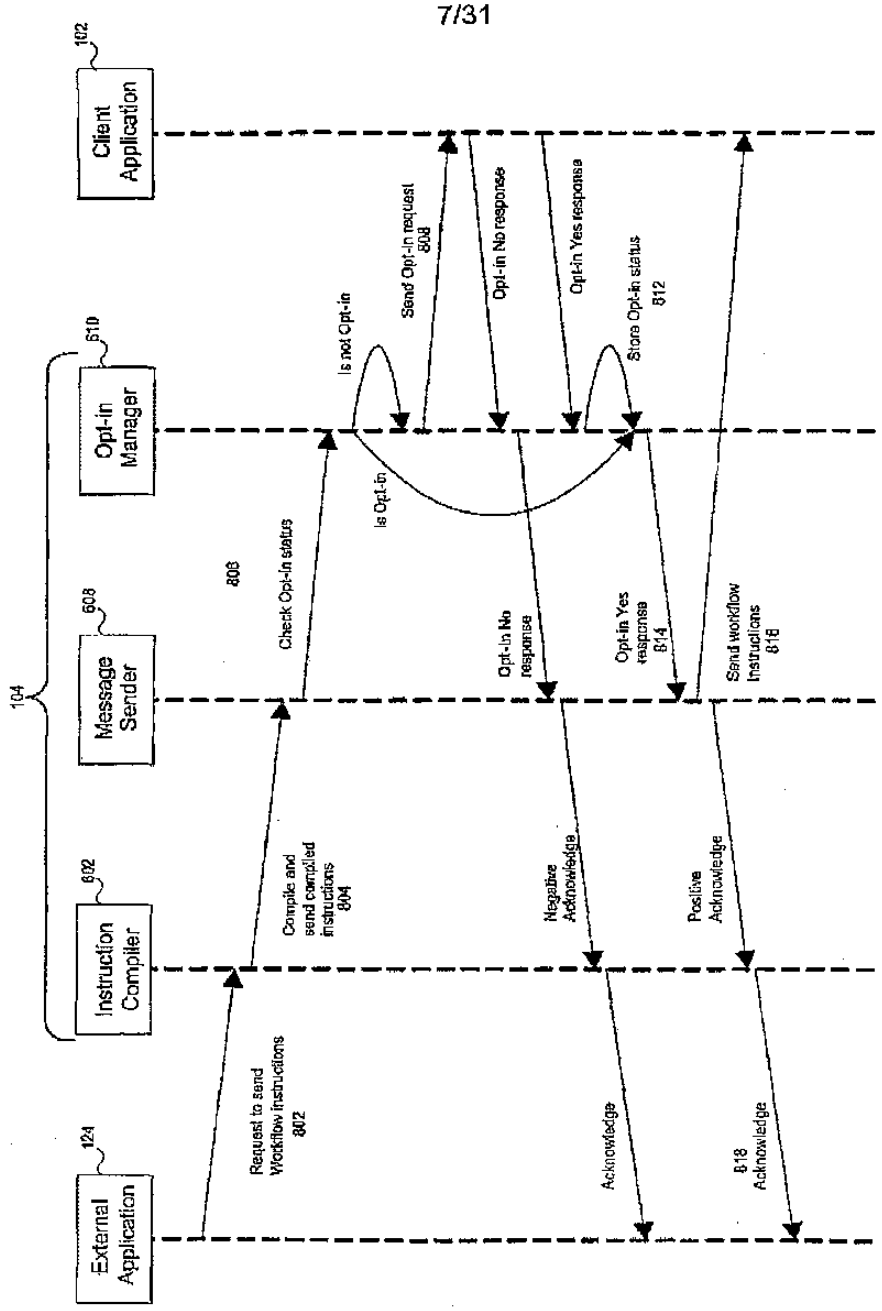


Figure 8

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1115 of 1360

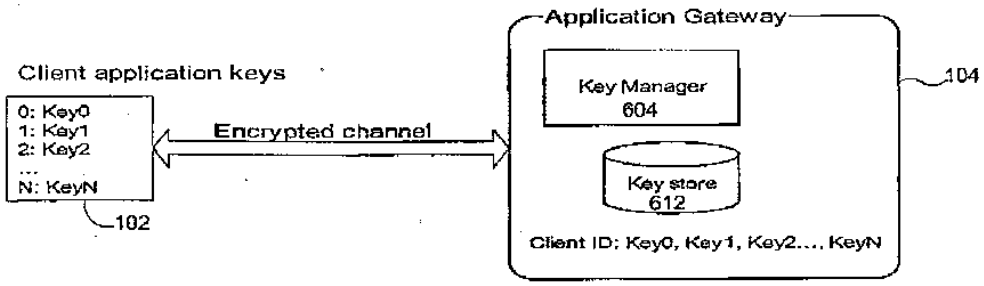

Application Gateway
Client application keys
0: Key0
1: Key1
2: Key2
...
N: KeyN
Encrypted channel
Key Manager
604
Key store
612
Client ID: Key0, Key1, Key2..., KeyN
102
104

FIGURE 9

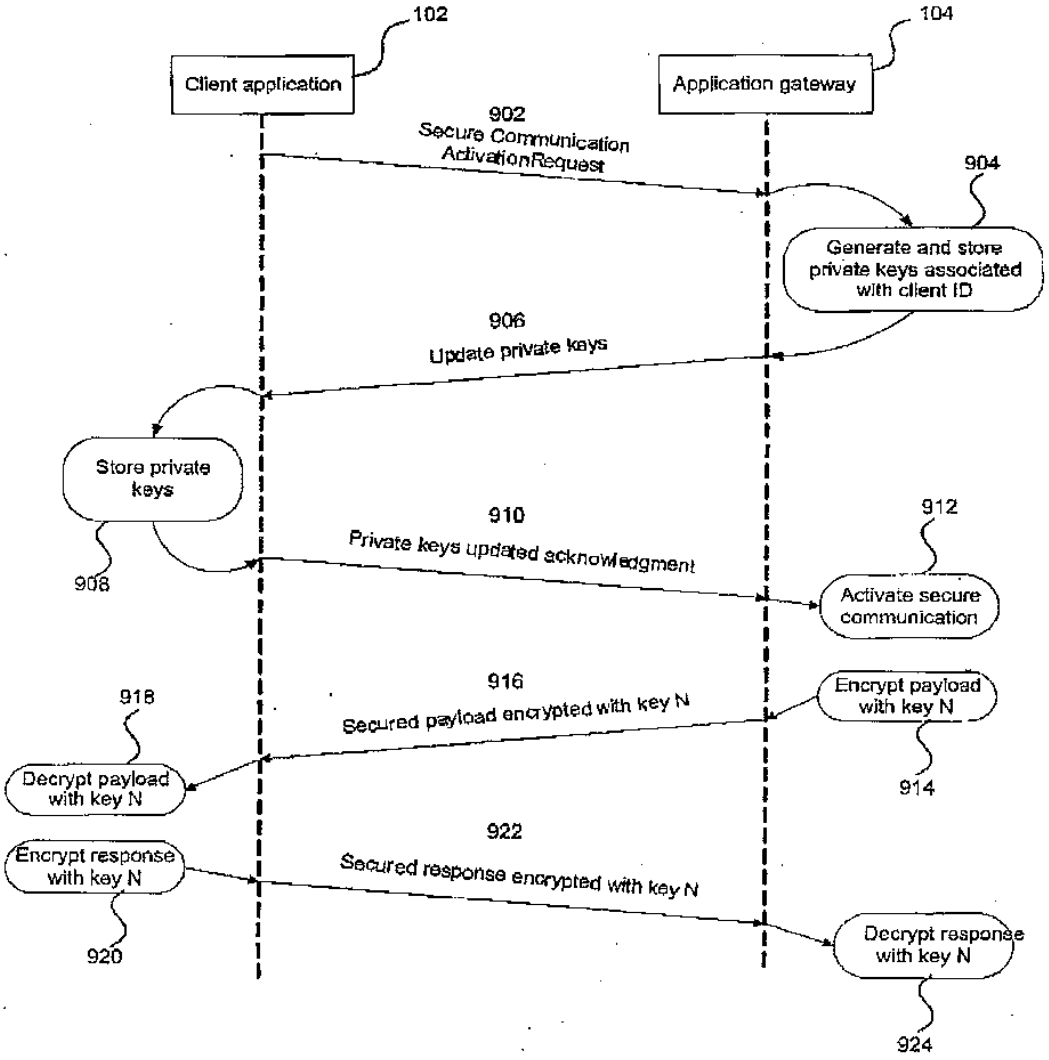


FIGURE 10

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1117 of 1360

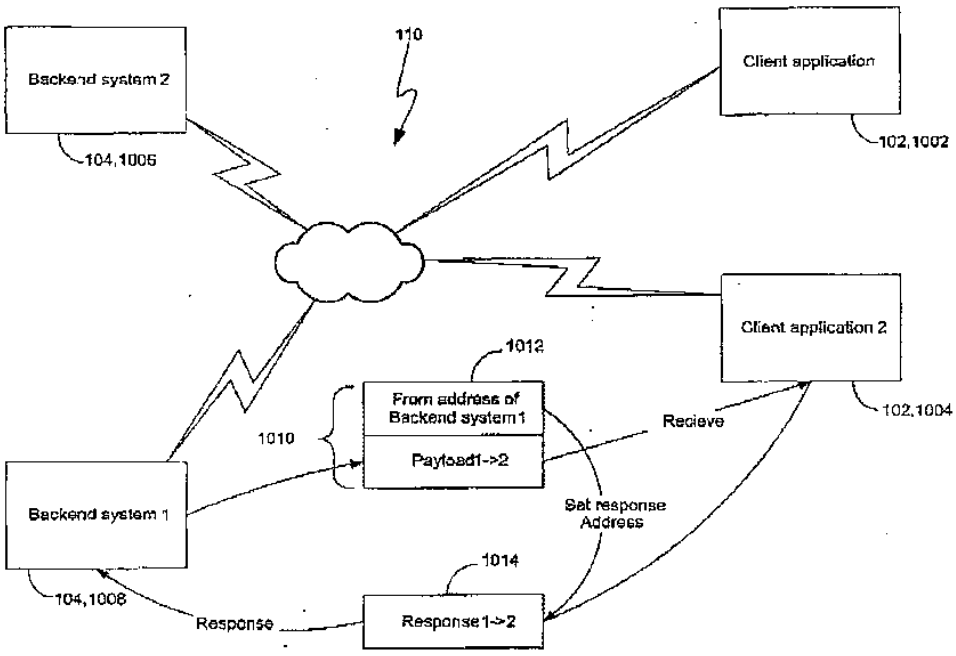

110
Backend system 2
104,1006
Client application
102,1002
Client application 2
102,1004
1012
From address of Backend system 1
Payload1->2
1010
Recieve
Backend system 1
Set response Address
1014
104,1008
Response
Response1->2

FIGURE 11

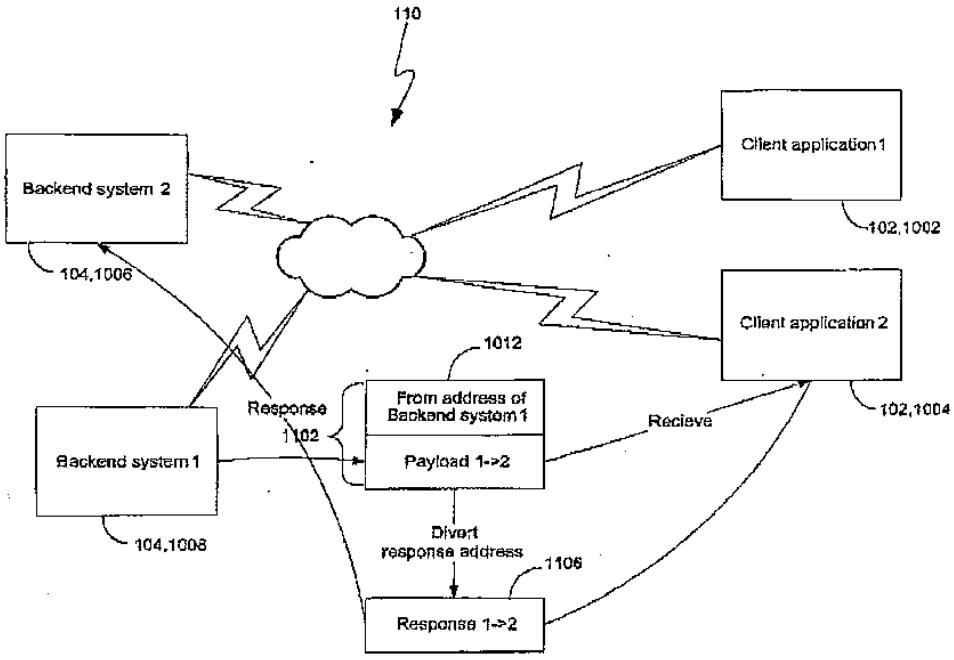

110
Backend system 2
104,1006
Client application1
102,1002
Client application 2
102,1004
1012
From address of Backend system1
Payload 1->2
Response 1102
Backend system1
104,1008
Recieve
Divert response address
1106
Response 1->2

FIGURE 12

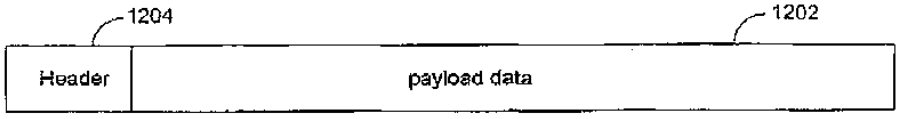


FIGURE 13

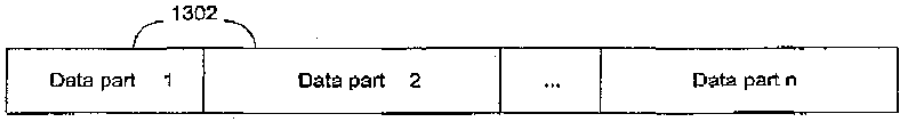


FIGURE 14

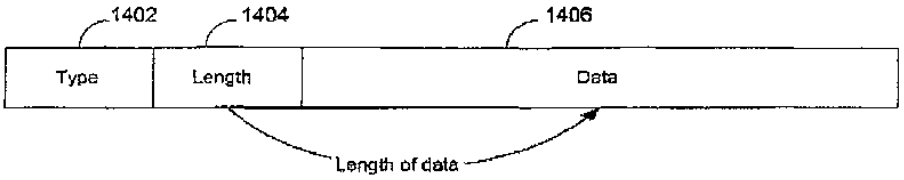


FIGURE 15

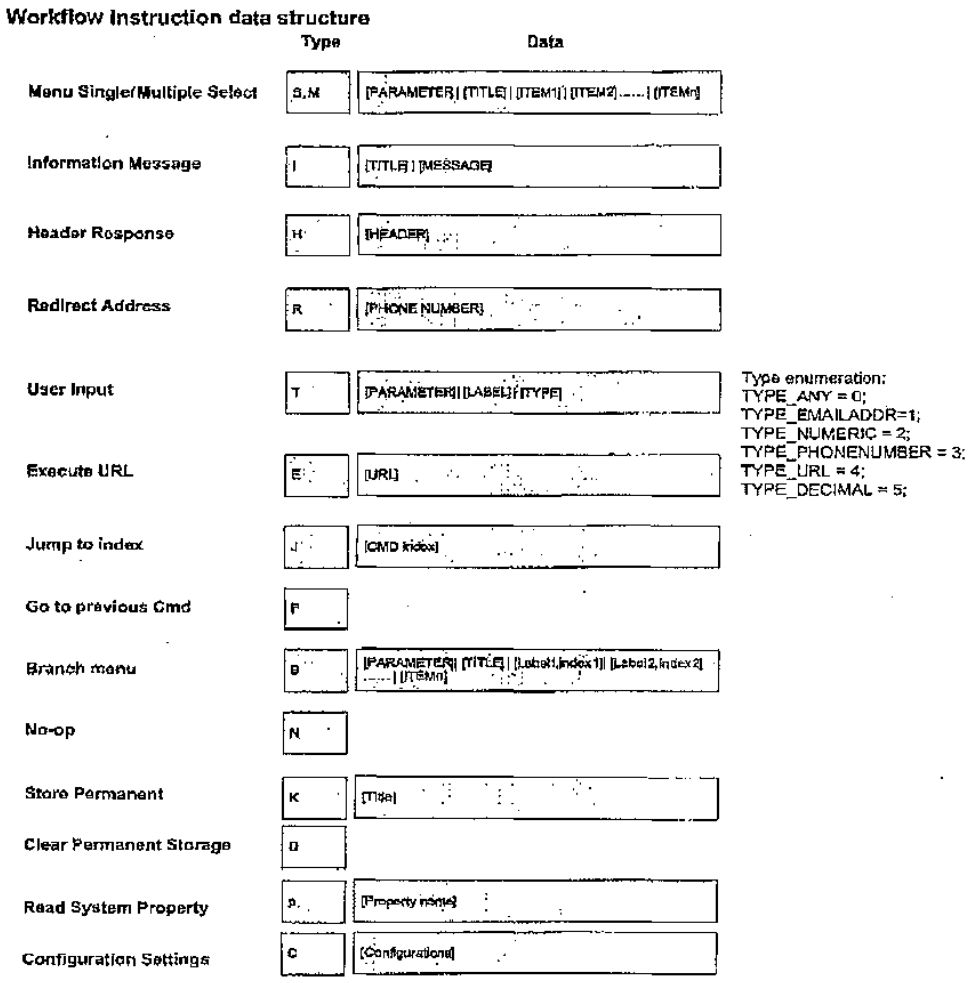


FIGURE 16

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1121 of 1360

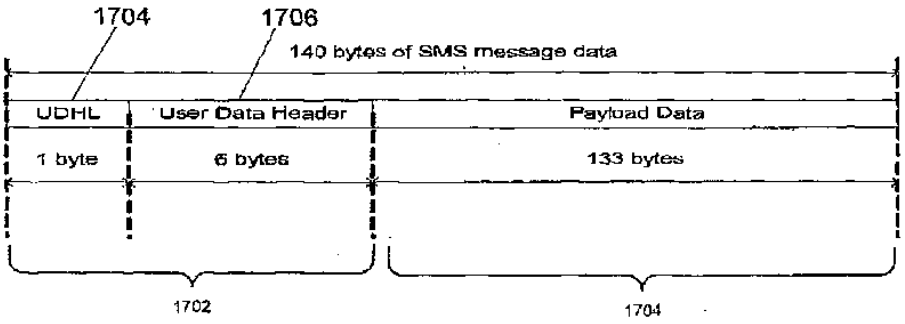


FIGURE 17

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1122 of 1360

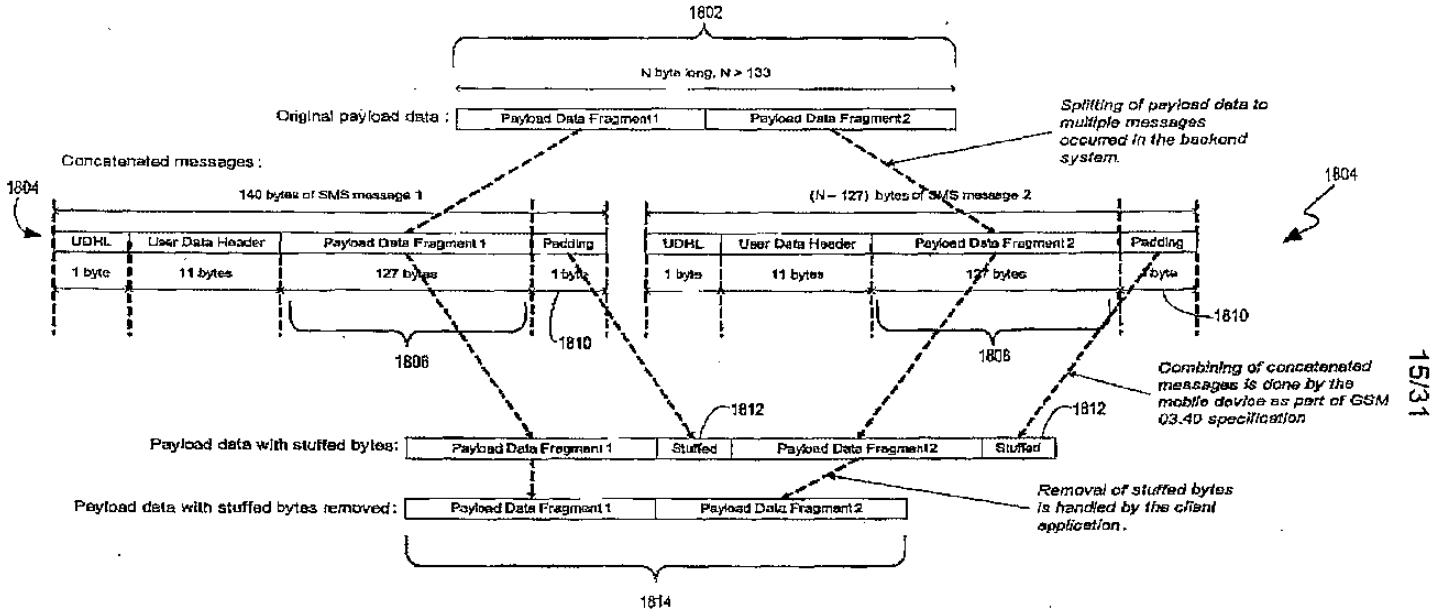


FIGURE 18

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1123 of 1360

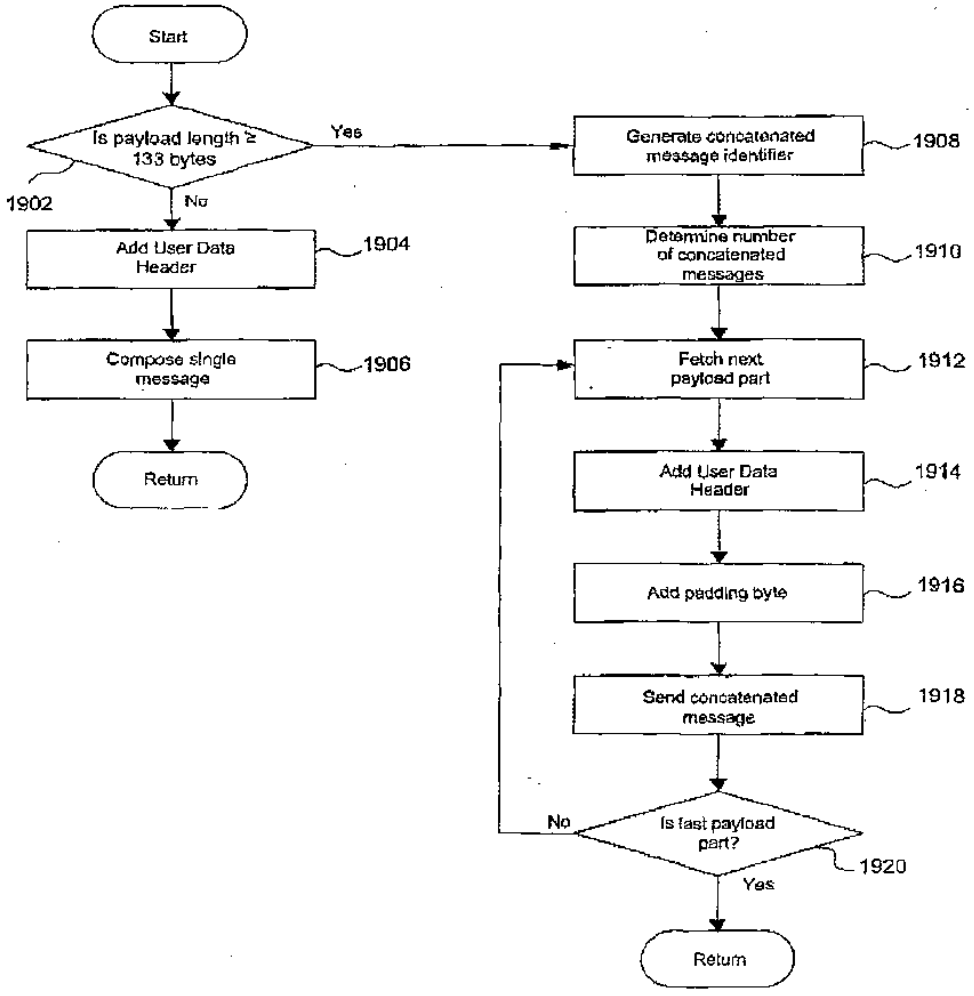

Start
Is payload length ≥ 133 bytes
Yes
No
1902
Add User Data Header
1904
Compose single message
1906
Return
Generate concatenated message identifier
1908
Determine number of concatenated messages
1910
Fetch next payload part
1912
Add User Data Header
1914
Add padding byte
1916
Send concatenated message
1918
Is last payload part?
No
Yes
1920
Return

FIGURE 19

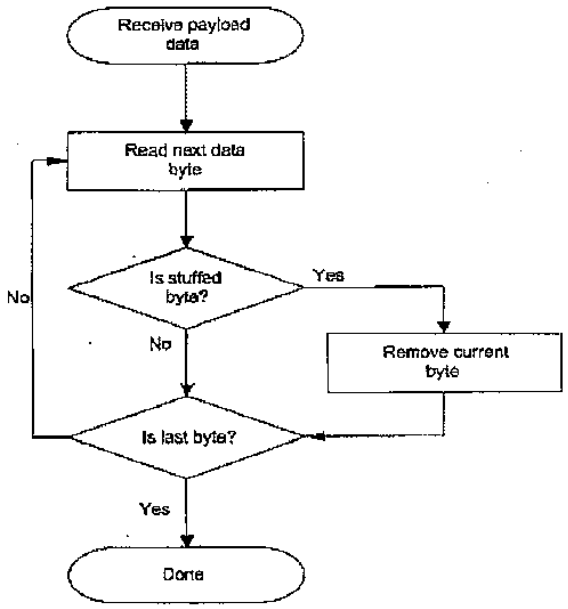

Receive payload data
Read next data byte
Is stuffed byte?
Yes
No
Remove current byte
Is last byte?
No
Yes
Done

FIGURE 20

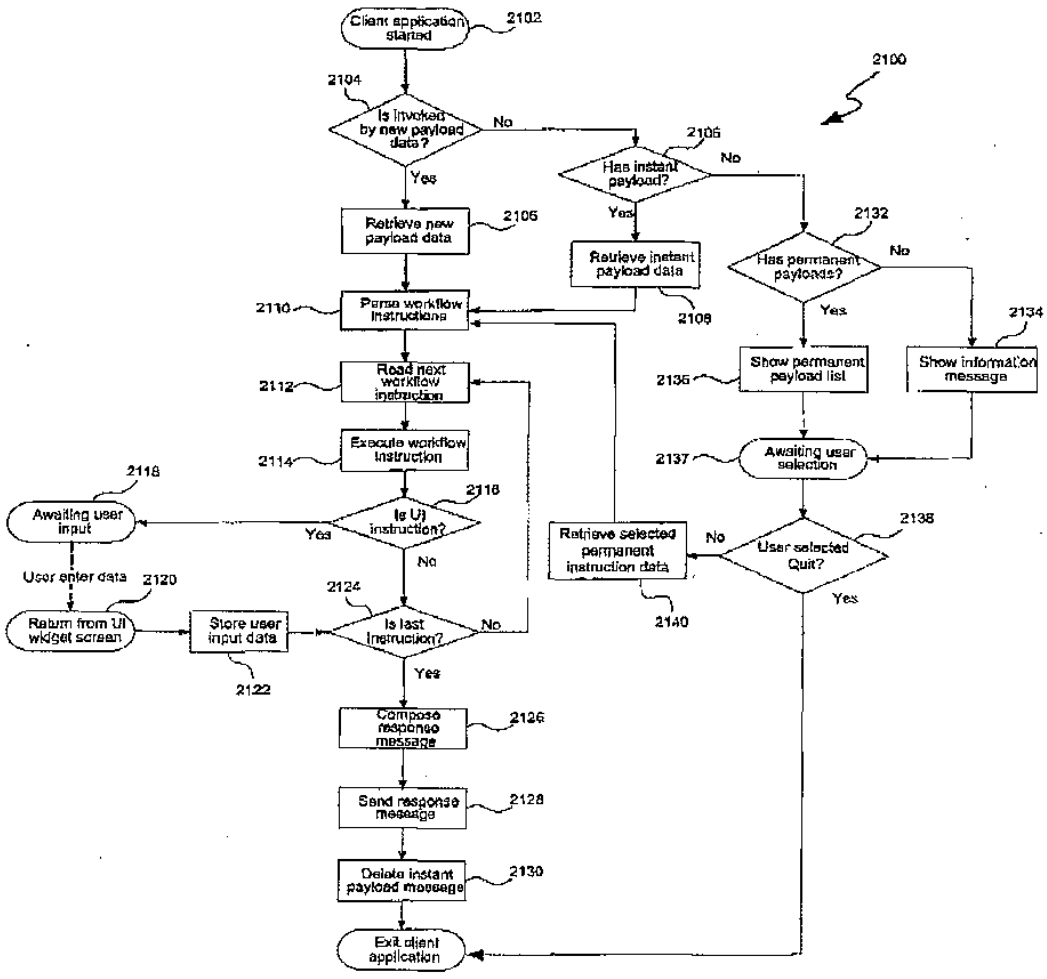

Client application started
2102
2100
2104
Is invoked by new payload data?
No
Yes
2105
Has instant payload?
No
Yes
Retrieve new payload data
2106
Retrieve instant payload data
2109
2132
Has permanent payloads?
No
Yes
2134
2110
Parse workflow instructions
Show permanent payload list
Show information message
2135
2112
Read next workflow instruction
2137
Awaiting user selection
2114
Execute workflow instruction
2118
Awaiting user input
2116
Is UI instruction?
Yes
No
2138
Retrieve selected permanent instruction data
No
User selected Quit?
Yes
2140
User enter data
2120
Return from UI widget screen
Store user input data
2122
2124
Is last instruction?
No
Yes
Compose response message
2126
Send response message
2128
Delete instant payload message
2130
Exit client application

FIGURE 21

0	Instruction 1 response
1	Instruction 2 response
n	Instruction n response

FIGURE 22

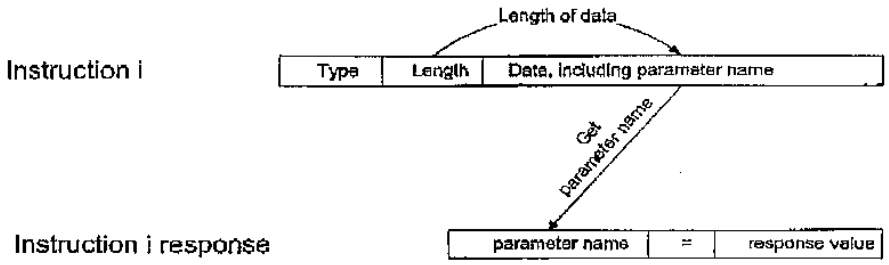


FIGURE 23

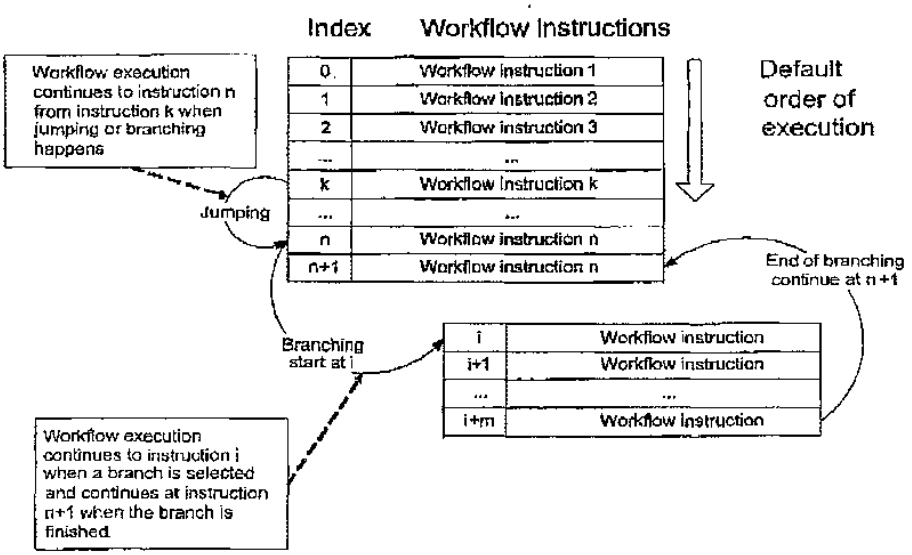

Index
Workflow Instructions
Workflow execution continues to instruction n from instruction k when jumping or branching happens
0
Workflow instruction 1
1
Workflow instruction 2
2
Workflow instruction 3
...
...
k
Workflow instruction k
...
...
n
Workflow instruction n
n+1
Workflow instruction n
Default order of execution
Jumping
End of branching continue at n+1
Branching start at i
i
Workflow instruction
i+1
Workflow instruction
...
...
i+m
Workflow instruction
Workflow execution continues to instruction i when a branch is selected and continues at instruction n+1 when the branch is finished

FIGURE 24

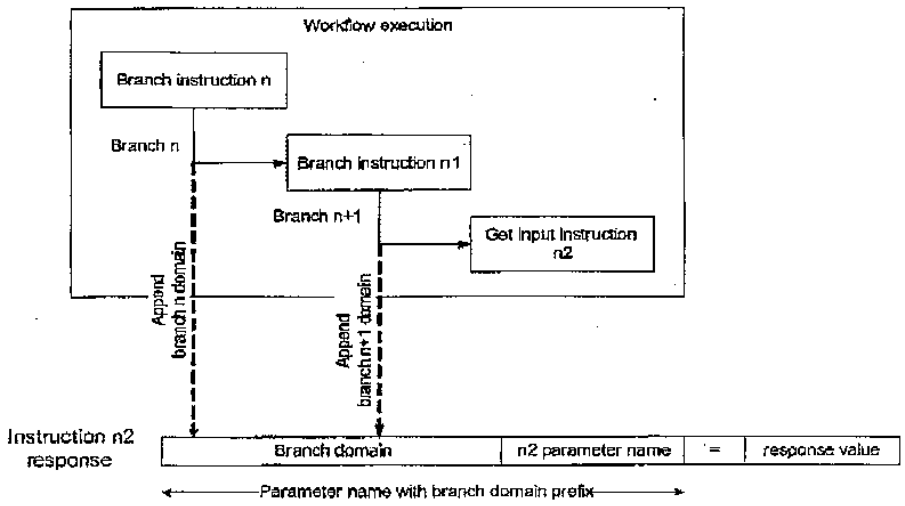

Workflow execution
Branch instruction n
Branch n
Branch instruction n1
Branch n+1
Get input instruction n2
Append branch n domain
Append branch n+1 domain
Instruction n2 response
Branch domain
n2 parameter name
=
response value
Parameter name with branch domain prefix

FIGURE 25

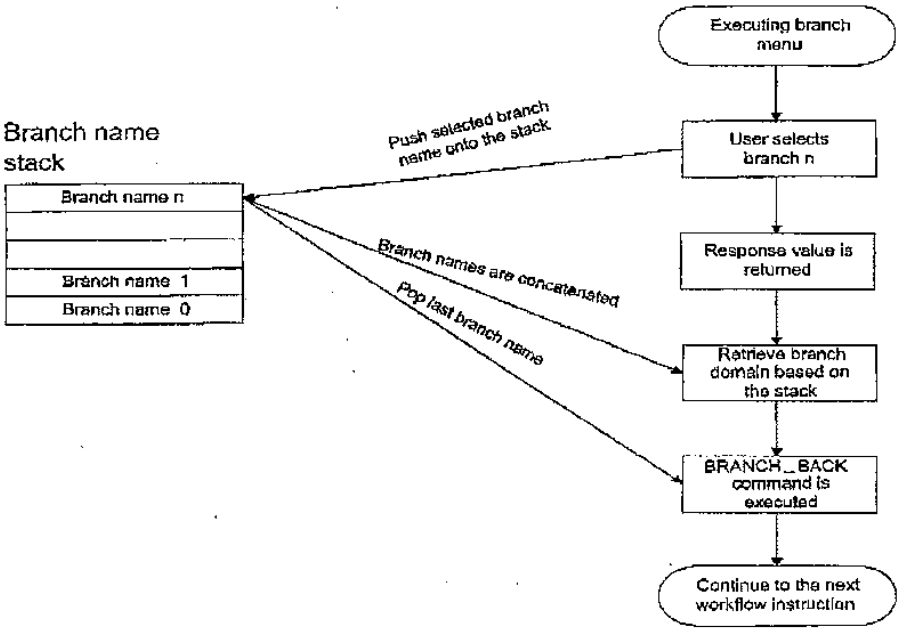

Executing branch menu
User selects branch n
Response value is returned
Retrieve branch domain based on the stack
BRANCH_BACK command is executed
Continue to the next workflow instruction
Push selected branch name onto the stack
Branch names are concatenated
Pop last branch name
Branch name stack
Branch name n
Branch name 1
Branch name 0

FIGURE 26

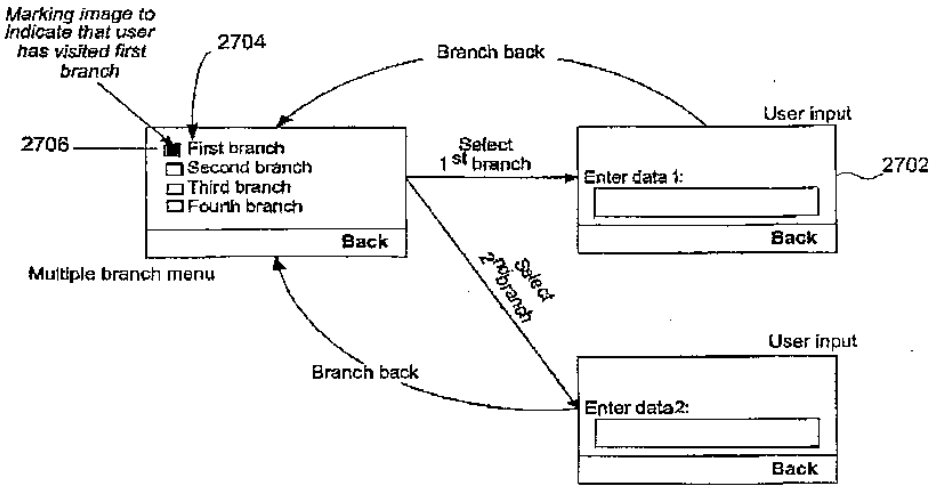


FIGURE 27

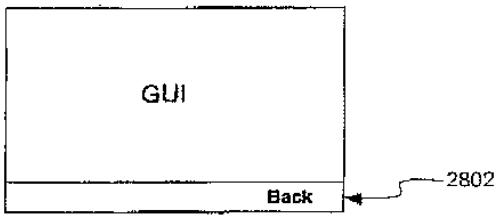


FIGURE 28

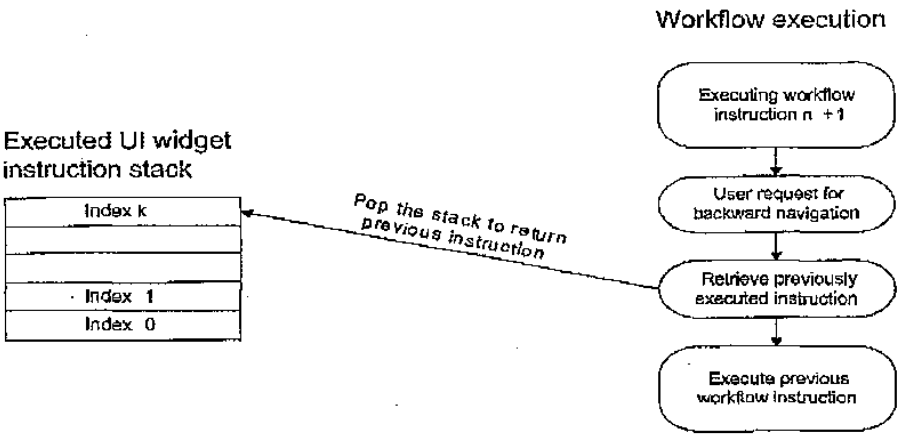

Workflow execution
Executing workflow instruction n +1
User request for backward navigation
Retrieve previously executed instruction
Execute previous workflow instruction
Pop the stack to return previous instruction
Executed UI widget instruction stack
Index k
Index 1
Index 0

FIGURE 29

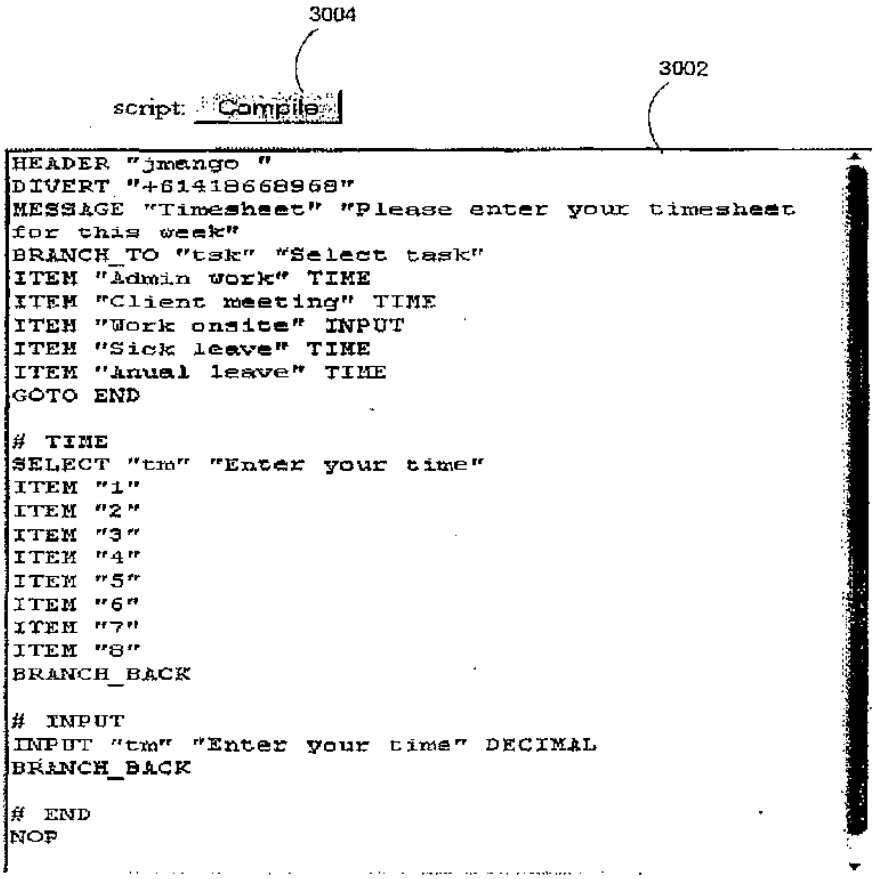


FIGURE 30

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1133 of 1360

```
private string SendWorkflowRequest(string sourceNumber,
    string destinationNumber, string bookingHeader,
    string bookingTitle, string bookingDetails)
{
3102 ---> J2MECommand workflowCommand = new J2MECommand();
3104 ---> if(bookingHeader != null)
        workflowCommand.AddCmdHeader(bookingHeader);

    // Add information message
3106 ---> workflowCommand.AddInfoMessage(bookingTitle, bookingDetails);
    // Add selection menu
3108 ---> workflowCommand.AddSingleMenu("action", "Select", new String[]{"Accept", "Reject"});
    // Add input text box to enter name
3110 ---> workflowCommand.AddUserInputCmd("name", "Enter your name", J2MECommand.InputType.ANY);
    // Add input text box to enter contact number
3112 ---> workflowCommand.AddUserInputCmd("contact", "Contact number", J2MECommand.InputType.PHONENUMBER);
    // Add redirection address where the response message is sent to
3114 ---> workflowCommand.AddRedirectHeader("sms://1991616");

    // Now send the command, in multiple messages if it is neede
3116 ---> IList messages = workflowCommand.BuildCommandMessages(1000);
    string sentIds = "";
    foreach(BinaryMessage binMessage in messages)
    {
3118    sentIds += _messageSender.SendBinaryMessage(sourceNumber, destinationNumber,
                                                    binMessage.UserData, binMessage.DataHeader);
        sentIds += ",";
    }
    return sentIds;
}
```

FIGURE 31

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1134 of 1360

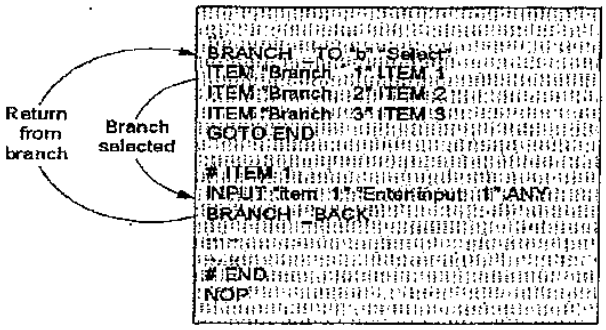


FIGURE 32

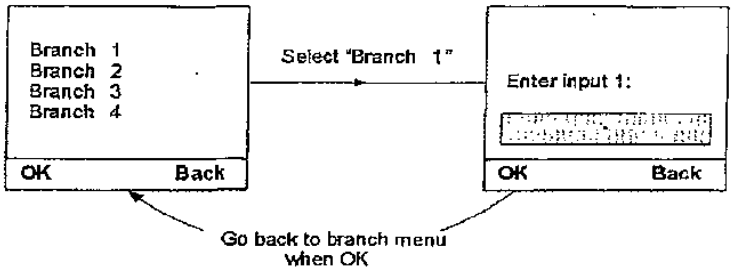


FIGURE 33

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1135 of 1360

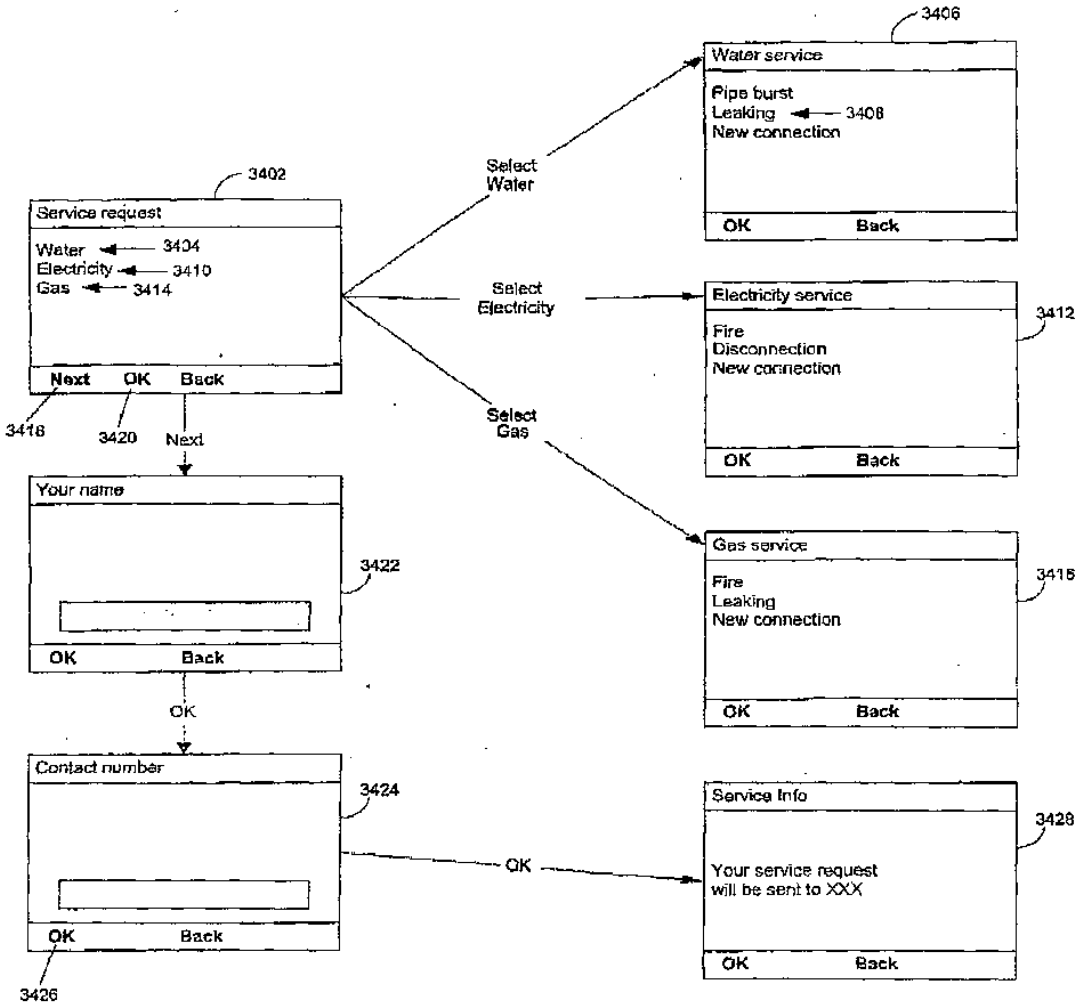

3406
Water service
Pipe burst
Leaking
3408
New connection
OK
Back
3402
Service request
Water
3404
Electricity
3410
Gas
3414
Next
OK
Back
3418
3420
Next
Select Water
Select Electricity
Select Gas
Electricity service
3412
Fire
Disconnection
New connection
OK
Back
Your name
3422
OK
Back
OK
Gas service
3416
Fire
Leaking
New connection
OK
Back
Contact number
3424
OK
Back
3426
OK
Service Info
3428
Your service request will be sent to XXX
OK
Back

FIGURE 34

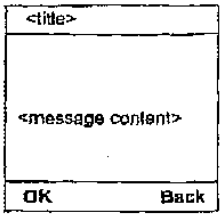


FIGURE 35

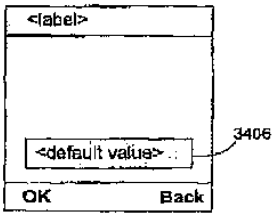


FIGURE 36

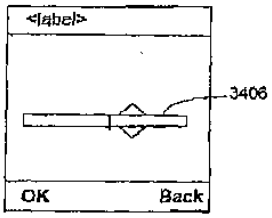


FIGURE 37

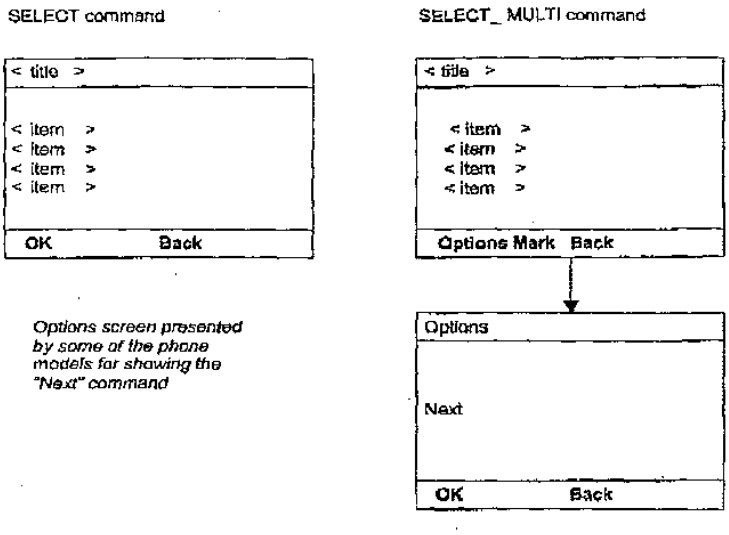

SELECT command
< title >
< item >
< item >
< item >
< item >
OK
Back
Options screen presented by some of the phone models for showing the "Next" command
SELECT_ MULTI command
< title >
< item >
< item >
< item >
< item >
Options Mark Back
Options
Next
OK
Back

FIGURE 38

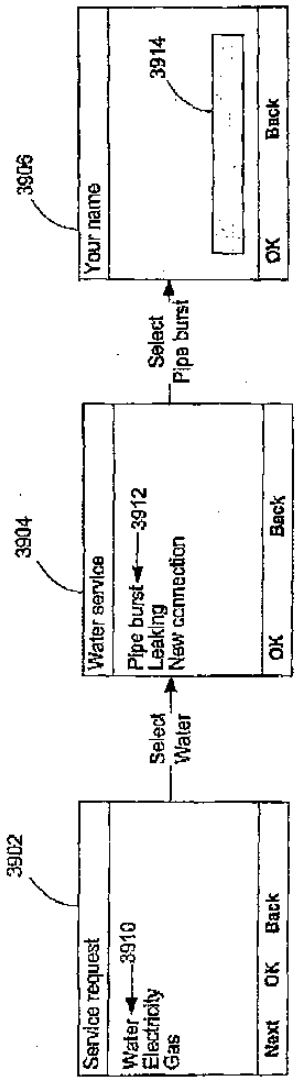


FIGURE 39

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1139 of 1360

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2007/001599

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04Q 7/22 (2006.01) ***H04M 3/493*** (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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)
DWPI & USPTO: Keywords: (interactive, SMS, encryption, compile, header, payload and like terms).

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/0095291 A1 (Cherney) 4 May 2006. See for example the title; abstract; fig 4A-4C, 5 and 7; paras [0013]-[0016], [0033]-[0041], [0057]-[0080] and [0089]-[0140].	1-25
X	EP 1509049 A1 (Accenture Global Services GMBH) 20 August 2003. See for example the abstract; paras [0033]-[0039]; and fig 2 and 5.	1-25
A	US 2002/0073023 A1 (Castro et al.) 13 June 2002.	

☐ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier 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
11 December 2007	20 DEC 2007
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **Malcolm Peh** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : (02) 6283 7914

Form PCT/ISA/210 (second sheet) (April 2007)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1140 of 1360

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU2007/001599

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	2006095291	EP	1836676	US	2006095290	WO	2006050413
EP	1509049	US	2007191032	WO	2005020609		
US	2002073023						

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1141 of 1360

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To
JOHN C. STRINGHAM
60 EAST SOUTH TEMPLE
SUITE 1000
SALT LAKE CITY, UT 84111

JCS 18756.8.1a
MS 2/4/13
Article 19 Amendments
3/29/13

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing (day month year) 29 JAN 2013

Applicant's or agent's file reference
18756.8.1A

FOR FURTHER ACTION See paragraphs 1 and 4 below

International application No
PCT/US 12/40131

International filing date (day month year) 31 May 2012 (31.05.2012)

Applicant MOZIDO, LLC

1 ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No. +41 22 338 82 70

For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 – 9.011

2 ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ With regard to any protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the ISA/
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450 Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer
Lee W. Young
PCT Helpdesk: 571-272-4300
Telephone No. PCT OSP 571-272-7774

Form PCT/ISA/220 (July 2010)

2/4/13

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
18756.8.1-A		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US 12/40131	31 May 2012 (31.05.2012)	03 June 2011 (03.06.2011)

Applicant
MOZIDO, LLC

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 8 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1 **Basis of the report**

a With regard to the **language**, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (see Box No. II).

3. ☐ **Unity of invention is lacking** (see Box No. III)

4 With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a the figure of the **drawings** to be published with the abstract is Figure No. 6B

☐ as suggested by the applicant.

☒ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1143 of 1360

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 12/40131

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 20/00 (2012.01)
USPC - 705/65
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 20/00 (2012.01)
USPC: 705/65

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/73; 705/39; 902/2 (keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase; Google Scholar, Google Patents; FreePatentsOnline. Search terms used: financial-transaction monetary-transaction, unbanked, subscriber member profile account, mobile-wallet mobile-purse mobile-payment Google-wallet smart-wallet mobile-banking mobile-commerce, fund account-balance account-amount available-fund stored-value top-up...

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X – Y	US 2009/0119190 A1 (REALINI) 07 May 2009 (07.05.2009) entire document, especially Abstract; para [0026], [0029], [0033], [0135], [0136], [0171], [0176]-[0178], [0180], [0186], [0189], [0193], [0194], [0196], [0206], [0253], [0254], [0260], [0264], [0267], [0270], [0273], [0328], [0336], [0344], [0351], [0370], [0392], [0393], [0423], [0427], [0440], [0521], [0524], [0529]-[0531], [0577], [0580], [0581], [0586], [0594], [0602], [0612], [0631], [0649], [0661], [0669], [0671], [0679], [0739], [0875], [0897], [0916], [0918], [1065], [1086], [1098], [1169]	20 --- 1-19
Y	US 2006/0253335 A1 (KEENA et al.) 09 November 2006 (09.11.2006) entire document, especially Abstract; para [0012], [0038], [0042]	1-19
Y	US 2009/0265272 A1 (DILL et al.) 22 October 2009 (22.10.2009) entire document, especially Abstract; para [0005], [0067]	13
Y	US 2009/0081989 A1 (WUHRER) 26 March 2009 (26.03.2009) entire document, especially Abstract; para [0007], [0076], [0088], [0106]	16, 17
A	US 2007/0255652 A1 (TUMMINARO et al.) 01 November 2007 (01.11.2007) entire document	1 - 20
A	US 2007/0255620 A1 (TUMMINARO et al.) 01 November 2007 (01.11.2007) entire document	1 - 20
A	US 2006/0287004 A1 (FUQUA) 21 December 2006 (21.12.2006) entire document	1 - 20
A	US 2007/0265984 A1 (SANTHANA) 15 November 2007 (15.11.2007) entire document	1 - 20

☐ 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
09 January 2013 (09.01.2013)	29 JAN 2013
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1144 of 1360

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN C. STRINGHAM
60 EAST SOUTH TEMPLE, SUITE 1000
SALT LAKE CITY, UT 84111

18756.37.1
2/4/13
Article 19 Amendments
2/29/13

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 18756.37.1A	Date of mailing *(day/month/year)* 29 JAN 2013 **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US 12/66013	International filing date *(day/month/year)* 20 November 2012 (20.11.2012)
Applicant MOZIDO, LLC	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   - **When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.
   - **Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9 004 9 011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3)

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer Lee W Young PCT Helpdesk: 571-272-4300 Telephone No. PCT OSP: 571-272-7774

Form PCT/ISA/220 (July 2010)

2/4/13

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1145 of 1360

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 18756.37.1A	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US 12/66013	International filing date *(day/month/year)* 20 November 2012 (20.11.2012)	(Earliest) Priority Date *(day/month/year)* 21 November 2011 (21.11.2011)
Applicant MOZIDO, LLC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2 ☐ **Certain claims were found unsearchable** (see Box No. II).

3. ☐ **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 2

☐ as suggested by the applicant.

☒ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1146 of 1360

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 12/66013

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 20/00 (2013.01)
USPC - 705/78
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 20/00 (2013.01)
USPC -705/78

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 705/64; 705/39 (See Keywords Below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Patbase; Google Scholar
Search Terms: Mobile wallet, payment, third party, other provider, different provider, payment, transaction, purchase, deposit, withdraw, transfer, authorization code, point of sale, agent, operator, cloud, network, confirmation, notify, wallet provider, bill payment, ...

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008/0208762 A1 (ARTHUR et al.), 28 August 2008 (28.08.2008), entire document, especially Abstract; para [0016], [0057], [0065], [0068]-[0069], [0071]-[0074], [0080], [0082], [0119], [0140]	1-20
Y	US 6,873,974 B1 (SCHUTZER), 29 March 2005 (29.03.2005), entire document, especially Abstract; col 3, ln 40 to col 4, ln 20; col 8, ln 60 to col 9, ln 40	1-20
Y	US 2007/0125840 A1 (LAW et al.), 07 June 2007 (07.06.2007), entire document, especially Abstract; para [0033]-[0035], [0042], [0117]-[0120], [0150]-[0152]	9-11 and 15-17
A	US 2009/0234751 A1 (CHAN et al.), 17 September 2009 (17.09.2009), entire document	1-20
A	US 2011/0196788 A1 (LU et al.), 11 August 2011 (11.08.2011), entire document	1-20

☐ 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
15 January 2013 (15.01.2013)	29 JAN 2013
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: JOHN C. STRINGHAM
60 EAST SOUTH TEMPLE
SUITE 1000
SALT LAKE CITY, UT 84111

JCS
M
Written opinion
1/29/13

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)* 29 JAN 2013

Applicant's or agent's file reference
18756.8.1A

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 12/40131	31 May 2012 (31.05.2012)	03 June 2011 (03.06.2011)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06Q 20/00 (2012.01)
USPC - 705/65

Applicant MOZIDO, LLC

1 This opinion contains indications relating to the following items:

- [X] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [X] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2 FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1 *bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	09 January 2013 (09.01.2013)	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

2/4/13

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1148 of 1360

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No
PCT/US 12/40131

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished

a. (means)

☐ on paper;

☐ in electronic form;

b. (time)

☐ in the international application as filed

☐ together with the international application in electronic form

☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished

5. Additional comments

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1149 of 1360

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 12/40131

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1 Statement

Novelty (N)	Claims	1-19	YES
	Claims	20	NO
Inventive step (IS)	Claims	None	YES
	Claims	1 - 20	NO
Industrial applicability (IA)	Claims	1 - 20	YES
	Claims	None	NO

2. Citations and explanations:

Claim 20 lacks novelty under PCT Article 33(2) as being anticipated by US 2009/0119190 A1 (Realini).

As to claim 20, Realini teaches a monetary transaction system, comprising: a mobile wallet application configured to perform one or more of the following: process incoming and outgoing transactions, authenticate transaction system subscribers, manage subscriber profiles, and manage interactions between monetary transaction system components (para [0875], [1168]); a monetary transaction processor configured to perform one or more of the following: manage account balances for mobile wallet subscribers, manage mobile wallet agent accounts, process balance inquiries, account credits, account debits, and transaction roll-backs (para [0336]); a mobile wallet rules engine that manages and applies rules and policies that are defined for transactions as the transactions are processed on the mobile wallet transaction system including rules that control at least one of the following: transaction fees, transaction limits, transaction velocity limits, commissions, mobile transaction system roles and permissions (para [0581]); a mobile wallet integration module that manages interaction between the mobile wallet transaction system and one or more external transaction systems including at least one of a wireless service provider's billing platform and a program partner bank (para [0669], [0875]); a mobile wallet database that stores mobile wallet transaction data used in mobile wallet transactions including one or more of the following: subscriber profiles, subscription data, transaction data, transaction logs, mobile wallet application configuration data and mobile wallet application run-time data (para [0423] - subscription fees; para [1065] - profile; para [1108] - runtime); and a mobile wallet wireless service that interfaces with the wireless service provider's network to allow communication between the mobile wallet application and other mobile wallet transaction system components via the wireless service provider's network (para [1098]).

Claims 1-12, 14, 15, 18 and 19 lack an inventive step under PCT Article 33(3) as being obvious over Realini in view of US 2006/0253335 A1 to Keena et al. (hereinafter, 'Keena').

As to claim 1, Realini teaches a monetary transaction system for conducting monetary transactions between unbanked subscribers and other entities, the system comprising (para [0029]); a mobile device configured to run a monetary transaction system application (para [0029]); an unbanked monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the unbanked subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system (para [0264]); a monetary transaction system processor that performs the one or more transactions specified by the unbanked subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile (para [0033]);

but fails to explicitly disclose at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system.

However, Keena does teach at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system (para [0012] - profiles; para [0038] - subscribers are not banked).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the virtual pooled account for mobile banking of Realini with the cash based purchasing using mobile communication of Keena, because Realini and Keena are directed to systems and methods for monetary transaction system. Furthermore, users and designers benefit from systems and/or methods adapted for enabling service providers or suppliers to pay a commission to point of sale vendors for use of the vendor's account and point of sale device to perform transactions for customers, because such systems/methods provides a system and method for cash based purchasing using electronic commerce channels such as mobile telephone networks (Keena, para [0012]).

As to claim 2, in combination with Realini, Keena further discloses wherein the monetary transaction system application provides a web interface that allows subscribers to perform the same functions provided by the monetary transaction system application (para [0042]).

As to claim 3, in combination with Keena, Realini further discloses wherein the monetary transaction system application is provided on a prepaid or postpaid phone (para [0253]).

- Please See Supplemental Box -

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1150 of 1360

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 12/40131

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:
Box V.2. Citations and explanations:

As to claim 4, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to enroll a user for a mobile wallet, including the following steps: receiving a subscriber-initiated transaction over one of a plurality of channels connected to the monetary transaction system (para [0631]); prompting for and receiving enrollment information for the unbanked subscriber over at least one of the plurality of channels (para [0171]); sending activation instructions over a second channel to activate the unbanked subscriber and create a subscriber account for the unbanked subscriber (para [0344]); generating a mobile wallet for the unbanked subscriber (para [0440]); and presenting the unbanked subscriber's account data associated with the mobile wallet to the unbanked subscriber (para [0186], [0875])

As to claim 5, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to add a mobile wallet platform stored value account to a mobile wallet, including the following steps: receiving subscriber data over one of a plurality of channels connected to the mobile wallet transaction system (para [0136], [0631]); performing one or more validation checks on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber (para [0351]); sending subscriber data to the at least one entity for identification of the unbanked subscriber, wherein the entity comprises a third party verification system (para [0270]-[0273]); receiving results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber (para [0440]); creating a stored value account for the unbanked subscriber, wherein the monetary transaction system processor maintains a recorded balance for the created stored value account (para [0679]); adding the stored value account to the unbanked subscriber's mobile wallet (para [0679]); and notifying the unbanked subscriber of the addition of the stored value account over at least one other of the plurality of channels connected to the mobile wallet platform (para [0631], [0649]).

As to claim 6, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to add a third party stored value account to a mobile wallet, including the following steps: receiving unbanked subscriber data, including account details, over one of a plurality of channels connected to the monetary transaction system (para [0206], [0440], [0531]); performing one or more validation checks on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber (para [0440]); sending subscriber data to the at least one entity for identification of the unbanked subscriber, wherein the entity comprises a third party verification system (para [0186]); receiving results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber (para [0270]-[0273]); submitting one or more of the unbanked subscriber's account details to a third party account processor (para [0440]); receiving an indication from the third party account processor that third party account processor created a third party stored value account for the subscriber (para [0679]); maintaining a link between the subscriber data and the third party stored value account (para [0679]); adding the third party stored value account to the unbanked subscriber's mobile wallet (para [0875]); and notifying the unbanked subscriber of the addition of the third party stored value account over at least one other of the plurality of channels connected to the monetary transaction system (para [0631], [0649]).

As to claim 7, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to deposit funds at an agent branch through a mobile wallet, including the following steps: receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system, the agent communication indicating that the unbanked subscriber desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account (para [0440]); validating the status of the unbanked subscriber's mobile wallet account (para [0351]); determining if the agent branch is authorized to receive deposited money (para [0586]); performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account (para [0427], [0594]); crediting the unbanked subscriber's mobile wallet account with the specified amount of funds (para [0440], [0975]); returning a notification to the agent branch confirming the deposit (para [0739], [0916]); and notifying the subscriber that the specified amount of funds was deposited in the unbanked subscriber's mobile wallet account over at least one of the plurality of channels connected to the monetary transaction system (para [0897])

As to claim 8, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to withdraw funds at an agent branch using a mobile wallet, including the following steps: receiving a communication from the unbanked subscriber over one of a plurality of channels connected to the monetary transaction system, the communication indicating that the unbanked subscriber desires to withdraw a specified amount of funds from the unbanked subscriber's mobile wallet account at the agent branch (para [0586]); validating the status of the unbanked subscriber's mobile wallet account (para [0351]); determining if the balance of the unbanked subscriber's mobile wallet account is sufficient to accommodate the requested withdrawal for the specified amount of funds (para [0028]); performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account (para [0427], [0594]); returning a secure, perishable withdrawal code to the subscriber over at least one of the plurality of channels connected to the monetary transaction system (para [0577]); receiving subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system, the agent branch communication indicating that the withdrawal code has been presented to the agent branch (para [1086]); debiting the unbanked subscriber's mobile wallet account by the specified amount of funds (para [0392]); returning a notification to the agent branch confirming the withdrawal (para [0739], [0916]); and notifying the subscriber that the specified amount of funds was withdrawn from the unbanked subscriber's mobile wallet account over at least one of the channels connected to the monetary transaction system (para [0897])

As to claim 9, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to pay a bill from a mobile wallet, including the following steps: receiving a subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to pay a bill for a specified amount using a specified payment method from the unbanked subscriber's mobile wallet (para [0028]); validating the status of the selected payment method (para [0661], [0671]); performing one or more of a limit check and a velocity check on the selected payment method (para [0427], [0594]); debiting the specified payment method by the specified amount of funds (para [0392]); processing the bill payment via at least one of a direct biller connection and a bill pay aggregator (para [0028], [0254]); and notifying the unbanked subscriber that the bill was paid over at least one of the plurality of channels connected to the monetary transaction system (para [0897]).

- Please See Supplemental Box

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1151 of 1360

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 12/40131

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of
Box V.2. Citations and explanations:

As to claim 10, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to buy airtime on a prepaid mobile account from a mobile wallet, including the following steps: receiving subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to top up a prepaid mobile account by a specified amount using a specified payment method from the unbanked subscriber's mobile wallet (para [0440]); validating the status of the selected payment method (para [0612]); performing at least one of a limit check and a velocity check on the selected payment method (para [0427], [0594]); debiting the specified payment method by the specified amount of funds (para [0392]); processing the mobile top-up via at least one of a billing system integrator and an aggregator (para [0180]); and notifying the subscriber that the prepaid mobile account was topped up over at least one of the plurality of channels connected to the monetary transaction system (para [0180], [0897]).

As to claim 11, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to transfer money between mobile wallets, including the following steps: receiving subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to transfer a specified amount of funds to specified recipient using a specified payment method from the subscriber's mobile wallet (para [0175], [0440]); validating the status of the selected payment method (para [0612]); performing at least one of a limit check and a velocity check on the selected payment method (para [0427], [0594]); validating the status of the specified recipient to ensure the specified recipient has a valid mobile wallet account (para [0612]); debiting the specified payment method by the specified amount of funds (para [0392]); transferring the specified amount of funds to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system (para [0176]); notifying the unbanked subscriber that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system (para [0176], [0631]).

As to claim 12, in combination with Keena, Realini further discloses wherein validating the status of the specified recipient comprises performing a check on the specified recipient to comply with the office of foreign assets control (para [0580]).

As to claim 14, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to make a purchase from a mobile wallet, including the following steps: receiving a communication from a subscriber over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to purchase an item for a specified amount of funds using a specified payment method from the unbanked subscriber's mobile wallet (para [0529]); returning a secure, perishable purchase code to the unbanked subscriber over at least one of the plurality of channels connected to the monetary transaction system (para [0529], [0577]); receiving subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system, the agent branch communication indicating that the purchase code has been presented to an agent (para [0529]); validating the status of the specified payment method (para [0427]); determining if the specified payment method can accommodate a purchase for the specified amount (para [0524]); performing at least one of a limit check and a velocity check on the selected payment method (para [0529], [0427], [0594]); debiting the specified payment method by the specified amount of funds (para [0521]); returning a notification to the agent branch authorizing the purchase (para [0529]); and sending a receipt to the unbanked subscriber over at least one of the plurality of channels connected to the monetary transaction system (para [0176], [0631]).

As to claim 15, Realini teaches a monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising: a mobile device configured to run a monetary transaction system application (para [0260], [0427]); a monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system (para [0530]); a monetary transaction system processor that performs the one or more transactions specified by the subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile (para [0033], [0916]);
but fails to explicitly disclose at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system.
However, Keena does teach at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system (para [0012] - profiles; para [0038] - subscribers are not banked).
It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the virtual pooled account for mobile banking of Realini with the cash based purchasing using mobile communication of Keena, because Realini and Keena are directed to systems and methods for monetary transaction system. Furthermore, users and designers benefit from systems and/or methods adapted for enabling service providers or suppliers to pay a commission to point of sale vendors for use of the vendor's account and point of sale device to perform transactions for customers, because such systems/methods provides a system and method for cash based purchasing using electronic commerce channels such as mobile telephone networks (Keena, para [0012]).

As to claim 18, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to deposit funds into a bank or credit union account using a mobile wallet, including the following steps: receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system, the agent communication indicating that a subscriber desires to deposit a specified amount of funds into a bank or credit union account (para [0177], [0529]); validating the status of the bank or credit union account (para [0328]); determining if the agent branch is authorized to deposit money (para [0586]); performing one or more of a limit check and a velocity check on the bank or credit union account (para [0427], [0594]); crediting the bank or credit union account with the specified amount of funds (para [0393]); returning a notification to the agent branch confirming the deposit (para [0739], [0918]); and notifying the subscriber that the specified amount of funds was deposited in the bank or credit union account over at least one of the plurality of channels connected to the monetary transaction system (para [0176], [0631]).

- Please See Supplemental Box

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1152 of 1360

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No
PCT/US 12/40131

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of
Box V.2. Citations and explanations:

As to claim 19, in combination with Keena, Realini further discloses wherein the monetary transaction system is implemented to withdraw funds from a bank or credit union account through a mobile wallet, including the following steps: receiving communication from a subscriber over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that a subscriber desires to withdraw a specified amount of funds from a bank or credit union account (para [0179], [0602]); validating the status of the bank or credit union account (para [0370]); determining if the balance of the bank or credit union account is sufficient to accommodate the requested withdrawal for the specified amount of funds (para [0328]); performing at least one of a limit check and a velocity check on the bank or credit union account (para [0427], [0594]); returning a secure, perishable withdrawal code to the subscriber over at least one of the plurality of channels connected to the monetary transaction system (para [0577]); receiving subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system, the agent branch communication indicating that the withdrawal code has been presented to an agent (para [1086]); debiting the bank or credit union account by the specified amount of funds (para [0521]); returning a notification to the agent branch confirming the withdrawal (para [0529]); and notifying the subscriber that the specified amount of funds were withdrawn from the bank or credit union account over at least one of the plurality of channels connected to the monetary transaction system (para [0176], [0631]).

Claim 13 lacks an inventive step under PCT Article 33(3) as being obvious over Realini in view of Keena, and further in view of US 2009/0265272 A1 to Dill et al. (hereinafter, "Dill").

As to claim 13, the combination of Realini and Keena teaches the monetary transaction system of claim 11, but fails to explicitly disclose wherein the money is transferred internationally between the mobile wallets. However, Dill does teach wherein the money is transferred internationally between the mobile wallets (para [0067]). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the virtual pooled account for mobile banking of Realini (as enhanced by Keena) with the money transfers utilizing a unique receiver identifier of Dill, because Realini, Keena and Dill are directed to systems and methods for monetary transaction system. Furthermore, users and designers benefit from systems and/or methods adapted for enabling the data of the request to be verified by the mobile application of the money transfer facilitator, the response may include information related to and/or describing fees, legal notices, etc., because such systems/methods allow for allowing financial transfers that utilize a unique identifier to facilitate flexible payment options for the transaction (Dill, para [0005]).

Claims 16 and 17 lack an inventive step under PCT Article 33(3) as being obvious over Realini in view of Keena, and further in view of US 2009/0081989 A1 (Wuhrer).

As to claim 16, the combination of Realini and Keena teaches the monetary transaction system of claim 15, and Realini further teaches wherein the monetary transaction system is implemented to add a bank or credit union account to a mobile wallet, including the following steps: receiving subscriber data, including bank or credit union account details, over at least one of a plurality of channels connected to the monetary transaction system (para [0177], [0875]); sending subscriber data to a third party verification system for identification of the subscriber (para [0194]); receiving results from the third party system indicating that the subscriber data appropriately identifies the subscriber (para [0189], [0193]); submitting bank or credit union account details for validation by the transaction processor (para [0196]); receiving an indication that the bank or credit union account details correspond to a valid bank or credit union account (para [0135]); maintaining a link between the subscriber data and the bank or credit union account (para [0176]); and notifying the subscriber of the bank or credit union account validation over at least one of the plurality of channels connected to the monetary transaction system (para [0176], [0631]);

but fails to explicitly disclose performing one or more validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber.

However, Wuhrer does teach performing one or more validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber (para [0076], [0098], [0106]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the virtual pooled account for mobile banking of Realini (as enhanced by Keena) with the system and method for financial transaction interoperability across multiple mobile networks of Wuhrer, because Realini, Keena and Wuhrer are directed to systems and methods for monetary transaction system. Furthermore, users and designers benefit from systems and/or methods adapted for enabling a mobile device to execute transactions via the system, and in some embodiments, transactions originate from a third party application through system platform APIs for the reload application and the gifting application; the system is coupled to multiple accounts of the user, including for example, a system account, a debit card account, a credit card account, a PayPal account, multiple prepaid accounts 364 and a bank account, because such systems/methods provide a platform and application layer that can function across an array of payment platforms or network types (Wuhrer, para [0007]).

Please See Supplemental Box -

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1153 of 1360

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:
Box V.2 Citations and explanations:

As to claim 17, the combination of Realini and Keena teaches the monetary transaction system of claim 1, and Realini further teaches wherein the monetary transaction system is implemented to add a debit or credit card account to a mobile wallet, including the following steps: receiving subscriber data, including a debit or credit card account number, over one of a plurality of channels connected to the monetary transaction system (para [0136]); sending subscriber data to a third party verification system for identification of the subscriber (para [0194]); receiving results from the third party system indicating that the subscriber data appropriately identifies the subscriber (para [0189], [0193]); securely storing the debit or credit card account number for access by the mobile wallet (para [0267], [0875]); adding the debit or credit card account number to the subscriber's mobile wallet (para [0267], [0875]); and notifying the subscriber of the addition of the debit or credit card account number over at least one of the plurality of channels connected to the monetary transaction system (para [0176], [0831]);

but fails to explicitly disclose performing one or more validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber.

However, Wuhrer does teach performing one or more validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber (para [0076], [0088], [0106]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the virtual pooled account for mobile banking of Realini (as enhanced by Keena) with the system and method for financial transaction interoperability across multiple mobile networks of Wuhrer, because Realini, Keena and Wuhrer are directed to systems and methods for monetary transaction system. Furthermore, users and designers benefit from systems and/or methods adapted for enabling a mobile device to execute transactions via the system, and in some embodiments, transactions originate from a third party application through system platform APIs for the reload application and the gifting application; the system is coupled to multiple accounts of the user, including for example, a system account, a debit card account, a credit card account, a PayPal account, multiple prepaid accounts 364 and a bank account, because such systems/methods provide a platform and application layer that can function across an array of payment platforms or network types (Wuhrer, para [0007]).

Claims 1 - 20 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used in industry.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1154 of 1360

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To JOHN C. STRINGHAM
60 EAST SOUTH TEMPLE, SUITE 1000
SALT LAKE CITY, UT 84111

18756.37.1a
2/4/13
Written Opinion

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	29 JAN 2013
Applicant's or agent's file reference 18756.37.1A	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 12/66013	20 November 2012 (20.11.2012)	21 November 2011 (21.11.2011)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06Q 20/00 (2013.01)
USPC - 705/78

Applicant MOZIDO, LLC

1. This opinion contains indications relating to the following items:

- [X] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [X] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2 **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1 *bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	16 January 2013 (16.01.2013)	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

2/4/13

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1155 of 1360

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 12/66013

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4 ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished

5. Additional comments:

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1156 of 1360

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 12/66013

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-20	YES
	Claims	None	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-20	NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-8, 12-14 and 18-20 lack an inventive step under PCT Article 33(3) as being obvious over US 2008/0208762 A1 to Arthur et al. (hereinafter 'Arthur') in view of US 6,873,974 B1 (Schutzer).

Regarding claim 1, Arthur teaches a cloud-based transaction platform including (Abstract): one or more processors (para [0016], [0065]); system memory (para [0065]); one or more computer-readable storage media having stored thereon computer executable instructions that, when executed by the one or more processors, cause the computing system to perform a method for performing a transaction using a mobile wallet, the method comprising the following (Abstract; para [0016], [0057], [0140]): an act of receiving communication from an agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that a customer desires to perform a mobile wallet transaction using their mobile wallet (para [0068]-[0069], [0071]-[0074], [0080], [0082], [0119]); an act of sending the agent communication to a mobile wallet platform (para [0080]-[0082], [0120]-[0123]); an act of receiving communication from the mobile wallet platform confirming processing of the transaction (para [0087]-[0090], [0121]-[0125]); and an act of sending communication to the agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the communication indicating confirmation of the processing of the transaction (para [0087]-[0090], [0121]-[0125]). Arthur does not specifically teach the mobile wallet is a third party mobile wallet. However, Schutzer teaches a payment processing system, wherein the payment system accepts and process account transaction requests from third party mobile wallets (Abstract; col 3, ln 40 to col 4, ln 20; col 8, ln 60 to col 9, ln 40). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur with those of Schutzer since doing so would enhance the flexibility of mobile users by allowing payments using third party mobile wallets.

Regarding claim 2, Schutzer teaches a transaction is performed by a second, different customer using a second, different third party mobile wallet (col 7, ln 7-53; col 8, ln 60 to col 9, ln 40).

Regarding claim 3, Schutzer teaches the third party mobile wallet platform comprises a third party processor (col 9, ln 5-63).

Regarding claim 4, Schutzer teaches the transaction using a third party mobile wallet comprises one or more of a deposit, a withdrawal, a transfer, a purchase, a bill payment, or topping up of a prepaid mobile account (col 5, ln 57 to col 6, ln 10 - purchase).

Regarding claim 5, Arthur teaches comprising an act of notifying the customer of confirmation of the processing of the transaction using the mobile wallet over at least one of the plurality of communication channels connected to the cloud-based transaction platform (para [0121]-[0125]).

Regarding claim 6, Schutzer teaches the third party mobile wallet is provided by a third party mobile wallet provider (Abstract; col 3, ln 40 to col 4, ln 20; col 8, ln 60 to col 9, ln 40).

Regarding claim 7, Arthur teaches each mobile wallet provider has their own point of sale (POS) processing system (para [00068]-[0072], [0087]-[0090]).

Regarding claim 8, Arthur teaches the mobile wallet providers' POS processing systems communicate with each other using the cloud-based transaction platform to process the transaction (para [0068]-[0072], [0083]-[0087]).

Regarding claim 12, Arthur teaches the transaction comprises making a purchase from a mobile wallet managed by a mobile wallet platform, including: an act of receiving communication from the customer over one of the plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's mobile wallet (para [0080]-[0082], [0120]-[0123]); an act of returning a secure, perishable purchase code to the customer over at least one of the plurality of channels connected to the cloud-based transaction platform (para [0067]-[0070], [0073]-[0074]); an act of receiving communication from the agent terminal over at least one of the plurality of channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code has been presented to an agent (para [0067]-[0070], [0073]-[0074]); an act of debiting the customer's mobile wallet by the specified amount of funds (para [0087]-[0090], [0121]-[0125]).

--- (See Continuation in Supplemental Box) ---

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1157 of 1360

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2 Citations and Explanations.

Regarding claim 13, Arthur teaches a cloud-based transaction platform including: one or more processors (para [0016], [0065]); system memory (para [0065]); one or more computer-readable storage media having stored thereon computer- executable instructions that, when executed by the one or more processors, cause the computing system to perform a method for performing a transaction using a point of sale (POS) system, the method comprising (Abstract; para [0016], [0057], [0140]): an act of receiving communication from a specified POS system implemented at an agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the POS communication indicating that a customer has initiated a mobile wallet transaction using their mobile wallet (para [0068]-[0069], [0071]-[0074], [0080], [0082], [0119]); an act of sending the POS communication to a corresponding transaction processing system that has been established to process POS transactions from the specified POS system (para [0080]-[0082], [0120]-[0123]); an act of receiving communication from the POS transaction processing system confirming processing of the transaction (para [0087]-[0090], [0121]-[0125]); and an act of sending communication to the specified POS system implemented at the agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the communication indicating confirmation of the processing of the transaction (para [0087]-[0090], [0121]-[0125]). Arthur does not specifically teach the mobile wallet is a third party mobile wallet. However, Schutzer teaches a payment processing system, wherein the payment system accepts and process account transaction requests from third party mobile wallets (Abstract; col 3, ln 40 to col 4, ln 20; col 8, ln 60 to col 9, ln 40). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur with those of Schutzer since doing so would enhance the flexibility of mobile users by allowing payments using third party mobile wallets.

Regarding claim 14, Arthur teaches the act of receiving a transaction fee paid by the specified POS system to the cloud-based transaction platform (para [0063]-[0068], [0084]-[0087]).

Regarding claim 18, Arthur teaches the transaction comprises making a purchase from a mobile wallet provided by a mobile wallet provider, including: an act of receiving communication from the customer over one of the plurality of communication channels connected to the mobile wallet platform, the customer communication indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's mobile wallet (para [0080]-[0082], [0120]-[0123]); an act of returning a secure, perishable purchase code to the customer over at least one of the plurality of communication channels connected to the cloud based transaction platform and an act of receiving subsequent agent terminal communication over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code has been presented to an agent (para [0067]-[0070], [0073]-[0074]); an act of validating the status of the specified payment method and an act of determining if the specified payment method can accommodate a purchase for the specified amount (para [0067]-[0070], [0073]-[0074]); an act of performing one or more of a limit check and a velocity check on the specified payment method and an act of debiting the customer's mobile wallet by the specified amount of funds by sending communication to the mobile wallet provider and an act of returning a notification to the POS system at the agent terminal authorizing the purchase (para [0087]-[0090], [0121]-[0125]); an act of sending a receipt to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform (para [0121]-[0125]).

Regarding claim 19, Arthur teaches a cloud-based transaction platform including: one or more processors (para [0016], [0065]); system memory (para [0065]); one or more computer-readable storage media having stored thereon computer-executable instructions that, when executed by the one or more processors, cause the computing system to perform a method for making a purchase from a mobile wallet provided by a mobile wallet provider, the method comprising the following (Abstract; para [0016], [0057], [0140]): an act of receiving communication from a customer over one of a plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's mobile wallet (para [0068]-[0069], [0071]-[0074], [0080], [0082], [0119]); an act of returning a secure, perishable purchase code to the customer over at least one the plurality of communication channels connected to the cloud-based transaction platform (para [0080]-[0082], [0120]-[0123]); an act of receiving communication from an agent terminal over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code has been presented to an agent (para [0087]-[0090], [0121]-[0125]); and an act of debiting the customer's mobile wallet by the specified amount of funds (para [0087]-[0090], [0121]-[0125]). Arthur does not specifically teach the mobile wallet is a third party mobile wallet. However, Schutzer teaches a payment processing system, wherein the payment system accepts and process account transaction requests from third party mobile wallets (Abstract; col 3, ln 40 to col 4, ln 20; col 8, ln 60 to col 9, ln 40). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur with those of Schutzer since doing so would enhance the flexibility of mobile users by allowing payments using third party mobile wallets.

Regarding claim 20, Schutzer teaches the item purchased by the customer comprises at least one of the following: health care services, music, games, and movies (col 6, ln 10-38 - purchase goods or services available on the web site).

--- (See Continuation in Supplemental Box) ---

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1158 of 1360

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2 Citations and Explanations.

Claims 9-11 and 15-17 lack an inventive step under PCT Article 33(3) as being obvious over Arthur in view of Schutzer and further in view of US 2007/0125840 A1 to Law et al. (hereinafter 'Law').

Regarding claim 9, neither Arthur nor Schutzer teaches the transaction comprises depositing funds into a mobile wallet owned by an entity different than the customer, including: an act of receiving communication from the agent terminal over one of the plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that the customer desires to deposit a specified amount of funds into their mobile wallet; and an act of crediting the mobile wallet with the specified amount of funds However, Law teaches the transaction comprises depositing funds into a mobile wallet owned by an entity different than the customer, including: an act of receiving communication from the agent terminal over one of the plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that the customer desires to deposit a specified amount of funds into their mobile wallet (para [0033]-[0035], [0150]-[0152]); and an act of crediting the mobile wallet with the specified amount of funds (para [0042], [0150]-[0152]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe deposit of money to mobile wallet account.

Regarding claim 10, neither Arthur nor Schutzer teaches the transaction comprises withdrawing funds from a third party mobile wallet owned by an entity different than the customer, including: an act of receiving communication from the customer over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet; an act of returning a secure, perishable withdrawal code to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform; an act of receiving communication from the agent terminal over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the withdrawal code has been presented to an agent; and an act of debiting the third party mobile wallet by the specified amount of funds. However, Law teaches the transaction comprises withdrawing funds from a mobile wallet owned by an entity different than the customer, including: an act of receiving communication from the customer over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the mobile wallet (para [0149]-[0152]); an act of returning a secure, perishable withdrawal code to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform and an act of receiving communication from the agent terminal over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the withdrawal code has been presented to an agent (para [0040]-[0043], [0117]-[0120]) an act of debiting the mobile wallet by the specified amount of funds (para [0102]-[0103], [0150]-[0151]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe withdrawal of money to mobile wallet account.

Regarding claim 11, neither Arthur nor Schutzer teaches the transaction comprises transferring money from a third party mobile wallet within the cloud-based transaction platform to a recipient at a second third party mobile wallet provided by a second mobile wallet provider, the method comprising: an act of receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that a customer desires to transfer a specified amount of funds to a specified recipient using a specified payment method from the third party mobile wallet; an act of debiting the third party mobile wallet by the specified amount of funds; and an act of transferring the specified amount of funds from the cloud-based transaction platform to the second different third party mobile wallet platform for delivery to the specified recipient, the specified amount of funds being transferred over at least one of the plurality of channels connected to the second third party mobile wallet platform. However, Law teaches the transaction comprises transferring money from a mobile wallet within the cloud-based transaction platform to a recipient at a second mobile wallet provided by a second mobile wallet provider, the method comprising: an act of receiving customer communication over one of the plurality of communication channels connected to the cloud based transaction platform, the customer communication indicating that a customer desires to transfer a specified amount of funds to a specified recipient using a specified payment method from the mobile wallet (para [0114]-[0118], [0140]-[0143]); an act of debiting the mobile wallet by the specified amount of funds and an act of transferring the specified amount of funds from the cloud-based transaction platform to the second different mobile wallet platform for delivery to the specified recipient, the specified amount of funds being transferred over at least one of the plurality of channels connected to the second mobile wallet platform (para [0114]-[0118], [0140]-[0143]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe transfer of money to mobile wallet account.

--- (See Continuation in Supplemental Box) ---

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1159 of 1360

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of:
Box V.2 Citations and Explanations.

Regarding claim 15, neither Arthur nor Schulzer the transaction comprises depositing funds into a third party mobile wallet provided by a third party mobile wallet provider, including: an act of receiving communication from the specified POS system implemented at the agent terminal over one of the plurality of channels connected to the cloud-based transaction platform, the POS communication indicating that the customer desires to deposit a specified amount of funds into the third party mobile wallet provided by the third party mobile wallet provider; an act of validating the status of the third party mobile wallet provided by the third party mobile wallet provider; an act of determining if the specified POS system implemented at the agent terminal is authorized to deposit money; an act of performing one or more of a limit check and a velocity check on the third party mobile wallet provided by the third party mobile wallet provider; an act of crediting the third party mobile wallet provided by the third party mobile wallet provider with the specified amount of funds; an act of returning a notification to the specified POS system implemented at the agent terminal confirming the deposit; and an act of notifying the customer that the specified amount of funds were deposited in the third party mobile wallet provided by the third party mobile wallet provider over at least one of the plurality of communication channels connected to the cloud-based transaction platform. However, Law teaches the transaction comprises depositing funds into a mobile wallet provided by a mobile wallet provider, including: an act of receiving communication from the specified POS system implemented at the agent terminal over one of the plurality of channels connected to the cloud-based transaction platform, the POS communication indicating that the customer desires to deposit a specified amount of funds into the mobile wallet provided by the mobile wallet provider (para [0033]-[0035], [0150]-[0152]); an act of validating the status of the mobile wallet provided by the mobile wallet provider and an act of determining if the specified POS system implemented at the agent terminal is authorized to deposit money and an act of performing one or more of a limit check and a velocity check on the mobile wallet provided by the mobile wallet provider (para [0040]-[0043], [0118]-[0123]); an act of crediting the mobile wallet provided by the mobile wallet provider with the specified amount of funds (para [0042], [0150]-[0152]); an act of returning a notification to the specified POS system implemented at the agent terminal confirming the deposit and an act of notifying the customer that the specified amount of funds were deposited in the mobile wallet provided by the mobile wallet provider over at least one of the plurality of communication channels connected to the cloud-based transaction platform (para [0147]-[0151]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe deposit of money to mobile wallet account.

Regarding claim 16, neither Arthur nor Schutzer teaches the transaction comprises withdrawing funds from a third party mobile wallet provided by a third party mobile wallet provider, including: an act of receiving communication from a customer over one of the plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet provided by the third party mobile wallet provider; an act of validating the status of the third party mobile wallet provided by the third party mobile wallet provider; an act of determining if the balance of the third party mobile wallet provided by the third party mobile wallet provider is sufficient to accommodate the requested withdrawal for the specified amount of funds; an act of performing one or more of a limit check and a velocity check on the third party mobile wallet; an act of returning a secure, perishable withdrawal code to the customer over at least one of the plurality of channels connected to the cloud-based transaction platform; an act of receiving subsequent POS communication over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the POS communication indicating that the withdrawal code has been presented to an agent; an act of debiting the third party mobile wallet provided by the third party mobile wallet provider by the specified amount of funds; an act of returning a notification to the POS system at the agent terminal confirming the withdrawal; and an act of notifying the customer that the specified amount of funds were withdrawn from the third party mobile wallet over at least one of the plurality of communication channels connected to the cloud-based transaction platform. However, Law teaches the transaction comprises withdrawing funds from a mobile wallet provided by a mobile wallet provider, including: an act of receiving communication from a customer over one of the plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the mobile wallet provided by the mobile wallet provider (para [0149]-[0152]); an act of validating the status of the mobile wallet provided by the mobile wallet provider and an act of determining if the balance of the mobile wallet provided by the mobile wallet provider is sufficient to accommodate the requested withdrawal for the specified amount of funds and an act of performing one or more of a limit check and a velocity check on the mobile wallet and an act of returning a secure, perishable withdrawal code to the customer over at least one of the plurality of channels connected to the cloud-based transaction platform (para [0040]-[0043], [0118]-[0123]); an act of receiving subsequent POS communication over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the POS communication indicating that the withdrawal code has been presented to an agent (para [0040]-[0043], [0117]-[0120]); an act of debiting the mobile wallet provided by the mobile wallet provider by the specified amount of funds (para [0102]-[0103], [0150]-[0151]); an act of returning a notification to the POS system at the agent terminal confirming the withdrawal and an act of notifying the customer that the specified amount of funds were withdrawn from the mobile wallet over at least one of the plurality of communication channels connected to the cloud-based transaction platform (para [0147]-[0151]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe withdrawal of money to mobile wallet account.

--- (See Continuation in Supplemental Box) ---

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1160 of 1360

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of
Box V.2 Citations and Explanations.

Regarding claim 17, neither Arthur nor Schutzer teaches the transaction comprises transferring money using a third party mobile wallet provided by a third party mobile wallet provider, including: an act of receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to transfer a specified amount of funds to a specified recipient having a third party mobile wallet, the transfer using a specified payment method from the customer's third party mobile wallet at the cloud-based transaction platform; an act of validating the status of the specified payment method; an act of performing one or more of a limit check and a velocity check on the specified payment method; an act of performing a check on the specified recipient having a third party mobile wallet to comply with the office of foreign assets control; an act of debiting the customer's mobile wallet at the cloud-based transaction platform by the specified amount of funds; an act of transferring the specified amount of funds to third party mobile wallet provider for delivery to the third party mobile wallet of the specified recipient over at least one of the plurality of channels connected between the cloud-based transaction platform and the third party mobile wallet provider; an act of notifying the customer that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the cloud-based transaction platform. However, Law teaches the transaction comprises transferring money using a mobile wallet provided by a mobile wallet provider, including: an act of receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to transfer a specified amount of funds to a specified recipient having a mobile wallet, the transfer using a specified payment method from the customer's mobile wallet at the cloud-based transaction platform (para [0114]-[0118], [0140]-[0143]); an act of validating the status of the specified payment method and an act of performing one or more of a limit check and a velocity check on the specified payment method and an act of performing a check on the specified recipient having a mobile wallet to comply with the office of foreign assets control; an act of debiting the customer's mobile wallet at the cloud-based transaction platform by the specified amount of funds (para [0040]-[0043], [0118]-[0123]); an act of transferring the specified amount of funds to mobile wallet provider for delivery to the mobile wallet of the specified recipient over at least one of the plurality of channels connected between the cloud-based transaction platform and the mobile wallet provider (para [0114]-[0118], [0140]-[0143]); an act of notifying the customer that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the cloud-based transaction platform (para [0147]-[0151]). It would have been obvious to one of ordinary skill in the art to combine the teachings of Arthur and Schutzer with those of Law since doing so would allow easy and safe transfer of money to mobile wallet account.

Claims 1-20 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used in industry

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1161 of 1360

Electronic Patent Application Fee Transmittal	
Application Number:	13484199
Filing Date:	30-May-2012
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Filer:	John C. Stringham/Michelle Stringham
Attorney Docket Number:	18756.8.1.1
Filed as Small Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	15692667
Application Number:	13484199
International Application Number:	
Confirmation Number:	5095
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Customer Number:	22913
Filer:	John C. Stringham/Michelle Stringham
Filer Authorized By:	John C. Stringham
Attorney Docket Number:	18756.8.1.1
Receipt Date:	05-MAY-2013
Filing Date:	30-MAY-2012
Time Stamp:	14:50:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$90
RAM confirmation Number	7528
Deposit Account	233178
Authorized User	STRINGHAM, JOHN C.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 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	Information Disclosure Statement (IDS) Form (SB08)	IDSMay13.pdf	479715 [illegible]	no	8
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	ChenNPL.pdf	539789 [illegible]	no	8
Warnings:					
Information:					
3	Foreign Reference	FR1.pdf	345489 [illegible]	no	7
Warnings:					
Information:					
4	Foreign Reference	FR2.pdf	2355356 [illegible]	no	62
Warnings:					
Information:					
5	Foreign Reference	FR3.pdf	989487 [illegible]	no	22
Warnings:					
Information:					
6	Foreign Reference	FR4.pdf	3691947 [illegible]	no	70
Warnings:					
Information:					
7	Foreign Reference	FR5.pdf	1668825 [illegible]	no	34
Warnings:					
Information:					

8	Foreign Reference	FR6.pdf	2571305 [illegible]	no	41
Warnings:					
Information:					
9	Foreign Reference	FR8.pdf	1253948 [illegible]	no	31
Warnings:					
Information:					
10	Foreign Reference	FR9.pdf	7393956 [illegible]	no	163
Warnings:					
Information:					
11	Foreign Reference	FR10.pdf	1647270 [illegible]	no	40
Warnings:					
Information:					
12	Foreign Reference	FR11.pdf	3553344 [illegible]	no	63
Warnings:					
Information:					
13	Foreign Reference	FR12.pdf	899960 [illegible]	no	23
Warnings:					
Information:					
14	Foreign Reference	FR13.pdf	1307435 [illegible]	no	31
Warnings:					
Information:					
15	Foreign Reference	FR7.pdf	1620533 [illegible]	no	48
Warnings:					
Information:					
16	Foreign Reference	FR14.pdf	1805135 [illegible]	no	33
Warnings:					
Information:					

17	Foreign Reference	FR15.pdf	2795889 [illegible]	no	84
Warnings:					
Information:					
18	Foreign Reference	FR16.pdf	442270 [illegible]	no	8
Warnings:					
Information:					
19	Foreign Reference	FR17.pdf	2108721 [illegible]	no	45
Warnings:					
Information:					
20	Foreign Reference	FR18.pdf	2108720 [illegible]	no	45
Warnings:					
Information:					
21	Foreign Reference	FR19.pdf	53124 [illegible]	no	2
Warnings:					
Information:					
22	Foreign Reference	FR20.pdf	53135 [illegible]	no	2
Warnings:					
Information:					
23	Foreign Reference	FR21.pdf	56331 [illegible]	no	2
Warnings:					
Information:					
24	Foreign Reference	FR22.pdf	168191 [illegible]	no	1
Warnings:					
Information:					
25	Foreign Reference	FR23.pdf	202638 [illegible]	no	1
Warnings:					
Information:					

26	Foreign Reference	FR24.pdf	82000 [illegible]	no	2
Warnings:					
Information:					
27	Foreign Reference	FR25.pdf	44396 [illegible]	no	1
Warnings:					
Information:					
28	Foreign Reference	FR26.pdf	5311333 [illegible]	no	85
Warnings:					
Information:					
29	Foreign Reference	FR27.pdf	5312263 [illegible]	no	85
Warnings:					
Information:					
30	Non Patent Literature	GAONPL.pdf	940035 [illegible]	no	10
Warnings:					
Information:					
31	Non Patent Literature	ISR8 1a.pdf	259972 [illegible]	no	3
Warnings:					
Information:					
32	Non Patent Literature	ISR37 1a.pdf	311401 [illegible]	no	3
Warnings:					
Information:					
33	Non Patent Literature	LabrouNPL.pdf	1092392 [illegible]	no	10
Warnings:					
Information:					
34	Non Patent Literature	MotorolaNPL.pdf	4979512 [illegible]	no	4
Warnings:					
Information:					

35	Non Patent Literature	NPLTechnobiography.pdf	1542743	no	29
Warnings:					
Information:					
36	Non Patent Literature	ValcourtNPL.pdf	535905	no	8
Warnings:					
Information:					
37	Non Patent Literature	WO8 1a.pdf	615197	no	7
Warnings:					
Information:					
38	Non Patent Literature	WO37 1a.pdf	570113	no	7
Warnings:					
Information:					
39	Fee Worksheet (SB06)	fee-info.pdf	30084	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	61739859		

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.

GREGORY R. LUNT
OFFICE DIRECT: 801 321 8948
EMAIL: glunt@WNLAW.COM

ELECTRONICALLY FILED

PATENT APPLICATION
Docket No. 18756.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of		)
	Michael A. Liberty	)
		)
Serial No.:	13/484,199	) Art Unit
		) 3691
Filed:	May 30, 2012	)
		)
Conf. No.:	5095	)
		)
For:	MONETARY TRANSACTION SYSTEM	)
		)
Examiner:	Edward Chang	)
		)
Customer No.:	22913	)

AMENDMENT "A" AND RESPONSE AFTER NON-FINAL

Via E-File AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office action mailed December 26, 2012 (paper no. 20121214), please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper; and

Remarks/Arguments begin on page 8 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A monetary transaction system for conducting monetary transactions between unbanked subscribers and other entities, the system comprising:

a mobile device configured to run a monetary transaction system application;

an unbanked monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the unbanked subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;

a monetary transaction system processor that performs the one or more transactions specified by the unbanked subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile; ~~and~~

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system; and

wherein the monetary transaction system is implemented to deposit funds at an agent branch through a mobile wallet, including performing the following steps:

receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system, the agent communication indicating that the unbanked subscriber desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account;

validating the status of the unbanked subscriber's mobile wallet account;

determining if the agent branch is authorized to receive deposited money;

performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account, the limit check determining whether sufficient funds are available to make the deposit amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1171 of 1360

crediting the unbanked subscriber's mobile wallet account with the specified amount of funds;

returning a notification to the agent branch confirming the deposit; and

notifying the subscriber that the specified amount of funds was deposited in the unbanked subscriber's mobile wallet account over at least one of the plurality of channels connected to the monetary transaction system.

2. (Original) The monetary transaction system of claim 1, wherein the monetary transaction system application provides a web interface that allows subscribers to perform the same functions provided by the monetary transaction system application.

3. (Original) The monetary transaction system of claim 1, wherein the monetary transaction system application is provided on a prepaid or postpaid phone.

4-14. (Cancelled)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1172 of 1360

15. (Currently Amended) A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising:

a mobile device configured to run a monetary transaction system application;

a monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;

a monetary transaction system processor that performs the one or more transactions specified by the subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile; ~~and~~

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system;

wherein the monetary transaction system is implemented to withdraw funds at an agent branch using a mobile wallet, including performing the following steps:

receiving a communication from the unbanked subscriber over one of a plurality of channels connected to the monetary transaction system, the communication indicating that the unbanked subscriber desires to withdraw a specified amount of funds from the unbanked subscriber's mobile wallet account at the agent branch;

validating the status of the unbanked subscriber's mobile wallet account;

determining if the balance of the unbanked subscriber's mobile wallet account is sufficient to accommodate the requested withdrawal for the specified amount of funds;

performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account, the limit check determining whether sufficient funds are available to make the deposit amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period;

returning a secure, perishable withdrawal code to the subscriber over at least one of the plurality of channels connected to the monetary transaction system;

receiving subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system, the agent branch communication indicating that the withdrawal code has been presented to the agent branch;

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1173 of 1360

debiting the unbanked subscriber's mobile wallet account by the specified amount of funds;

returning a notification to the agent branch confirming the withdrawal; and

notifying the subscriber that the specified amount of funds was withdrawn from the unbanked subscriber's mobile wallet account over at least one of the channels connected to the monetary transaction system.

16-20. (Cancelled)

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1174 of 1360

21. (New) A monetary transaction system for conducting monetary transactions between unbanked subscribers and other entities, the system comprising:

a mobile device configured to run a monetary transaction system application;

a monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;

a monetary transaction system processor that performs the one or more transactions specified by the subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile;

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system; and

wherein the monetary transaction system is implemented to transfer money between mobile wallets, including performing the following steps:

receiving subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to transfer a specified amount of funds to specified recipient using a specified payment method from the subscriber's mobile wallet;

validating the status of the selected payment method;

performing at least one of a limit check and a velocity check on the selected payment method, the limit check determining whether sufficient funds are available to make the deposit amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period;

validating the status of the specified recipient to ensure the specified recipient has a valid mobile wallet account;

debiting the specified payment method by the specified amount of funds;

transferring the specified amount of funds to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system;

notifying the unbanked subscriber that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1175 of 1360

22. (New) The monetary transaction system of claim 21, wherein validating the status of the specified recipient comprises performing a check on the specified recipient to comply with the office of foreign assets control.

23. (New) The monetary transaction system of claim 21, wherein the money is transferred internationally between the mobile wallets.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1176 of 1360

REMARKS

Initially, Applicants thank the Examiner for the time spent reviewing the application and preparing the current Office Action.

Claims 15 and 20 were rejected under 35 U.S.C. § 102(b) as being anticipated by Labrou et al. (U.S. Pat. Pub. No. 2005/0187873), hereinafter "Labrou". Claims 1-4 were rejected under 35 U.S.C § 103(a) as being obvious in view of Labrou in view of Valdes et al. (U.S. Pat. Pub. No. 2011/0145149), hereinafter "Valdes". Claims 5-7, 9-13, and 17-18 were rejected under 35 U.S.C § 103(a) as being obvious in view of Labrou, Valdes, and Sato et al., (U.S. Pat. Pub. No. 2008/0204358). Claims 8, 14, and 19 were rejected under 35 U.S.C § 103(a) as being obvious in view of Labrou, Valdes, and Sato and Lyons et al., (U.S. Pat. No. 7,819,307). Claim 16 was rejected under 35 U.S.C § 103(a) as being obvious in view of Labrou and Sato. [1]

By this amendment claims 1 and 15 have been amended, claims 4-14 and 16-20 have been canceled, and claims 21-23 are new.[2] Accordingly, claims 1-3, 15 and 21-23 are pending, of which claims 1, 15 and 21 are the only independent claims at issue.

Embodiments of the claimed invention are generally directed to providing a monetary transaction system for conducting monetary transactions between entities. For example, claim 1 defines a mobile device configured to run a monetary transaction system application. Next, claim 1 defines an unbanked monetary transaction system subscriber that has a profile with the monetary transaction system, where the unbanked subscriber indicates, via the monetary transaction system application, various specified transactions that are to be performed using the monetary transaction system. The monetary transaction system further includes a processor that performs the transactions specified by the unbanked subscriber. Performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile. Still further, the monetary transaction system includes an entity that is to be involved in the specified transaction, the entity having a profile with the monetary transaction system.

---

[1] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

[2] Support for the amendments to the claims and for the new claims is found throughout the specification and previously presented claims, including but not limited to paragraphs [0052], [0058], [0071], [0072], [0107] and Figures 2-6B, 14 and 16.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1177 of 1360

Claim 1 further defines implementing the monetary transaction system to deposit funds at an agent branch through a mobile wallet, including: receiving communication from an agent branch over a communication channel, where the agent communication indicates that the unbanked subscriber desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account. The monetary transaction system then performs steps of validating the status of the unbanked subscriber's mobile wallet account, determining if the agent branch is authorized to receive deposited money, performing a limit check and/or a velocity check on the unbanked subscriber's mobile wallet account, crediting the unbanked subscriber's mobile wallet account with the specified amount of funds, returning a notification to the agent branch confirming the deposit; and notifying the subscriber that the specified amount of funds was deposited in the unbanked subscriber's mobile wallet account over the communication channel.

Applicants respectfully submit that the cited art of record does not anticipate or otherwise render the amended claims unpatentable for at least the reason that the cited art does not disclose, suggest, or enable each and every element of these claims.

35 U.S.C. 103(a) Rejection of Independent Claim 1

As discussed during the interview, the Labrou reference describes a secure transaction server (STS) that performs various actions. For example, as shown in Figure 1A, the STS can select software authentication parameters, create a personal identification entry (PIE) for a mobile device user, store authentication parameters and PIEs in a database, install mobile payment software in a mobile phone and execute a mobile phone user electronically authenticable transaction. The STS allows mobile phone cashless monetary transactions to be performed according to the Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol (par. [0045]). Other transactions include person-to-person transactions (see par. [0119]) and financial transactions such as browsing, selling, buying or transferring stocks, funds or bonds using funds, broker accounts, banks or debit/credit cards (par. [0145]). However, Labrou fails to teach or suggest one or more aspects of the invention as claimed, as indicated on p. 6 of the current Office Action.

To overcome the shortcomings of Labrou, the Valdes reference has been cited. Valdes describes methods, apparatuses, and systems for supporting purchases of goods and services via prepaid telecommunication accounts (Title). The prepaid accounts may include accounts associated with both mobile devices and fixed-line prepaid services such as landline telephone,

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1178 of 1360

cable and/or digital television, and internet access (par. [0056]). If sufficient funds are not available to pay for an item or service, a "facilitation" amount may be advanced to the prepaid account to cover the difference (*Id.*). Valdes also refers to transferring funds from a mobile banking prepaid account to another user or mobile device. Such balance transfers are referred to as "Mobile Banking" or "Banking the Unbanked." (par. [0039]).

The Sato reference is cited primarily to show a timing manager that generates reply timings for display devices, so that the number of display devices capable of sharing a communication channel at the same time does not exceed an allowable number of devices for the channel (par. [0053]). The Lyons reference was cited primarily to show a system that can flag a mobile device as being lost or stolen, or can indicate credit limits on the amount of monetary value to be held by a mobile device (Col. 5:15-20).

However, none of the cited references teach or suggest "performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account", as claimed in claim 1. The Examiner states that the combination of Labrou and Valdes fails to teach or suggest this limitation (as indicated on p. 12 of the Office Action). Sato has been cited as teaching this limitation. The Sato reference describes an advertising system where digital devices display advertisements and report back to a display confirmation server. When reporting back to the server, communication channels get congested, so a timing manager is implemented (see Abs. and par. [0053]). The timing manager generates reply timings so that the number of display devices capable of sharing a communication channel at the same time does not exceed an allowable number of devices for the channel (*Id.*). This has little, if anything, to do with mobile wallets or performing transactions using mobile wallets. Moreover, generating reply timings to limit the number of devices on a communication channel is not the same as performing a limit check (or a velocity check) on a mobile wallet account. The limit check is to determine whether sufficient funds are available to make the deposit amount. The velocity check is to determine whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period. Neither Sato nor the other cited references teach or suggest this limitation.

Accordingly, at least for the reasons outlined above, claim 1 patentably defines over the art of record. At least for any of these same reasons, new claim 21 also patentably defines over the art of record. Since each of dependent claims 2-3 and 22-23 depend from claims 1 and 21, each of the dependent claims also patentably defines over the art of record for at least any of the same reasons.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1179 of 1360

35 U.S.C. 102(b) Rejection of Independent Claims 15 and 20

Claim 20 has been canceled, rendering its 102(b) rejection moot. Claim 15 has been amended to include the following limitation: "performing at least one of a limit check and a velocity check on the selected payment method, the limit check determining whether sufficient funds are available to make the deposit amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period." Claim 15 patentably defines over Labrou for at least any of the same reasons discussed above with regard to claim 1. Indeed, the Examiner has already indicated Labrou's shortcomings regarding this limitation (see at least p. 12 of the current Office Action).

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at (801) 533-9800.

Dated this 26th day of April, 2013.

Respectfully submitted,

/GREGORY R. LUNT/

JOHN C. STRINGHAM
Registration No. 40,831
GREGORY R. LUNT
Registration No. 57,354
Attorneys for Applicant
Customer No. 22913

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1180 of 1360

Electronic Patent Application Fee Transmittal	
Application Number:	13484199
Filing Date:	30-May-2012
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Filer:	GREGORY LUNT/Connie Thompson
Attorney Docket Number:	18756.8.1.1
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	200	200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	200

Electronic Acknowledgement Receipt	
EFS ID:	15626285
Application Number:	13484199
International Application Number:	
Confirmation Number:	5095
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Customer Number:	22913
Filer:	GREGORY LUNT/Connie Thompson
Filer Authorized By:	GREGORY LUNT
Attorney Docket Number:	18756.8.1.1
Receipt Date:	26-APR-2013
Filing Date:	30-MAY-2012
Time Stamp:	16:15:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$200
RAM confirmation Number	5019
Deposit Account	233178
Authorized User	LUNT, GREGORY
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 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	Miscellaneous Incoming Letter	Transmittal.pdf	291514	no	2
Warnings:					
Information:					
2	Extension of Time	Ext_of_Time.pdf	159015	no	2
Warnings:					
Information:					
3		Amend_A.pdf	345236	yes	11

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	11

Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30298	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	826063		

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.

GREGORY R. LUNT
OFFICE DIRECT: 801 321 8948
EMAIL: glunt@wnlaw.com

VIA eFILE

PATENT APPLICATION
Docket No. 18756.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	Michael A. Liberty	)
Serial No.:	13/484,199	) Art Unit) 3691
Filed:	May 30, 2012	)
Conf. No.:	5095	)
For:	MONETARY TRANSACTION SYSTEM	)
Examiner:	Edward Chang	)
Customer No.:	22913	)

TRANSMITTAL FOR AMENDMENT "A"
AND RESPONSE AFTER NON-FINAL

VIA eFILE AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Transmitted herewith is an Amendment "A" and Response for entry in the above-identified application.

__X__ To render the transmitted Amendment "A" and Response timely filed enclosed are the following:

__X__ Petition for One (1) Month Extension of Time ($200.00).

The fee has been calculated as follows:

			SMALL ENTITY		LARGE ENTITY	
CLAIMS REMAINING AFTER	**HIGHEST NO. PREVIOUSLY PAID FOR**	**PRESENT EXTRA**	**RATE**	**ADDT'L FEE**	**RATE**	**ADDT'L FEE**
TOTAL 7	MINUS 20	= 0	X		X $80.00	00.00
INDEPENDENT 3	MINUS 3	= 0	X		X $420.00	00.00
1st PRESENTATION OF MULTIPLE DEPENDENT CLAIM			-		-	
			TOTAL		**TOTAL**	00.00

__X__ Payment in the amount of $200.00 using the Credit Card payment option in E-Filer with RAM will be used to cover the payment of the fees with respect to this Extension of Time.

__X__ The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to **Deposit Account No. 23-3178**: (1) any filing fees required under 37 CFR § 1.16; (2) any patent application and reexamination processing fees under 37 CFR § 1.17; and/or (3) any post issuance fees under 37 CFR § 1.20. In addition, if any additional extension of time is required, which has not otherwise been requested, please consider this a petition therefore and charge any additional fees that may be required to **Deposit Account No. 23-3178**.

Dated this 26th day of April, 2013.

Respectfully submitted,

/GREGORY R. LUNT/

JOHN C. STRINGHAM
Registration No. 40,831
GREGORY R. LUNT
Registration No. 57,354
Attorneys for Applicant
Customer No. 22913

JCS:GRL:crt
4121232_1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744

VIA eFILE

PATENT APPLICATION
Docket No: 18756.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of		)
	Michael A. Liberty	)
		)
Serial No.:	13/484,199	) Art Unit
		) 3691
Filed:	May 30, 2012	)
		)
Conf. No.:	5095	)
		)
For:	MONETARY TRANSACTION SYSTEM	)
		)
Examiner:	Edward Chang	)
		)
Customer No.:	22913	)

PETITION FOR EXTENSION OF TIME

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 37 C.F.R. § 1.136(a), it is respectfully requested that the shortened statutory period which was set for responding to the Office Action dated December 26, 2012 (paper no. 20121214), be extended for One (1) month until April 26, 2013.

Payment in the amount of $200.00 using the Credit Card payment option in E-Filer with RAM will be used to cover the payment of the fees with respect to this extension of time.

The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to Deposit Account No. 23-3178: (1) any filing fees required under 37 CFR § 1.16; (2) any patent application and reexamination

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1188 of 1360

processing fees under 37 CFR § 1.17; and/or (3) any post issuance fees under 37 CFR § 1.20. In addition, if any additional extension of time is required, which has not otherwise been requested, please consider this a petition therefore and charge any additional fees that may be required to Deposit Account No. 23-3178.

DATED this 26th day of April, 2013.

Respectfully submitted,

/GREGORY R. LUNT/

JOHN C. STRINGHAM
Registration No. 40,831
GREGORY R. LUNT
Registration No. 57,354
Attorneys for Applicant
Customer No. 22913

JCS:GRL:crt
4121214_1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1189 of 1360

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/484,199	Filing Date 05/30/2012	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT	04/26/2013	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	(Column 3) ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 7	Minus	** 20	= 0	X $80 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	(Column 3) ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ 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.
** 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 number found in the appropriate box in column 1.

LIE
/BRENDA HARRISON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/484,199	05/30/2012	Michael A. Liberty	18756.8.1.1	5095

22913 7590 12/26/2012

Workman Nydegger
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

EXAMINER	
CHANG, EDWARD	

ART UNIT	PAPER NUMBER
3697	

NOTIFICATION DATE	DELIVERY MODE
12/26/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing@wnlaw.com

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1191 of 1360

Office Action Summary	Application No.	Applicant(s)	
	13/484,199	LIBERTY, MICHAEL A.	
	Examiner	Art Unit	
	EDWARD CHANG	3691	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.

Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *May 30, 2012*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ 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.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, 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.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *May 30, 2012* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

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)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

4) ☐ Other: _____.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1192 of 1360

DETAILED ACTION

Status of Claims

1. This action is in reply to the Application filed on 30th of May 2012.

2. Claims 1-20 are currently pending and have been examined.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 15 and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Labrou et al. (hereinafter "Labrou"); (US 2005/0187873 A1).

As per Claim 15:

Labrou as shown discloses the following limitations:

- *a mobile device configured to run a monetary transaction system application;* (See at least Fig. 1A, Item 106)
- *a monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;* (See at least Paragraph 0043, "...registering a phone number of a mobile phone of the user via the activation link...")
- *a monetary transaction system processor that performs the one or more transactions specified by the subscriber, wherein performing the specified transactions includes*

communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile; and (See at least Paragraph 0119, "...in case of person-to-person payment transaction...will determine if the payee is valid mobile OPS user...")

- *at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system.* (See at least Paragraph 0051, "...wireless wallet application to interface with the merchant retail application software...", merchant = entity)

As per Claim 20:

Labrou as shown discloses the following limitations:

- *a mobile wallet application configured to perform one or more of the following: process incoming and outgoing transactions, authenticate transaction system subscribers, manage subscriber profiles, and manage interactions between monetary transaction system components;* (See at least Paragraph 0019, "...initializing at a secure transaction server...authentication parameter...inputting, by a user, the PIE to the installed authentic mobile payment software to generate according to the PIE and the software authentication parameter...cashless monetary transaction is performed according to an agreement view(s) protocol...").
- *a monetary transaction processor configured to perform one or more of the following: manage account balances for mobile wallet subscribers, manage mobile wallet agent accounts, process balance inquiries, account credits, account debits, and transaction roll-backs;* (See at least Paragraph 0145, "...services comprise various types of financial transactions...")
- *a mobile wallet rules engine that manages and applies rules and policies that are defined for transactions as the transactions are processed on the mobile wallet transaction system including rules that control at least one of the following: transaction fees,*

transaction limits, transaction velocity limits, commissions, mobile transaction system roles and permissions; (See at least Paragraph 0043, "...software authentication parameters...", parameters = rules)

- *a mobile wallet integration module that manages interaction between the mobile wallet transaction system and one or more external transaction systems including at least one of a wireless service provider's billing platform and a program partner bank;* (See at least Fig. 1A, Item 106)
- *a mobile wallet database that stores mobile wallet transaction data used in mobile wallet transactions including one or more of the following: subscriber profiles, subscription data, transaction data, transaction logs, mobile wallet application configuration data and mobile wallet application runtime data; and* (See at least Fig. 3, Item 120)
- *a mobile wallet wireless service that interfaces with the wireless service provider's network to allow communication between the mobile wallet application and other mobile wallet transaction system components via the wireless service provider's network.* (See at least Paragraph 0112, "...enables consumers to make payments to other consumers..."); (See at least Fig. 3, Items 106a, 106b, 310)

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. The factual inquiries set forth in Graham **v.** John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 1-4 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Labrou et al. (hereinafter "Labrou"); (US 2005/0187873 A1) in view of Valdes et al. (hereinafter "Valdes"); (US 2011/0145149 A1).

As per Claim 1:

Labrou as shown discloses the following limitations:

- *a mobile device configured to run a monetary transaction system application;* (See at least Fig. 1A, Item 106)
- *an unbanked monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the unbanked subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;* (See at least Paragraph 0043, "...registering a phone number of a mobile phone of the user via the activation link...")
- *a monetary transaction system processor that performs the one or more transactions specified by the unbanked subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile; and* (See at least Paragraph 0119, "...in case of person-to-person payment transaction...will determine if the payee is valid mobile OPS user...")
- *at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system.* (See at least Paragraph 0051, "...wireless wallet application to interface with the merchant retail application software...", merchant = entity)

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 2:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *wherein the monetary transaction system application provides a web interface that allows subscribers to perform the same functions provided by the monetary transaction system application.* (See at least Paragraph 0038, "...user browses the retailer's web pages using a mobile device...")

As per Claim 3:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Valdes discloses the following limitations:

- *wherein the monetary transaction system application is provided on a prepaid or postpaid phone.* (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 4:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving a subscriber-initiated transaction over one of a plurality of channels connected to the monetary transaction system; prompting for and receiving enrollment information for the unbanked subscriber over at least one of the plurality of channels; sending activation instructions over a second channel to activate the unbanked subscriber and create a subscriber account for the unbanked subscriber; generating a mobile wallet for the unbanked subscriber; and presenting the unbanked subscriber's account data associated with the mobile wallet to the unbanked subscriber.* (See at least Paragraph 0019, "...initializing at a secure transaction server...authentication parameter...inputting, by a user, the PIE to the installed authentic mobile payment software to generate according to the PIE and the software authentication parameter...cashless monetary transaction is performed according to an agreement view(s) protocol...").

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid"

account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

8. Claims 5-7, 9-13, and 17-18 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Labrou and Valdes as applied in claim 1, in further view of Sato et al. (hereinafter "Sato"); (US 2008/0204358 A1).

As per Claim 5:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving subscriber data over one of a plurality of channels connected to the mobile wallet transaction system;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment software...")
- *sending subscriber data to the at least one entity for identification of the unbanked subscriber, wherein the entity comprises a third party verification system; receiving results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *creating a stored value account for the unbanked subscriber, wherein the monetary transaction system processor maintains a recorded balance for the created stored value account;* (See at least Paragraph 0055, "...creates a new wireless wallet executable...")
- *adding the stored value account to the unbanked subscriber's mobile wallet; and* (See at least Paragraph 0145, "...transferring...funds...")

- *notifying the unbanked subscriber of the addition of the stored value account over at least one other of the plurality of channels connected to the mobile wallet platform.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing one or more validation checks on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 6:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving unbanked subscriber data, including account details, over one of a plurality of channels connected to the monetary transaction system;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment software...")
- *sending subscriber data to the at least one entity for identification of the unbanked subscriber, wherein the entity comprises a third party verification system; receiving results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber; submitting one or more of the unbanked subscriber's account details to a third party account processor;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *receiving an indication from the third party account processor that third party account processor created a third party stored value account for the subscriber;* (See at least Paragraph 0031, "...message flow between a requestor device, a secure transaction server...")
- *maintaining a link between the subscriber data and the third party stored value account;* (See at least Fig. 3, Items 120, 200 (108a and 106a)
- *adding the third party stored value account to the unbanked subscriber's mobile wallet; and* (See at least Paragraph 0145, "...transferring...funds...")
- *notifying the unbanked subscriber of the addition of the third party stored value account over at least one other of the plurality of channels connected to the monetary transaction system.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing one or more validation checks on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 7:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system, the agent communication indicating that the unbanked subscriber desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment software..."); (See at least Paragraph 0145, "...transferring...funds...", Fig. 3, Item 310, 315, merchant = agent)

- *validating the status of the unbanked subscriber's mobile wallet account; determining if the agent branch is authorized to receive deposited money;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *crediting the unbanked subscriber's mobile wallet account with the specified amount of funds;* (See at least Paragraph 0145, "...transferring...funds...")
- *returning a notification to the agent branch confirming the deposit; and* (See at least Paragraph 0070, "...merchant also receives a notification of the successful transaction...")
- *notifying the subscriber that the specified amount of funds was deposited in the unbanked subscriber's mobile wallet account over at least one of the plurality of channels connected to the monetary transaction system.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of

accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 9:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving a subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to pay a bill for a specified amount using a specified payment method from the unbanked subscriber's mobile wallet;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment software..."); (See at least Paragraph 0145, "...transferring...funds...", Fig. 3, Item 310, 315, merchant = agent)
- *validating the status of the selected payment method;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *debiting the specified payment method by the specified amount of funds;* (See at least Paragraph 0145, "...transferring...funds...")
- *notifying the unbanked subscriber that the bill was paid over at least one of the plurality of channels connected to the monetary transaction system.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts..."). Also teaches the following limitation:

- *processing the bill payment via at least one of a direct biller connection and a bill pay aggregator; and* (See at least Paragraph 0017, "...billing subsystems...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing one or more of a limit check and a velocity check on the selected payment method;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 10:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to top up a prepaid mobile account by a specified amount using a specified payment method from the unbanked subscriber's mobile wallet;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment

software..."); (See at least Paragraph 0145, "...transferring...funds...", Fig. 3, Item 310, 315, merchant = agent, top up = adding)

- *validating the status of the selected payment method;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *debiting the specified payment method by the specified amount of funds;* (See at least Paragraph 0145, "...transferring...funds...")
- *notifying the subscriber that the prepaid mobile account was topped up over at least one of the plurality of channels connected to the monetary transaction system.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts..."). Also teaches the following limitation:

- *processing the mobile top-up via at least one of a billing system integrator and an aggregator; and* (See at least Paragraph 0017, "...billing subsystems...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing at least one of a limit check and a velocity check on the selected payment method;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of

accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 11:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to transfer a specified amount of funds to specified recipient using a specified payment method from the subscriber's mobile wallet;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment software..."); (See at least Paragraph 0145, "...transferring...funds...", Fig. 3, Item 310, 315, merchant = agent, Paragraph 0112, "...credit cards, bank accounts...so that any of those accounts can be used...")
- *validating the status of the selected payment method;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *validating the status of the specified recipient to ensure the specified recipient has a valid mobile wallet account;* (See at least Paragraph 0107, "...request that can be validated...")
- *debiting the specified payment method by the specified amount of funds;* (See at least Paragraph 0145, "...transferring...funds...", Paragraph 0112, "...credit cards, bank accounts...so that any of those accounts can be used...")
- *transferring the specified amount of funds to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system;* (See at least Paragraph 0145, "...transferring...funds...")

- *notifying the unbanked subscriber that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing at least one of a limit check and a velocity check on the selected payment method;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 12:

Combination of Labrou, Valdes, and Sato discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *wherein validating the status of the specified recipient comprises performing a check on the specified recipient to comply with the office of foreign assets control.* (See at least Paragraph 0137, "...comply with UPTF...", it is obvious to substitute UPTF with office of foreign assets control)

As per Claim 13:

Combination of Labrou, Valdes, and Sato discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *wherein the money is transferred internationally between the mobile wallets.* (See at least Paragraph 0112, "...enables consumers to make payments to other consumers...")

As per Claim 17:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving subscriber data, including a debit or credit card account number, over one of a plurality of channels connected to the monetary transaction system;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment software...")
- *sending subscriber data to a third party verification system for identification of the subscriber; receiving results from the third party system indicating that the subscriber data appropriately identifies the subscriber;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *securely storing the debit or credit card account number for access by the mobile wallet; adding the debit or credit card account number to the subscriber's mobile wallet; and*

notifying the subscriber of the addition of the debit or credit card account number over at least one of the plurality of channels connected to the monetary transaction system. (See at least Paragraph 0112, "...credit cards, bank accounts...so that any of those accounts can be used...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing one or more validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 18:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system, the agent communication indicating that a subscriber desires to deposit a specified amount of funds into a bank or credit union account;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment software..."); (See at least Paragraph 0145, "...transferring...funds...", Fig. 3, Item 310, 315, merchant = agent)
- *validating the status of the bank or credit union account; determining if the agent branch is authorized to deposit money;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *crediting the bank or credit union account with the specified amount of funds;* (See at least Paragraph 0145, "...transferring...funds...")
- *returning a notification to the agent branch confirming the deposit; and* (See at least Paragraph 0070, "...merchant also receives a notification of the successful transaction...")
- *notifying the subscriber that the specified amount of funds was deposited in the bank or credit union account over at least one of the plurality of channels connected to the monetary transaction system.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed

the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing one or more of a limit check and a velocity check on the bank or credit union account;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

9. Claims 8, 14, and 19 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Labrou and Valdes as applied in claim 1, in further view of Sato et al. (hereinafter "Sato"); (US 2008/0204358 A1) and Lyons et al. (hereinafter "Lyons");(US 7,819,307 B2).

As per Claim 8:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving a communication from the unbanked subscriber over one of a plurality of channels connected to the monetary transaction system, the communication indicating that the unbanked subscriber desires to withdraw a specified amount of funds from the unbanked subscriber's mobile wallet account at the agent branch;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment software..."); (See at least Paragraph 0145, "...transferring...funds...", Fig. 3, Item 310, 315, merchant = agent)

- *validating the status of the unbanked subscriber's mobile wallet account;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *returning a secure, perishable withdrawal code to the subscriber over at least one of the plurality of channels connected to the monetary transaction system;* (See at least Paragraph 0046, "...providing...the PIE to the user...")
- *receiving subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system, the agent branch communication indicating that the withdrawal code has been presented to the agent branch;* (See at least Paragraph 0066, "...the payee (operator) enters its PIE that is also generated...")
- *debiting the unbanked subscriber's mobile wallet account by the specified amount of funds;* (See at least Paragraph 0145, "...transferring...funds...")
- *returning a notification to the agent branch confirming the withdrawal; and* (See at least Paragraph 0070, "...merchant also receives a notification of the successful transaction...")
- *notifying the subscriber that the specified amount of funds was withdrawn from the unbanked subscriber's mobile wallet account over at least one of the channels connected to the monetary transaction system.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed

the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Secondly, combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally, combination of Labrou, Valdes, and Sato does not teach the following limitation. But Lyons does:

- *determining if the balance of the unbanked subscriber's mobile wallet account is sufficient to accommodate the requested withdrawal for the specified amount of funds;* (See at least Column 5, Lines 15-26, "...limits on the amount of monetary value to be held by mobile device...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to check for purchase limit as taught by Lyons since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 14:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving a communication from a subscriber over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to purchase an item for a specified amount of funds using a specified payment method from the unbanked subscriber's mobile wallet;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment software..."); (See at least Paragraph 0145, "...transferring...funds...", Fig. 3, Item 310, 315, merchant = agent, Paragraph 0112, "...credit cards, bank accounts...so that any of those accounts can be used...")
- *returning a secure, perishable purchase code to the unbanked subscriber over at least one of the plurality of channels connected to the monetary transaction system;* (See at least Paragraph 0046, "...providing...the PIE to the user...")
- *receiving subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system, the agent branch communication indicating that the purchase code has been presented to an agent;* (See at least Paragraph 0066, "...the payee (operator) enters its PIE that is also generated...")
- *validating the status of the specified payment method;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *debiting the specified payment method by the specified amount of funds;* (See at least Paragraph 0145, "...transferring...funds...", Paragraph 0112, "...credit cards, bank accounts...so that any of those accounts can be used...")
- *returning a notification to the agent branch authorizing the purchase; and* (See at least Paragraph 0070, "...merchant also receives a notification of the successful transaction...")

- *sending a receipt to the unbanked subscriber over at least one of the plurality of channels connected to the monetary transaction system.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Secondly, combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing at least one of a limit check and a velocity check on the selected payment method;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally, combination of Labrou, Valdes, and Sato does not teach the following limitation. But Lyons does:

- *determining if the specified payment method can accommodate a purchase for the specified amount;* (See at least Column 5, Lines 15-26, "...limits on the amount of monetary value to be held by mobile device...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to check for purchase limit as taught by Lyons since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

As per Claim 19:

Combination of Labrou and Valdes discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving communication from a subscriber over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that a subscriber desires to withdraw a specified amount of funds from a bank or credit union account;*
- *validating the status of the bank or credit union account;* (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")
- *returning a secure, perishable withdrawal code to the subscriber over at least one of the plurality of channels connected to the monetary transaction system;* (See at least Paragraph 0046, "...providing...the PIE to the user...")
- *receiving subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system, the agent branch communication indicating that the withdrawal code has been presented to an agent;* (See at least Paragraph 0066, "...the payee (operator) enters its PIE that is also generated...")

- *debiting the bank or credit union account by the specified amount of funds;* (See at least Paragraph 0145, "...transferring...funds...")
- *returning a notification to the agent branch confirming the withdrawal; and* (See at least Paragraph 0070, "...merchant also receives a notification of the successful transaction...")
- *notifying the subscriber that the specified amount of funds were withdrawn from the bank or credit union account over at least one of the plurality of channels connected to the monetary transaction system.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou specifically does not mention "unbanked subscriber". But it is well known in the art to use "pre-paid" account as source of funding; this was also taught by Valdes (See at least Paragraph 0056, "...purchases of goods and services via prepaid telecommunication accounts...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to use "pre-paid" account as source of funding as taught by Valdes since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Secondly, combination of Labrou and Valdes does not teach the following limitation. But Sato does:

- *performing at least one of a limit check and a velocity check on the bank or credit union account;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same

function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally, combination of Labrou, Valdes, and Sato does not teach the following limitation. But Lyons does:

- *determining if the balance of the bank or credit union account is sufficient to accommodate the requested withdrawal for the specified amount of funds;* (See at least Column 5, Lines 15-26, "...limits on the amount of monetary value to be held by mobile device...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to check for purchase limit as taught by Lyons since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

10. Claim 16 is rejected under 35 U.S.C. 103 (a) as being unpatentable over Labrou as applied in claim 15, in view of Sato et al. (hereinafter "Sato"); (US 2008/0204358 A1).

As per Claim 16:

Labrou discloses the limitations as shown in the rejections above. Furthermore, Labrou discloses the following limitations:

- *receiving subscriber data, including bank or credit union account details, over at least one of a plurality of channels connected to the monetary transaction system;* (See at least Paragraph 0019, "...inputting, by a user, the PIE to the installed authentic mobile payment software...")
- *sending subscriber data to a third party verification system for identification of the subscriber; receiving results from the third party system indicating that the subscriber*

data appropriately identifies the subscriber; submitting bank or credit union account details for validation by the transaction processor; (See at least Paragraph 0061, "...sending party's encrypted message, authenticates the sending party...")

- *receiving an indication that the bank or credit union account details correspond to a valid bank or credit union account;* (See at least Paragraph 0031, "...message flow between a requestor device, a secure transaction server...")
- *maintaining a link between the subscriber data and the bank or credit union account; and* (See at least Fig. 3, Items 120, 200 (108a and 106a)
- *notifying the subscriber of the bank or credit union account validation over at least one of the plurality of channels connected to the monetary transaction system.* (See at least Paragraph 0066, "...sends receipts...")

However, Labrou does not teach the following limitation. But Sato does:

- *performing one or more validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber;* (See at least Paragraph 0053, "...does not exceed the allowable number of devices for the channel...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the wireless wallet system of Labrou the ability to limit number of accounts per subscriber as taught by Sato since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Conclusion

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **Edward Chang** whose telephone number is **571.270.3092.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **ALEXANDER KALINOWSKI** can be reached at **571.272.6771**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair <http://pair-direct.uspto.gov >. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

P.O. Box 1450
Alexandria, VA 22313-1450

or faxed to **571-273-8300.**

Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window:**

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

December 14, 2012
/Edward Chang/ Examiner, Art Unit 3691

Notice of References Cited	Application/Control No. 13/484,199	Applicant(s)/Patent Under Reexamination LIBERTY. MICHAEL A.	
	Examiner EDWARD CHANG	Art Unit 3691	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0187873	08-2005	Labrou et al.	705/040
*	B	US-2011/0145149	06-2011	Valdes et al.	705/44
*	C	US-2008/0204358	08-2008	Sato et al.	345/2.2
*	D	US-7,819.307	10-2010	Lyons et al.	235/379
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1222 of 1360

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13484199	LIBERTY, MICHAEL A.
	Examiner	Art Unit
	EDWARD CHANG	3691

SEARCHED			
Class	Subclass	Date	Examiner
705	40	12/16/2012	EC

SEARCH NOTES		
Search Notes	Date	Examiner
EAST - Keyword Search	12/16/2012	EC

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
705	40	12/16/2012	EC

/EDWARD CHANG/ Examiner.Art Unit 3691	

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1223 of 1360

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

BIB DATA SHEET

CONFIRMATION NO. 5095

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/484,199	05/30/2012 RULE	705	3691	18756.8.1.1

APPLICANTS
Michael A. Liberty, Windermere, FL;

**** CONTINUING DATA ***************************
This appln claims benefit of 61/522,099 08/10/2011
and claims benefit of 61/493,064 06/03/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
06/08/2012

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
❑ Yes ☑ No	❑ Yes ☑ No	/EDWARD CHANG/ Examiner's Signature	❑ Initials	FL	21	20	3

ADDRESS

Workman Nydegger
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111
UNITED STATES

TITLE

MONETARY TRANSACTION SYSTEM

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
1380	No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1224 of 1360

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3699	(705/40).ccls.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/12/16 00:43
S1	100	("20120209762" "6142369" "6725303" "6976011" "20060265339" "20070063017" "20070106564" "20080270253" "20080314971" "20100030651" "7819307" "7822688" "20030004876" "20050187873" "20070095892" "20080162318" "20100088188" "20120197794" "20120259698" "20090055913" "20100274678" "20110137791" "20110145086" "20110145139" "20110145140" "20110145149" "20110313924" "20120226611" "20120290449" "6338140" "20100023417" "20040169073" "5315636" "5514862" "5848161" "5943624" "6038548" "6178335" "6185436" "6726092" "6913191" "7546944" "7784693" "20010007132" "20030078789" "20030121967" "20030177088" "20040243477" "20050164739" "20060173776" "20070123305" "20090106119" "20090233577" "20120036067" "20120108204" "20120172089" "20040039651" "20090097658" "5557518" "5621797" "5642419" "5815657" "5878139" "5963924" "6016484" "6019284" "6116506" "6230971" "4260055" "4992646" "5221838" "5671280" "5703949" "5745886" "5890052" "5940510" "5949880" "5949045" "6029151" "6068183" "6081790" "6088797" "6112984" "6175921" "6205436" "6315195" "6394343" "6425522" "6450407" "6502748" "6702181" "6905072" "6913193" "6970852" "7040533" "7140550" "7201313" "7207477" "7216800" "7344066").pn.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/12/14 13:15
S2	391	exceed with number with account	US-PGPUB; USPAT; USOCR	OR	OFF	2012/12/15 14:40
S3	4	exceed with number with account with allowable	US-PGPUB; USPAT; USOCR	OR	OFF	2012/12/15 14:40

EAST Search History (Interference)

<This search history is empty>

12/16/2012 12:44:32 AM
C:\Users\echang1\Documents\EAST\Workspaces\Applicaiton -- 13484199 -- Monetary Transaction System.wsp

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1225 of 1360

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13484199	LIBERTY, MICHAEL A.
	Examiner	Art Unit
	EDWARD CHANG	3691

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/16/2012								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1226 of 1360

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
13/484,199	05/30/2012	Michael A. Liberty	18756.8.1.1

CONFIRMATION NO. 5095

22913
Workman Nydegger
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

PUBLICATION NOTICE

OC000000058009992

Title:MONETARY TRANSACTION SYSTEM

Publication No.US-2012-0310824-A1
Publication Date:12/06/2012

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 Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, 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 http://pair.uspto.gov/. 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

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1227 of 1360

PLUS Search Results for S/N 13484199, Searched Thu Nov 29 13:46:50 EST 2012

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

20120209762 73
6142369 59
6725303 59
6976011 59
20060265339 59
20070063017 59
20070106564 59
20080270253 59
20080314971 59
20100030651 59
7819307 58
7822688 58
20030004876 58
20050187873 58
20070095892 58
20080162318 58
20100088188 58
20120197794 58
20120259698 58
20090055913 53
20100274678 53
20110137791 53
20110145086 53
20110145139 53
20110145140 53
20110145149 53
20110313924 53
20120226611 53
20120290449 52
6338140 49
20100023417 48
20040169073 47
5315636 47
5514862 47
5848161 47
5943624 47
6038548 47
6178335 47
6185436 47
6726092 47
6913191 47
7546944 47
7784693 47
20010007132 47
20030078789 47
20030121967 47
20030177088 47
20040243477 47
20050164739 47
20060173776 47
20070123305 47
20090106119 47
20090233577 47
20120036067 47
20120108204 47
20120172089 47
20040039651 46
20090097658 46
5557518 46
5621797 46
5642419 46
5815657 46
5878139 46
5963924 46
6016484 46
6019284 46
6116506 46
6230971 46
4260055 46
4992646 46
5221838 46
5671280 46
5703949 46
5745886 46
5890052 46
5940510 46
5949880 46
5949045 46
6029151 46
6068183 46
6081790 46
6088797 46
6112984 46
6175921 46
6205436 46
6315195 46
6394343 46
6425522 46
6450407 46
6502748 46
6702181 46
6905072 46
6913193 46
6970852 46
7040533 46
7140550 46
7201313 46
7207477 46
7216800 46
7344066 46

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/484,199

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(S)	OTHER THAN SMALL ENTITY FEE(S)
BASIC FEE (37 CFR 1.16(a), (b) or (c))	N/A	N/A	N/A			N/A	380
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 60	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 250 =	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			TOTAL	1250

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	RATE ($)	ADDITIONAL FEE($)		RATE ($)	ADDITIONAL FEE($)
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.

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
13/484,199	05/30/2012	2876	1380	18756.8.1.1	20	3

CONFIRMATION NO. 5095

22913
Workman Nydegger
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

UPDATED FILING RECEIPT

OC000000055929225

Date Mailed: 08/16/2012

Receipt is acknowledged of this non-provisional 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 APPLICANT, 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 Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections 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**

Applicant(s)

Michael A. Liberty, Windermere, FL;

Power of Attorney: The patent practitioners associated with Customer Number 022913

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/522,099 08/10/2011
and claims benefit of 61/493,064 06/03/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 06/08/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/484,199**

Projected Publication Date: 12/06/2012

Non-Publication Request: No

Early Publication Request: No

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1230 of 1360

Title

MONETARY TRANSACTION SYSTEM

Preliminary Class

235

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 (1-866-999-4158).

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

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1231 of 1360

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 USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1232 of 1360

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
13/484,199	05/30/2012	Michael A. Liberty	18756.8.1.1

CONFIRMATION NO. 5095

22913
Workman Nydegger
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

DOCKETED
Atty JCS File # 18756.8.1.1
By LDN On 6/12/12
Action Missing Parts
Response Due 8/12/12

FORMALITIES LETTER

OC000000054748670

Date Mailed: 06/12/2012

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 oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of **$130** for a non-small entity, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is **$130** for a non-small entity
- **$130** Surcharge.

Verified
By: CU On: 06/12/2012

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1233 of 1360

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.
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.

/hnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1234 of 1360

Electronic Patent Application Fee Transmittal	
Application Number:	13484199
Filing Date:	30-May-2012
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Filer:	John C. Stringham/Sue Held
Attorney Docket Number:	18756.8.1.1
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late filing fee for oath or declaration	1051	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	130

Electronic Acknowledgement Receipt	
EFS ID:	13437243
Application Number:	13484199
International Application Number:	
Confirmation Number:	5095
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Customer Number:	22913
Filer:	John C. Stringham/Sue Held
Filer Authorized By:	John C. Stringham
Attorney Docket Number:	18756.8.1.1
Receipt Date:	07-AUG-2012
Filing Date:	30-MAY-2012
Time Stamp:	15:08:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$130
RAM confirmation Number	1678
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Transmittal Letter	18756_8_1_1_Response_To_Missing Parts.pdf	123887	no	3
Warnings:					
Information:					
2	Oath or Declaration filed	18756 8 1 1 Declaration.pdf	118604	no	3
Warnings:					
Information:					
3	Miscellaneous Incoming Letter	18756_8_1_1_Notice_To_File_Missing Parts.pdf	131792	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	29901	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	404184		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PATENT APPLICATION
Docket: 18756.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:		)
		)
	Michael A. Liberty	)
		) Art Unit
Serial No.:	13/484,199	) 2876
		)
Confirmation No.:	5095	)
		)
Filed:	May 30, 2012	)
		)
For:	MONETARY TRANSACTION SYSTEM	)
		)

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

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

Sir:

In response to the Notice to File Missing Parts of Nonprovisional Application Filed Under 37 CFR 1.53(b) mailed June 12, 2012, please find enclosed herewith the following items for filing in the United States Patent and Trademark Office in connection with the above-identified patent application:

_X_ A Combined Declaration and Power of Attorney executed by the inventor Michael A. Liberty.

___ An Assignment conveying the invention to _____, including a Form PTO-1595 recordation cover sheet.

X A copy of the Notice to File Missing Parts of Nonprovisional Application Filed Under 37 CFR 1.53(b)

___ To render the Response timely filed, enclosed are the following:

____ Petition for a (__) Month Extension of Time.

_X_ Payment by credit card using the payment option in E-Filer with RAM will be used to cover the payment of the fees as follows:

___ The $ _____ government filing fee.

___ The $ recordation fee of the enclosed assignment.

X_ The $130.00 surcharge fee pursuant to 37 C.F.R. § 1.16(e).

____ The $___ fee for Petition for a one (1) Month Extension of Time.

The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or to credit any overpayment to Deposit Account No. 23-3178.

_X_ Any additional filing fees required under 37 C.F.R. § 1.16.

X_ Any patent application processing fees under 37 C.F.R. § 1.17.

The Commissioner is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. 23-3178.

_X Any filing fees under 37 C.F.R. § 1.16 for presentation of extra claims.

_X_ Any patent application processing fees under 37 C.F.R. § 1.17.

__ The issue fee set in 37 C.F.R. § 1.18 at or before mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1240 of 1360

Please address all future correspondence in connection with this case to the attention of the undersigned.

DATED this 13 day of August, 2012.

Respectfully submitted,

JOHN C. STRINGHAM
Registration No. 40,831
WORKMAN NYDEGGER
Attorneys for Applicant
Customer No. 022913
Telephone No. 801.533.9800

3840963_1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1241 of 1360

COMBINED DECLARATION and POWER OF ATTORNEY FOR UTILITY or DESIGN PATENT APPLICATION

As a below named inventor, I hereby declare that:

INVENTORSHIP IDENTIFICATION

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am the original, first and joint inventors of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

MONETARY TRANSACTION SYSTEM

SPECIFICATION IDENTIFICATION

The specification of which was previously filed on May 30, 2012, and assigned U.S. Patent Application No. 13/484,199.

ACKNOWLEDGEMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claim(s), as amended by any amendment specifically referred to in the declaration, referred to above.

I acknowledge the duty to disclose information that is material to patentability as defined in 37, Code of Federal Regulations, § 1.56, including for continuation-in-part applications, material information that becomes available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application. Specifically, pursuant to 37 C.F.R. § 1.63 (b) (3), I acknowledge my duty to disclose to the United States Patent and Trademark Office all information known to be "material to patentability as defined in Section 1.56."

U.S. PRIORITY CLAIM (35 USC § 120)

I hereby claim the benefit under 35 USC § 120 of any United States application(s) or § 365(c) of any PCT international application designating the United States of America listed below, if any,

and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of title 35 USC § 112, I acknowledge duty to disclose information which is material to patentability as defined in title 37, Code of Federal Regulations § 1.56 which became available between the filing date of the prior application and the national or PCT international application filing date of this application.

U.S. or PCT PATENT APPLICATION NO.	FILING DATE (month, day, year)	PARENT PATENT NO. (if applicable)

PROVISIONAL APPLICATION CLAIM
(35 USC § 119(e))

I hereby claim the benefit under 35 USC § 119(e) of any United States Provisional application listed below, if any.

U.S. PROVISIONAL PATENT APPLICATION NO.	FILING DATE (month, day, year)
61/522,099	08/10/2011
61/493,064	06/03/2011

POWER OF ATTORNEY

I hereby appoint as my attorneys and/or patent agents all attorneys and/or patent agents listed under the following Customer Number, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

022913

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1243 of 1360

All correspondence and telephonic communications should be directed to:

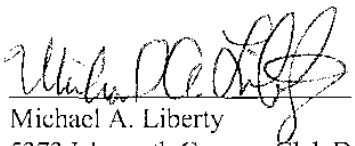
JOHN C. STRINGHAM
WORKMAN NYDEGGER
Telephone (801) 533-9800

DECLARATION

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.

SIGNATURE

Date: 7/10/12

Inventor's Signature: 
Inventor's Name: Michael A. Liberty
Residence: 5373 Isleworth Country Club Drive
Windermere, Florida 34786

Mailing Address: 5373 Isleworth Country Club Drive
Windermere, Florida 34786

Citizenship: United States

3784470_1

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1244 of 1360

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/484,199

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(S)	OTHER THAN SMALL ENTITY FEE(S)
BASIC FEE (37 CFR 1.16(a), (b) or (c))	N/A	N/A	N/A			N/A	380
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 60	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 250 =	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			TOTAL	1250

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	RATE ($)	ADDITIONAL FEE($)		RATE ($)	ADDITIONAL FEE($)
	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.

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
13/484,199	05/30/2012	2876	1250	18756.8.1.1	20	3

CONFIRMATION NO. 5095

22913
Workman Nydegger
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

FILING RECEIPT

Date Mailed: 06/12/2012

Receipt is acknowledged of this non-provisional 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 APPLICANT, 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 Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections 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**

Applicant(s)

Michael A. Liberty, Windermere, FL;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/522,099 08/10/2011
and claims benefit of 61/493,064 06/03/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 06/08/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/484,199**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1246 of 1360

Title

MONETARY TRANSACTION SYSTEM

Preliminary Class

235

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 (1-866-999-4158).

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

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1247 of 1360

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 USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1248 of 1360

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
13/484,199	05/30/2012	Michael A. Liberty	18756.8.1.1

CONFIRMATION NO. 5095

22913
Workman Nydegger
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

FORMALITIES LETTER

Date Mailed: 06/12/2012

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 oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $**130** for a non-small entity, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is $**130** for a non-small entity
- $**130** Surcharge.

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1249 of 1360

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.
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.

/lnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1250 of 1360

PATENT APPLICATION
Docket No. 18456.8.1.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL FOR PATENT APPLICATION

Sir:

Transmitted herewith for filing under 37 C.F.R. § 1.53(b) is a United States patent application entitled **MONETARY TRANSACTION SYSTEM** in the name of the following inventor(s): Michael A. Liberty.

Enclosed are the following:

X A specification, claims, abstract, and cover page in total comprising seventy-seven (77) pages.

X Twenty-one (21) sheets of drawings.

X Priority to U.S. Provisional Application Serial No. 61/522,099 filed on August 10, 2011 and U.S. Provisional Application Serial No. 61/493,064 filed on June 3, 2011 is claimed under 35 U.S.C. § 119.

The filing fee has been calculated as shown below.

			SMALL ENTITY		LARGE ENTITY	
FOR	NO. FILED	NO. EXTRA	RATE	FEE	RATE	FEE
BASIC FEE					380.00	$380.00
SEARCH FEE					620.00	$620.00
EXAMINATION FEE					250.00	$250.00
TOT. CLAIMS	20 -20=		X =	$0.00	X =	
IND. CLAIMS	3 -3=		X =	$0.00	X =	
MULTIPLE DEPENDENT CLAIM			= =	$0.00	+ =	
			TOTAL	$0.00	**TOTAL**	$1,250.00

X Payment by credit card using the payment option in E-Filer with RAM will be used to cover the payment of the fees as follows:

X The $1,250.00 government filing fee.

X The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment to Deposit Account No. 23-3178: (1) any filing fees required under 37 CFR § 1.16; and/or (2) any patent application and reexamination processing fees under 37 CFR § 1.17.

X Any additional filing fees required under 37 C.F.R. § 1.16.

X Any patent application processing fees under 37 C.F.R. § 1.17.

X The Commissioner is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. 23-3178.

X Any filing fees under 37 C.F.R. § 1.16 for presentation of extra claims.

X Any patent application processing fees under 37 C.F.R. § 1.17.

The issue fee set forth in 37 C.F.R. § 1.18 at or before mailing of the Notice of Allowance, pursuant to 37 C.F.R. § 1.311(b).

Please address all future correspondence in connection with the above-identified patent application to the attention of the undersigned.

Dated this 30th day of May, 2012

Respectfully submitted,

/GREGORY R. LUNT/

John C. Stringham
Registration No. 40,831
GREGORY R. LUNT
Registration No. 57354
Attorneys for Applicant
Customer No. 022913

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. 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	18756.8.1.1
	Application Number	
Title of Invention	MONETARY TRANSACTION SYSTEM	

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.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Michael	A.	Liberty	

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

City	Windermere	State/Province	FL	Country of Residence i	US

Citizenship under 37 CFR 1.41(b) i: US

Mailing Address of Applicant:

Address 1	5373 Isleworth Country Club Drive		
Address 2			
City	Windermere	State/Province	FL
Postal Code	34786	Country i	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	22913		
Email Address	jstringham@wnlaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	MONETARY TRANSACTION SYSTEM		
Attorney Docket Number	18756.8.1.1	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	21	Suggested Figure for Publication (if any)	1

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. 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	18756.8.1.1
	Application Number	
Title of Invention	MONETARY TRANSACTION SYSTEM	

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). Enter either 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	22913		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) 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)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61522099	2011-08-10
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61493064	2011-06-03

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 benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			○ Yes ◉ No

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

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1254 of 1360

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. 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	18756.8.1.1
	Application Number	
Title of Invention	MONETARY TRANSACTION SYSTEM	

Assignee Information:

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.

Assignee [1] Remove

If the Assignee is an Organization check here. ☐

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

Mailing Address Information:

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

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

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Gregory R. Lunt, Reg.# 57354/			Date (YYYY-MM-DD)	2012-05-30
First Name	GREGORY R.	Last Name	LUNT	Registration Number	57354

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.**

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1255 of 1360

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1256 of 1360

FILED VIA E-FILING

PATENT APPLICATION
Docket No.: 18756.8.1.1

UNITED STATES PATENT APPLICATION

Of

Michael A. Liberty

For

MONETARY TRANSACTION SYSTEM

MONETARY TRANSACTION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of U.S. Provisional Application Ser. No. 61/522,099, filed on August 10, 2011, entitled "Mobile Wallet Platform", and also claims priority to and the benefit of U.S. Provisional Application Ser. No. 61/493,064, filed on June 3, 2011, entitled "Mobile Wallet Platform". Both of the aforementioned provisional applications are incorporated by reference in their entirety herein.

BACKGROUND

[0002] Mobile phones and other digital devices have become increasingly popular in recent years. Many mobile device users use their devices to perform countless different daily tasks. For instance, mobile devices allow users to check email, send and receive instant messages, check calendar items, take notes, set up reminders, browse the internet, play games or perform any number of different things using specialized applications or "apps". These applications allow mobile devices to communicate with other computer systems and perform a wide variety of network-connected tasks previously not possible with a mobile device.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1258 of 1360

BRIEF SUMMARY

[0003] Embodiments described herein are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one embodiment, the monetary transaction system includes a mobile device configured to run a monetary transaction system application. The monetary transaction system also includes a monetary transaction system subscriber that has a profile with the system. The subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber. Performing these transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile.

[0004] The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity. The subscriber may have access to a bank account, or may be an "unbanked user" that does not have access to a bank account. Each of the terms included above will be described in greater detail below in conjunction with the drawings.

[0005] The monetary transaction system may be used for many different tasks including enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet,

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1259 of 1360

paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below.

[0006] 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 as an aid in determining the scope of the claimed subject matter.

[0007] Additional features and advantages will be set forth in the description which follows, and in part will be apparent to one of ordinary skill in the art from the description, or may be learned by the practice of the teachings herein. Features and advantages of embodiments described herein may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. Features of the embodiments described herein will become more fully apparent from the following description and appended claims.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1260 of 1360

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] To further clarify the above and other features of the embodiments described herein, a more particular description will be rendered by reference to the appended drawings. It is appreciated that these drawings depict only examples of the embodiments described herein and are therefore not to be considered limiting of its scope. The embodiments will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

[0009] Figure 1 illustrates a monetary transaction system architecture in which embodiments described herein may operate.

[0010] Figure 2 illustrates an alternate example embodiment of a monetary transaction system.

[0011] Figure 3 illustrates an example data flow for performing a subscriber deposit via a mobile wallet.

[0012] Figure 4 illustrates an example data flow for performing a subscriber withdrawal via a mobile wallet.

[0013] Figures 5A and 5B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber eMoney transfers via a mobile wallet, respectively.

[0014] Figures 6A and 6B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber international eMoney transfers via a mobile wallet, respectively.

[0015] Figure 7 illustrates an example data flow for performing a subscriber airtime purchase via a mobile wallet.

[0016] Figure 8 illustrates an example data flow for performing a subscriber-initiated bill pay via a mobile wallet.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1261 of 1360

[0017] Figure 9 illustrates an example data flow for performing a subscriber-initiated retail purchase via a mobile wallet.

[0018] Figures 10A and 10B illustrate example data flows for requesting and repaying micro-loans via a mobile wallet, respectively.

[0019] Figure 11A illustrates an example data flow of a subscriber receiving a direct deposit via a mobile wallet.

[0020] Figure 11B illustrates an example data flow of a subscriber receiving a governmental welfare payment via a mobile wallet.

[0021] Figure 12A illustrates an example data flow of an agent administrator distributing eMoney via a mobile wallet.

[0022] Figure 12B illustrates an example data flow of an agent company making a deposit using a mobile wallet.

[0023] Figure 13 illustrates an example data flow of an agent company making a withdrawal using a mobile wallet.

[0024] Figure 14 illustrates an example data flow of a subscriber making a deposit at an agent branch using a mobile wallet.

[0025] Figure 15 illustrates an example data flow of a subscriber making a deposit with a non-agent using a mobile wallet.

[0026] Figure 16 illustrates an example data flow of a subscriber making a withdrawal with an agent using a mobile wallet.

[0027] Figure 17A illustrates an example data flow of a subscriber making a withdrawal from an ATM using a mobile wallet.

[0028] Figure 17B illustrates an example data flow of a subscriber-to-subscriber money transfer using a mobile wallet.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1262 of 1360

[0029] Figure 17C illustrates an example data flow of a subscriber-to-non-subscriber money transfer using a mobile wallet.

[0030] Figure 18A illustrates an example data flow of a subscriber-to-subscriber international money transfer using a mobile wallet.

[0031] Figure 18B illustrates an example data flow of a subscriber-to-non-subscriber international money transfer using a mobile wallet.

[0032] Figure 19A illustrates an example data flow of a subscriber-to-subscriber international money transfer using a mobile wallet.

[0033] Figure 19B illustrates an example data flow of a non-subscriber-to-subscriber international money transfer using a mobile wallet.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1263 of 1360

DETAILED DESCRIPTION

[0034] Embodiments described herein are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one embodiment, the monetary transaction system includes a mobile device configured to run a monetary transaction system application. The monetary transaction system also includes a monetary transaction system subscriber that has a profile with the system. The subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber. Performing these transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile.

[0035] The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity. The subscriber may have access to a bank account, or may be an "unbanked user" that does not have access to a bank account. Each of the terms included above will be described in greater detail below in conjunction with the drawings.

[0036] The monetary transaction system may be used for many different tasks including enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet,

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1264 of 1360

paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below.

[0037] The following discussion now refers to a number of methods and method steps or acts that may be performed. It should be noted, that although the method steps may be discussed in a certain order or illustrated in a flow chart as occurring in a particular order, no particular ordering is necessarily required unless specifically stated, or required because a step is dependent on another step being completed prior to the step being performed.

[0038] Embodiments of the mobile transaction system or "mobile wallet platform" described herein may comprise or utilize a special purpose or general-purpose computer including computer hardware, such as, for example, one or more processors and system memory, as discussed in greater detail below. Embodiments described herein also include physical and other computer-readable media for carrying or storing computer-executable instructions and/or data structures. Such computer-readable media can be any available media that can be accessed by a general purpose or special purpose computer system. Computer-readable media that store computer-executable instructions in the form of data are computer storage media. Computer-readable media that carry computer-executable instructions are transmission media. Thus, by way of example, and not limitation, embodiments described herein can comprise at least two distinctly different kinds of computer-readable media: computer storage media and transmission media.

[0039] Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1265 of 1360

memory (PCM), or other types of memory, or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store desired program code means in the form of computer-executable instructions, data or data structures and which can be accessed by a general purpose or special purpose computer.

[0040] A "network" is defined as one or more data links and/or data switches that enable the transport of electronic data between computer systems and/or modules and/or other electronic devices. When information is transferred or provided over a network (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a transmission medium. Transmission media can include a network which can be used to carry data or desired program code means in the form of computer-executable instructions or in the form of data structures and which can be accessed by a general purpose or special purpose computer. Combinations of the above should also be included within the scope of computer-readable media.

[0041] Further, upon reaching various computer system components, program code means in the form of computer-executable instructions or data structures can be transferred automatically from transmission media to computer storage media (or vice versa). For example, computer-executable instructions or data structures received over a network or data link can be buffered in RAM within a network interface module (e.g., a network interface card or "NIC"), and then eventually transferred to computer system RAM and/or to less volatile computer storage media at a computer system. Thus, it should be understood that computer storage media can be included in computer system components that also (or even primarily) utilize transmission media.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1266 of 1360

[0042] Computer-executable (or computer-interpretable) instructions comprise, for example, instructions which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, or even source code. Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the described features or acts described above. Rather, the described features and acts are disclosed as example forms of implementing the claims.

[0043] Those skilled in the art will appreciate that various embodiments may be practiced in network computing environments with many types of computer system configurations, including personal computers, desktop computers, laptop computers, message processors, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, tablets, pagers, routers, switches, and the like. Embodiments described herein may also be practiced in distributed system environments where local and remote computer systems that are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, each perform tasks (e.g. cloud computing, cloud services and the like). In a distributed system environment, program modules may be located in both local and remote memory storage devices.

[0044] In this description and the following claims, "cloud computing" is defined as a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). The

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1267 of 1360

definition of "cloud computing" is not limited to any of the other numerous advantages that can be obtained from such a model when properly deployed.

[0045] For instance, cloud computing is currently employed in the marketplace so as to offer ubiquitous and convenient on-demand access to the shared pool of configurable computing resources. Furthermore, the shared pool of configurable computing resources can be rapidly provisioned via virtualization and released with low management effort or service provider interaction, and then scaled accordingly.

[0046] A cloud computing model can be composed of various characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, and so forth. A cloud computing model may also come in the form of various service models such as, for example, Software as a Service ("SaaS"), Platform as a Service ("PaaS"), and Infrastructure as a Service ("IaaS"). The cloud computing model may also be deployed using different deployment models such as private cloud, community cloud, public cloud, hybrid cloud, and so forth. In this description and in the claims, a "cloud computing environment" is an environment in which cloud computing is employed.

[0047] Additionally or alternatively, the functionally described herein can be performed, at least in part, by one or more hardware logic components. For example, and without limitation, illustrative types of hardware logic components that can be used include Field-programmable Gate Arrays (FPGAs), Program-specific Integrated Circuits (ASICs), Program-specific Standard Products (ASSPs), System-on-a-chip systems (SOCs), Complex Programmable Logic Devices (CPLDs), and other types of programmable hardware.

[0048] Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1268 of 1360

whole. This modularity allows for increased flexibility when approaching issues of platform scalability and, to this end, provides a variety of advantages. System complexity and growth can be managed more easily through the use of smaller-scale parts with limited functional scope. Platform fault tolerance is enhanced through the use of these loosely coupled modules. Individual components can be grown incrementally as business needs dictate. Modular development also translates to decreased time to market for new functionality. New functionality can be added or subtracted without impacting the core system.

[0049] Various terminology will be used herein to describe the monetary transaction system (also referred to as a "mobile wallet platform", "mobile wallet program" or "mobile wallet transaction system"). The term "agent" is used to refer to an individual with mobile financial services (mFS) transaction system tools and training to support specific mFS functions. These mFS functions include subscriber registration and activation, and the deposit and withdrawal of funds from the mFS transaction system. Agents are representatives of the mFS transaction system or "program". Agents can be employees or contractors of the program provider, or other companies and organizations that partner with the program provider to provide these services themselves. Agents may be found in every facet of a typical economy, and may include large retailers, mobile network operators (MNO) airtime sales agents, gas stations, kiosks, or other places of business.

[0050] The mobile wallet platform includes a mobile wallet application, web interface or some other type of functionality that allows the user to interact with the mFS platform using their mobile device. The mobile wallet application may include a subscriber identity module (SIM) application, an Unstructured Supplementary Service Data (USSD) application, a smartphone application, a web application, a mobile web

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1269 of 1360

application, a Wireless Application Protocol (WAP) application, a Java 2 Platform, Micro Edition (J2ME) application, a tablet application or any other type of application or interface that provides tools for the agent to register, activate, and offer other services to the mFS subscriber.

[0051] As used herein, a mobile wallet application is a mobile wallet application installed on a SIM card. A USSD application is an application that implements USSD for various functionality including prepaid callback service, location-based content services, menu-based information services and other mobile wallet platform services. A web application is one that implements or uses the internet to provide mobile wallet platform functionality. A mobile web application is similar to a web application, but is tailored for mobile devices. A WAP application is one that uses the wireless application protocol to communicate with the mobile wallet platform to provide the platform's functionality. A J2ME application is an application developed in Java and is designed to provide mobile wallet functionality on a variety of different hardware. A tablet application is an application specifically designed for a touchscreen-based tablet that provides mobile wallet platform functionality for tablet devices. , and as part of configuring the phone on the network. Any of these applications (or any combination thereof) may be provided on the user's mobile device. This functionality can also be made available on a retail point of sale (POS) system or web site.

[0052] The term "agent administrator" refers to an individual with mFS program tools and training to administrate the allocation of funds to agent branches (e.g. retail locations). As agents perform mFS transactions with subscribers, such as depositing and withdrawing money, the agents are adding and removing money from their own accounts. If there are insufficient funds in the agent's account to complete a transaction, additional money will need to be transferred from the agent company's

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1270 of 1360

master account to that agent branch account to cover that transaction. An agent administrator is responsible for these funds transfers. Any of the applications referred to above may be configured to provide tools used by the agent administrator to view the agent company balance, view the agent branch balances, and transfer funds into and out of agent branch mobile wallets. This functionality can also be made available on a website for easier access.

[0053] The term "agent administrator mobile wallet application" refers to a software program or application installed on the agent administrator's terminal in the agent administrator's mobile device (such as a mobile phone or tablet). This software application provides the agent administrator the ability to securely perform agent administrator functions such as querying the agent company account balance or transferring funds into and out of agent branch accounts. The agent administrator's mobile wallet application may be installed on a global system for mobile communications (GSM) SIM card (or on any other type of SIM card), and may be accessed using a GSM mobile phone. The agent administrator's application may also be installed on a code division multiple access (CDMA) mobile phone, a 3G, 4G, 4G LTE (Long Term Evolution) or other wireless carrier standard. The application may, additionally or alternatively, be installed directly on the agent administrator's mobile device. The application communicates with the mFS transaction system using binary and/or text short message service (SMS) messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates.

[0054] In some embodiments, the mFS platform application may utilize triple data encryption standard (3DES) encryption (or some other type of encryption), encrypted message signing, and password security on some or all of its communications with the

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1271 of 1360

mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

[0055] The term "agent branch" refers to any location where an agent provides support for subscriber services of the mFS platform. Funds are allocated by the agent administrator from the agent company's main account to each agent branch to fund the subscriber mFS functions such as depositing or withdrawing cash, in-store purchases, bill payments, prepaid airtime top-ups and money transfers. In some cases, multiple agents may work in a single branch. However, at least in some cases, monetary funds are allocated to from the agent company's main account on a per branch basis.

[0056] The term "agent branch account balance" refers to the amount of money residing in a particular agent branch account at a given time. Funds can be deposited into the branch account by the agent administrator, or the funds can come from participating in subscriber mFS transactions such as depositing or withdrawing cash from the subscriber's mobile wallet accounts, or making retail purchases with the mobile wallet.

[0057] Each agent branch is to maintain a balance in their branch account. This applies more strongly in countries where mFS program and financial services infrastructure is still developing. In cases where real-time processing of financial transactions including card processing is not practical, subscribers leverage the applications on their mobile phones to submit transactions and conduct business with retailers, businesses, and other subscribers. The mFS platform manages the balance of mobile wallet accounts for each subscriber as value is transferred from one mobile wallet to another (e.g. from a subscriber's mobile wallet to an agent's mobile wallet in payment for goods or services). This value is referred to herein as "eMoney".

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1272 of 1360

[0058] As subscribers conduct business with mFS agents, they deposit or withdraw cash from their mobile wallet accounts. Virtual or eMoney credits are transferred between the subscriber's mobile wallet account and the agent branch's account as a form of currency to support the transaction. As agents accept cash into their cash register by mFS subscribers, they transfer the equivalent amount of eMoney credits into the mFS subscriber's mobile wallet account. For instance, if an mFS subscriber gives an mFS agent $10 to deposit into the subscriber's mobile wallet account, the agent would place the cash into his register and transfer $10 from the agent branch's eMoney account into the subscriber's mobile wallet account. While the agent acquired $10 in his register, he transferred out $10 of eMoney credits from his branch eMoney account.

[0059] In some embodiments, in countries with more developed economies, it may be beneficial to use program-issued pre-paid debit cards, pre-paid access accounts, stored value accounts or gift cards to conduct business along with the added convenience of card processing networks such as Cirrus, STAR, or Visa for POS and automated teller machine (ATM) functionality. Agents, particularly those in retail outlets and kiosks, can still support subscribers with deposits, withdrawals, and other transfers, but in this case bank external card processors manage the mobile wallet and branch account balances and provide the real-time transfer of funds.

[0060] The term "agent branch ledger" refers to a written (or electronic) ledger maintained by the mFS platform. Agent branch transactions are performed on the agent's and subscriber's mobile phones where an electronic record of the transaction is generated and stored on the mFS platform. These electronic transactions are then reconciled with agent branch ledgers to ensure the security and integrity of the transaction. Agent branch ledgers are printed or electronic transaction logs that are

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1273 of 1360

distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

[0061] The term "agent company" refers to a business that registers to participate in the mFS program as a partner of the mFS program provider or owner. The agent company has one or more agent branches which conduct mFS business with mFS program subscribers. In some cases, the agent company may be referred to as a distributor or retailer.

[0062] The term "agent company account balance" refers to the sum of the funds deposited at a "partner bank" (defined below) by the agent company to fund the agent company's daily transactions. The funds in the agent company account are then distributed to agent branches by the agent company's agent administrator to conduct everyday business such as accepting cash deposits and cash withdrawals from mFS subscribers. This balance is sometimes referred to as the "agent company float".

[0063] An "agent manager" is a supervisor of company agents for a given company. The agent manager has the training and tools to create, delete or modify agent accounts for a company, as well as monitor the transactions performed by agents. The agent manager may have a special application or an increased level of rights to access applications features not available to other users. The special application is a program installed on the agent manager's terminal. This application provides the agent manager the ability to securely perform agent manager functions such as registering and activating new agent accounts.

[0064] The mFS agent manager application may be installed on any terminal or device. It communicates with the mFS platform using binary and/or text SMS messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates. The mFS platform mobile wallet

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1274 of 1360

applications may utilize 3DES encryption (or any other type of encryption), encrypted message signing, and password security on some or all of its communications with the mFS platform in order to ensure that the transactions are properly secured and authenticated.

[0065] The term "agent application" refers to an application that provides all the tools necessary for an agent to register, activate, and offer other services to the mFS subscriber. The agent application is a program installed on the agent's SIM card or otherwise installed in the agent's mobile device's memory. This application provides the agent the ability to securely perform agent functions such as registering and activating new subscribers and depositing and withdrawing funds from mobile wallet accounts. The mFS agent application may be installed on a GSM SIM card or mobile phone and may be accessed using a GSM or CDMA mobile phone. A wireless service provider or MNO provides the data and SMS network infrastructure on which the mFS platform operates.

[0066] The terms "mFS platform", "mobile wallet platform" and "monetary transaction system" refer to an overall platform or ecosystem of different components that work together to provide the various functions described herein on a global scale. At least some of the various logic components include the following: the application. The "mobile wallet application" or "mFS application" manages the processing of incoming transactions regardless of their source. The application handles end-user authentication, transaction processing, subscriber profile management, and further manages interactions between the various platform components.

[0067] The mFS platform further includes a transaction processor. This component is used when the mFS application is implemented in a country where real-time processing of financial transactions is not practical (or not possible). The

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1275 of 1360

transaction processor manages the balance of mobile wallet accounts, agent accounts, and the accounts of any other program participant. The transaction processor handles balance inquiries, credits, debits, and transaction roll-backs.

[0068] The mFS platform further includes a rules engine that manages and applies the rules and policy that are defined for transactions as they are processed on the mFS platform. Rules impact transaction fees, limits, velocity limits, and commissions as well as program actor roles and permissions. Rules can be customized for each implementation. The mFS platform also includes an integration interface that manages the integration and interaction between external systems (i.e. external to the mFS platform) and the mFS platform. Connectivity to the wireless service provider's pre-paid airtime billing platform and the program partner bank, for example, are managed by the integration interface.

[0069] The mFS platform further includes a transaction database that stores the data that supports the mFS platform. This includes subscriber profiles and subscription data, transaction data and logs, and application configuration and run-time data, among other types of data. Another component of the mFS platform is a handset support service that interfaces with the wireless service provider's SMS network to allow communication between the mobile wallet applications and the back-office systems via SMS messaging or some other form of data transfer. Still further, another component of the mFS platform is a web component that provides a web interface to the mFS program participants that allows the subscriber to perform the same functions in the web interface that they would have available through their applications.

[0070] The term "bill pay company" refers to a business that signs-up to participate in the mFS transaction system. As a participant in the mFS transaction

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1276 of 1360

system, the company accepts payment from mFS mobile wallet accounts, either in the form of eMoney or through periodic settlements.

[0071] At least in some embodiments, financial transactions that take place in the mFS mobile wallet platform are funded through pre-paid mobile wallet accounts. Mobile wallet platform subscribers can deposit cash into their mobile wallet account through a process referred to herein as 'cash-in'. The cash-in process is supported by mFS agents at agent branch locations. The agent accepts the cash from the subscriber and transfers the equivalent amount of eMoney to the subscriber's mobile wallet account. This process is similar to withdrawing cash from a bank account.

[0072] As mentioned above, in some embodiments, financial transactions that take place in the mobile wallet platform are funded through pre-paid mobile wallet accounts. Mobile wallet platform subscribers can withdraw cash from their mobile wallet account through a process known as "cash-out". The cash-out process is supported by mFS agents at agent branch locations. The subscriber transfers eMoney from their mobile wallet account to the agent's eMoney account. Upon receiving the eMoney, the agent gives the subscriber cash from their branch cash register.

[0073] Accounts managed on the mFS platform by the mFS eMoney transaction processor maintain the mobile wallet balance of mFS program participants including subscribers, agent branches, agent companies, and non-agent companies. eMoney is moved between Mobile Wallet accounts by the transaction processor based on mFS transaction processing. Only when transactions involving cash (i.e. depositing or withdrawing funds from the mFS program) or the movement of money from mFS participants to non-mFS program participants are funds moved from the master bank accounts.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1277 of 1360

[0074] As subscribers, agents, and other mFS program participants conduct business in the mFS program, value is transferred from one account to the next as payment for services rendered or goods purchased. This value can be in the form of real currency or the electronic representation referred to herein as eMoney.

[0075] Among other situations, eMoney is used in mFS implementations where the real-time processing of financial transactions including card processing is not practical. The mFS platform utilizes an internal transaction processor for managing the real-time balance of mobile wallet and agent accounts as value (eMoney) is transferred from one mobile wallet to another in payment for services.

[0076] As subscribers conduct business with mFS agents, they deposit or withdraw cash from their mobile wallet accounts. Virtual or eMoney credits are transferred between the subscriber mobile wallet accounts and the agent branch accounts as a form of currency to support the transaction. As agents accept cash into their cash register by mFS subscribers, they transfer the equivalent amount of eMoney credits into the mFS subscriber's mobile wallet account. For example, if an mFS subscriber gives an mFS agent $10 to deposit into the subscriber's mobile wallet account, the agent would place the cash into his or her register, and transfer $10 from the agent branch eMoney account into the subscriber's mobile wallet account. While the agent acquired $10 in his or her register, the agent transferred-out $10 of eMoney credits from his or her branch eMoney account. This will be explained in greater detail below.

[0077] In some embodiments, employers may wish to participate in the mFS program by allowing the direct deposit of paychecks into subscribers' mobile wallet accounts. Accordingly, each payday, the user's pay is directly transferred to the subscribers' mobile wallet.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1278 of 1360

[0078] The term "know your customer" or "KYC" refers to information collected about an individual that identifies that individual. Such information is used to establish a mobile wallet account with the mobile wallet platform. Regulatory requirements in some countries require that new bank account creation must be preceded by a display of a valid government ID. These KYC regulations may vary from country to country. Accordingly, different KYC information may be requested from subscribers in different countries in order to establish a mobile wallet account.

[0079] The term micro-finance institution (MFI) refers to a lender that issues small loans. MFIs participating in the mFS program lend to mFS program subscribers and accept loan repayment either in the form of eMoney or settlements with the mFS platform provider.

[0080] The term "mFS program", like the term "mFS platform" refers to the ecosystem of companies, service providers, and subscribers that participate in providing mobile financial services to their customers. In some embodiments, there may be one mFS program implementation per country. Each program includes a program owner and operator, a program platform, a partner wireless services provider or MNO, and a partner bank.

[0081] The term "mFS program master account" refers to a bank account maintained by the mFS program partner bank to provide funds and float for the operation of the mFS platform. Depending on the type of mFS implementation, the master account can include sub-accounts for each of the agent branches and subscriber mobile wallets, giving the bank visibility into all transactions on a per-user basis. The mFS platform can also manage the balance of sub-accounts and interact with the bank's master account when funds need to be deposited or withdrawn from the account.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1279 of 1360

[0082] The term mobile network operator (MNO) refers to a provider of mobile phone service including basic voice, SMS, unstructured supplementary service data (USSD) and data service, and may also be referred to as a "wireless service provider".

[0083] The term "mobile wallet" or "mobile wallet account" refers to a stored value account or prepaid access account (PPA) that allows the owner (or "subscriber") to pay for goods and services on the mFS platform from his or her mobile wallet account. When the mFS eMoney transaction processor is used, the mobile wallet balance is maintained by the mFS platform and value is exchanged within the mFS program as eMoney. When the mFS platform is integrated to an external card processor, the mobile wallet utilizes funds from the subscriber's prepaid debit card and bank account to exchange value on the mFS platform.

[0084] The term "non-agent company" refers to a mFS program participant who accepts payments from mFS subscribers but does not provide the same services as mFS agent companies. Payment is accepted either in the form of eMoney or through periodic settlements with the mFS platform provider. Examples of non-agent companies include bill pay providers and micro-finance lenders.

[0085] The term "non-mFS subscribers" refers to unregistered users that participates in various use cases in the mFS program. Non-mFS subscribers can send money to or receive money from mFS subscribers through interaction with the mFS program agents or with international remittance providers.

[0086] The term "partner bank" refers to the primary bank participating in the mFS program. The partner bank is responsible for holding the mFS program master accounts that hold the funds for all mFS services and transactions. A "PIN" refers to a numeric password that may be required to perform a transaction via the mobile wallet application. A "transaction processor" refers to an application or service that manages

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1280 of 1360

the mFS program account balances. The transaction processor determines the amount of funds or eMoney is in a particular account at any given time, and manages account balances. Mobile transaction system requests to credit, debit, or view the balance of a particular mobile wallet or program account are handled by the transaction processor (in conjunction with other components of the mobile wallet platform).

[0087] The term "sub-accounts" refers to accounts that are maintained within the mFS platform or by an external card processor. A partner bank may elect to maintain a separate bank account for each subscriber and/or agent branch, or a single master account may be established that contains the funds for all of the subscriber mobile wallet and agent branch accounts (at least within a country or other geographical region). The balance of each individual user may be managed by the mFS transaction processor.

[0088] When using a master account, the bank is involved only in transactions that require the movement of funds external to the mFS program. For example, subscriber cash-in and cash-out transactions involve the addition and removal of cash from the mFS program and would consequently include a deposit or withdrawal from the master account. Retail purchases from participating mFS program retailers or the exchange of funds between mFS subscribers results in no net change in the mFS program balance and thus do not require involvement by the partner bank.

[0089] The term "subscriber" refers to a participant of the mFS mobile wallet platform. The subscriber maintains a mobile wallet balance and performs transactions using the mFS application. An "unbanked subscriber" is a subscriber that does not have (or does not have access to) a bank account or credit union account. The application or "mobile wallet application" provides mobile wallet functionality to the (unbanked) subscriber. The mobile wallet application is installed on a mobile device

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1281 of 1360

in the device's memory, on a SIM card (such as a GSM SIM card) or is otherwise accessible to the mobile device. The mobile wallet application provides the subscriber the ability to securely perform subscriber functions such as making retail purchases, paying bills, or transferring money to other mFS subscribers and non-subscribers. The mobile wallet application communicates with the mFS platform using binary and text SMS messages, among other forms of wireless communication. A wireless service provider or MNO provides the GSM network infrastructure on which the mFS platform operates.

[0090] Figure 1 illustrates an example system architecture for a mobile wallet platform. Integration tier 101 is configured to manage mobile wallet sessions and maintain integrity of financial transactions. Integration tier 101 can also include a communication (e.g., Web services) API and/or other communication mechanisms to accept messages from channels 111. Other mechanisms include, but are not limited to: International Standards Organization ("ISO") 8583 for Point of Sale ("POS") and Automated Teller Machines ("ATM") devices and Advanced Message Queuing Protocol ("AMQP") for queue based interfaces. Each of channels 111 can be integrated to one or more mechanisms for sending messages to integration tier 101. Notification services 102 is configured to send various notifications through different notification channels 112, such as, for example, Short Message Peer-to-Peer ("SSMP") for Short Messaging Service ("SMS") and Simple Mail Transfer Protocol ("SMTP") for emails. Notification services 102 can be configured through a web services API.

[0091] Service connectors 103 are a set of connectors configure to connect to 3rd party systems 113. Each connector can be a separate module intended to integrate an external service to the system architecture. Business process services 104 are

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1282 of 1360

configured to implement business workflows, including executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects. Payment handler 105 is configured to wrap APIs of different payment processors, such as, for example, banking accounts, credit/debit cards or processor 121. Payment handler 105 exposes a common API to facilitate interactions with many different kinds of payment processors.

[0092] Security services 106 are configured to perform subscriber authentication. Authorization services 107 are configured to perform client authorization, such as, for example, using a database-based Access Control List ("ACL") table.

[0093] Database 108 is configured to manage customer accounts (e.g., storing customer accounts and properties), manage company accounts (e.g., storing company accounts and properties), manage transaction histories (e.g., storing financial transaction details), store customer profiles, storing dictionaries used by the mobile wallet platform, such as, for example, countries, currencies, etc., and managing money containers. Rules engine 109 is configured to gather financial transaction statistics and uses the statistics to provide transaction properties, such as, for example, fees and bonuses. Rules engine 109 is also configured to enforce business constraints, such as, for example, transactions and platform license constraints.

[0094] Name matching engine 110 is configured to match different objects according to specified configuration rules. Matching engine 110 can be use to find similarities between names, addresses, etc. Transaction processor 121 is configured to manage financial accounts and transactions. The transaction processor 121 can be used to hold, load, withdraw and deposit funds to mobile wallet accounts. Transaction processor 121 can also be used as a common interface to a third party processor system. When used as a common interface, financial operations may be delegated to

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1283 of 1360

the external processor. A Clearing House subsystem of transaction processor 121 can be used to exchange the financial information with a bank.

[0095] Components of a mobile wallet platform can be connected to one another over (or be part of) a system bus and/or a network. Networks can include a Local Area Network ("LAN"), a Wide Area Network ("WAN"), and even the Internet. Accorindlgy, components of the mobile wallet platform can be "in the cloud". As such, mobile wallet platform components as well as any other connected computer systems and their components, can create message related data and exchange message related data (e.g., Internet Protocol ("IP") datagrams and other higher layer protocols that utilize IP datagrams, such as, Transmission Control Protocol ("TCP"), Hypertext Transfer Protocol ("HTTP"), Simple Mail Transfer Protocol ("SMTP"), etc.) over the system bus and/or network.

[0096] The components depicted in Figure 1 can interoperate to provide a number of financial and other services including but not limited to enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet, paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below. These services will be described in greater detail below with regard to system Figures 1 and 2, as well as Figures 3-19B.

[0097] Figure 2 depicts a monetary transaction system 200 similar to that described in Figure 1. The monetary transaction system 200 may provide a more

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1284 of 1360

simplified system structure in which each of the above services may be provided. The system includes a subscriber 205. The subscriber may have access to a bank account, or may be an unbanked subscriber. The subscriber has a profile 211 with the monetary transaction system 210. The profile includes the subscriber's KYC information, as well as any associated bank accounts, credit union accounts, bill pay accounts or other accounts. The subscriber has (or has access to) a mobile device 206 such as a phone or tablet. The mobile device runs the mobile wallet application (or mobile wallet application) 207.

[0098] The subscriber can indicate, using the mobile application 207 which transaction or other action he or she would like to perform. The indicated transaction 208 is sent to the mobile wallet platform 210 to be carried out by the platform. The transaction processor 216 (which may be similar to or the same as transaction processor 121 of Figure 1) performs the transaction(s) specified by the (unbanked) subscriber 205. The transaction processor may implement various other components to perform the transaction including memory 217, (wireless) communication module 215, rules engine 210 and/or transaction database 225.

[0099] Performing the specified transactions may include communicating with the monetary transaction database 225 to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile (for instance, whether the subscriber has enough eMoney in his or her stored value account, or has enough money in his or her bank account). Rules engine 220 may also be consulted to determine whether the subscriber has exceeded a specified number of allowed transactions. Then, if funds are available, and the transaction is otherwise permissible, the monetary transaction system can transfer money or eMoney 221 to or from an

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1285 of 1360

entity such as a user or agent (e.g. entity 222) to or from an establishment such as a retail store or agent company (e.g. entity 223).

[00100] In some cases, the monetary transaction system 210 application provides a web interface that allows subscribers to perform the same functions provided by the monetary transaction system application. For instance, mobile wallet application 207 may provide a web interface that allows a user to enroll for a mobile wallet. The web interface (or the mobile wallet application itself) receives a subscriber-initiated transaction over one of a plurality of channels (111 from Figure 1) connected to the monetary transaction system 210. The web interface or mobile wallet application may prompt for and receive enrollment information (e.g. KYC information) for the (unbanked) subscriber 205 over at least one of the plurality of channels (e.g. web, point-of-sale (POS), interactive voice response (IVR, etc.). The web interface or mobile wallet application may then send activation instructions over the same or a different channel to activate the (unbanked) subscriber 205 and create a subscriber account for the (unbanked) subscriber.

[00101] Once the subscriber has an account, the monetary transaction system generates a corresponding mobile wallet for the unbanked subscriber (available via the web interface and/or the mobile wallet application. The system then presents the (unbanked) subscriber's account data associated with the mobile wallet and/or a notification indicating that enrollment was successful to the subscriber. Accordingly, the mobile wallet application or the web interface may be used to provide user enrollment functionality. It should also be understood that either the mobile wallet application or the web interface may be used to provide substantially all of the mobile wallet functionality described herein.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1286 of 1360

[00102] It should also be noted that the mobile device 206 may be any type of plan-based phone or tablet, or prepaid phone or tablet. Many subscribers, such as unbanked subscribers, may primarily use prepaid phones. The mobile wallet application 207 may be installed on both plan-based phones and prepaid phones. The mobile wallet application may be installed on the device's SIM card, or on the device's main memory. Accordingly, the monetary transaction system 200 may be accessed and used via substantially any type of plan-based or prepaid mobile device.

[00103] Figure 3 shows three different graphics (301-303) and corresponding method steps (310-370) that illustrate an unbanked subscriber making a deposit using a mobile wallet (and, by extension, using the mobile wallet transaction system 210). In at least some of the embodiments described below, the actions of each participant are shown and described. This will also, at least in some embodiments, include an illustration of money flow throughout the mobile wallet transaction system. In the graphics, various terms are used as follows: $C = Cash Balance and $E = Electronic Money (eMoney) Balance.

[00104] At graphic 301, it is assumed that the unbanked subscriber (e.g. 205) has already registered and activated an eMoney account at an agent branch location (e.g. a retail store, gas station, or other location that has registered to be an agent branch). To deposit cash in order to get eMoney credit, the subscriber informs the agent manager or agent that they want to deposit a certain amount of cash (in 301). The agent manager/agent takes the cash and notifies the mobile wallet transaction system of the deposit using their agent manager or agent application (302). The transaction system 210 then credits the subscriber's eMoney account (303). Accordingly, any location that has registered to accept eMoney payments from subscribers' mobile wallets can also accept cash deposits. The agent branch's eMoney balance is reduced because

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1287 of 1360

their actual money balance was increased by the amount of the deposit. The subscriber's mobile wallet account is credited with eMoney in the amount of the deposit. In this manner, a subscriber can deposit cash into their mobile wallet account (in the form of eMoney) at any retail location or other agent branch location.

[00105] Thus, the agent manager receives the physical cash deposit into the subscriber's eMoney account via the agent manager or agent's application. The subscriber gives cash to agent manager or agent, and the mFS platform processes the request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends details (such as eMoney account balances, transaction logs, etc.) to bank specified by the mobile wallet platform. These details may be sent instantaneously as transactions occur, or in batches at pre-determined intervals.

[00106] In one embodiment, the monetary transaction system 210 of Figure 2 is implemented to deposit funds at an agent branch using a mobile wallet. The monetary transaction system 210 receives communication from an agent branch over one of a plurality of channels (e.g. 111) connected to the monetary transaction system (step 310). The agent communication indicates that the unbanked subscriber 205 desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account. The transaction processor 216 then validates the status of the unbanked subscriber's mobile wallet account (step 320) and determines if the agent branch is authorized to receive deposited money (i.e. determine if it has pre-registered as an official agent branch) (step 330).

[00107] The monetary transaction system may then use rules engine 220 to perform a limit check (to determine whether sufficient funds are available) and/or a velocity check (to determine whether the user has exceeded a specified number of (hourly, daily, or weekly) transactions) on the unbanked subscriber's mobile wallet

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1288 of 1360

account (step 340). The transaction system then credits the unbanked subscriber's mobile wallet account with the specified amount of funds (step 350) and returns a notification to the agent branch confirming the deposit (step 360) and returns another notification to the subscriber notifying the subscriber that the specified amount of funds was deposited in the their mobile wallet account (step 370). Any of channels 111 may be used to perform these communications.

[00108] Figure 4 shows three different graphics (401-403) and corresponding method steps (410-490) that illustrate an unbanked subscriber making a withdrawal using a mobile wallet (and, by extension, using the mobile wallet transaction system 210). As above, the terms in the graphics include "$C" representing cash balance and "$E" representing eMoney balance.

[00109] To withdraw cash at an agent branch, a subscriber submits a withdrawal request using their application (401). The subscriber may also enter information about the agent branch (e.g. name of establishment, name of agent, location or other information) that allows the monetary transaction system 210 to identify the agent branch. The transaction processor 216 may then determine whether the unbanked subscriber has enough eMoney to withdraw the requested amount. If he or she does have enough eMoney, then the subscriber's eMoney is deducted and that amount is transferred to the agent branch's eMoney account (402). Then, the agent branch gives the subscriber the requested amount of cash (403). In this manner, any entity that has established itself as an agent branch (including retail stores, gas stations, service providers, etc.) can provide cash withdrawal to a mobile wallet subscriber (whether banked or unbanked). The agent's or agent manager's role is to verify the withdrawal request (e.g. via SMS on the agent's or agent manager's phone) and gives the cash to subscriber. The subscriber requests cash withdrawal from agent branch's eMoney

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1289 of 1360

account via the application, and receives physical cash from agent manager/agent. The mobile wallet platform processes the request, updates the agent branch's and subscriber's eMoney balances, logs the transaction, and sends transaction details to a specified bank at pre-determined intervals.

[00110] In one embodiment, the monetary transaction system 210 is implemented to withdraw funds at an agent branch using a mobile wallet. The communication module 215 receives a communication from an unbanked subscriber over one of a plurality of channels 111 connected to the monetary transaction system 210 (step 410). The communication indicates that the unbanked subscriber 205 desires to withdraw a specified amount of funds from the unbanked subscriber's mobile wallet account at the agent branch. The monetary transaction system 210 validates the status of the unbanked subscriber's mobile wallet account (step 420) and determines if the balance of the unbanked subscriber's mobile wallet account is sufficient to accommodate the requested withdrawal for the specified amount of funds (step 430).

[00111] The transaction processor 216 performs one or more of a limit check (to verify sufficient funds) and a velocity check (to verify the subscriber hasn't exceeded specified transfer limits) on the unbanked subscriber's mobile wallet account (step 440). The monetary transaction system 210 then returns a secure, perishable withdrawal code to the subscriber 205 over at least one of the plurality of channels 111 connected to the monetary transaction system (step 450). The monetary transaction system 210 receives subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system indicating that the withdrawal code has been presented to the agent branch (step 460). The monetary transaction system 210 then debits the unbanked subscriber's mobile wallet account by the specified amount of funds (step 470), returns a notification to

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1290 of 1360

the agent branch confirming the withdrawal (step 480) and notifies the subscriber that the specified amount of funds was withdrawn from the unbanked subscriber's mobile wallet account over at least one of the channels 111 connected to the monetary transaction system (step 490). Accordingly, the monetary transaction system 210 may be used to allow subscribers to withdraw cash using their mobile wallet applications at any store or other entity registered as an agent branch.

[00112] Figure 5A depicts a subscriber-to-subscriber eMoney transfer. To perform such a transfer, subscriber A (501) enters some type of identification information identifying subscriber B (e.g. subscriber B's phone number) and an amount of money he or she wishes to transfer. The transaction processor 216 of the monetary transaction system 210 determines if there are sufficient funds to complete the transfer. If sufficient funds are available, the monetary transaction system 210 decrements subscriber A's account and credits subscriber B's account (502). The system then sends some kind of notification (e.g. SMS) to subscriber B indicating that a certain amount of money was transferred to their account. Subscriber A may also receive a notification that the transfer was successful. Accordingly, eMoney may be transferred between two mFS platform subscribers, one or both of which may be unbanked. The monetary transaction system 210 processes the subscribers' requests, updates the subscribers' eMoney balances, logs the transactions, and sends transaction information to a specified bank when needed.

[00113] Figure 5B illustrates a subscriber-to-non-subscriber eMoney transfer. In graphic 505, subscriber A wishes to send eMoney to another individual that is not a subscriber to the mFS platform. The transaction is initiated in the same fashion as the subscriber-to-subscriber transfer scenario. However, since non-subscriber B does not have a mobile wallet account, the monetary transaction system 210 cannot credit them

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1291 of 1360

with eMoney. Instead, the monetary transaction system 210 sends a notification (e.g. via SMS) to non-subscriber B with instructions for how to pick-up the transferred money, along with an authorization code (506). The monetary transaction system 210 puts a hold on subscriber A's account for the amount transferred. Subscriber B then has a specified number of days to pick up the cash before the hold expires and the amount is credited back to subscriber A's eMoney account by the monetary transaction system 210.

[00114] When non-subscriber B goes to pick up the money at an agent branch, the agent branch's manager or agent verifies the authorization code via an agent manager or agent mobile wallet application (that, in turn, accesses the mFS platform). Once the transfer has been validated, the agent gives the cash to non-subscriber B. The agent branch's mFS account is credited with the transfer amount (507) and the user leaves with the cash in hand (508). The mFS platform processes the transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction details to a platform-specified bank.

[00115] Figure 6A illustrates a subscriber-to-subscriber international eMoney transfer. This embodiment is, at least in some respects, similar to sending eMoney to an mFS subscriber domestically. In this case the monetary transaction system 210 leverages one or more existing international money transfer organizations or "remittance companies" such as MoneyGram®. In some embodiments, MoneyGram® is pre-integrated to the monetary transaction system 210, but other international money transfer organizations may also be used. Still further, at least in some embodiments, subscriber B may need to have an eMoney account with a foreign mFS program that is also affiliated with MoneyGram® or another international money transfer organization.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1292 of 1360

[00116] In Figure 6A, subscriber A initiates the international eMoney transfer at 601, the international money transfer organization (e.g. MoneyGram®) transfers the eMoney to subscriber B at 602 and subscriber B's eMoney balance is increased by the transferred amount. Thus, subscriber A requests to send eMoney from his or her eMoney account via the mobile wallet application. The eMoney is transferred using an international money transfer organization, and subscriber B receives a notification (that may, for example, include a reference number, among other information) that their eMoney balance has increased by the transfer amount. The monetary transfer system 210 processes subscriber A's request, updates subscriber A's and subscriber B's eMoney balances, logs the transaction, and send transaction details to a mFS platform-specified bank.

[00117] Figure 6B illustrates a subscriber-to-non-subscriber international eMoney transfer. In this illustration, subscriber A wishes to send cash to subscriber B who is not an mFS program subscriber. Similar to the scenario described in Figure 6A, the monetary transaction system 210 leverages various international money transfer organizations or remittance companies such as MoneyGram® to transfer the eMoney. Subscriber A initiates a typical eMoney transfer at 605 by providing non-subscriber B's identification information, as well as the amount to be transferred. The Monetary transaction system 210 recognizes the eMoney transfer is not destined for a domestic phone number and routes the request to the international money transfer organization (e.g. MoneyGram®) (606).

[00118] The international money transfer organization sends non-subscriber B a notification (e.g. via SMS) with instructions for how and where to pick up the money (in embodiments where MoneyGram® transfers the eMoney, the notification may include a MoneyGram® reference number (MGRN)) (607). Non-subscriber B can

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1293 of 1360

then show the MGRN to an agent at an agent branch (608) and then receive the cash (609). The monetary transaction system 210 then decrements subscriber A's eMoney account for the transferred amount. The monetary transfer system 210 thus processes subscriber A's transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction detail to a platform-specified bank. It should also be noted that an mFS subscriber may also receive money in a foreign country from either a subscriber or a non-subscriber in a similar manner.

[00119] Figure 7 illustrates a subscriber purchasing airtime using a mobile wallet. Mobile wallet platform subscribers may buy airtime by using their mobile wallet application 207. The monetary transaction system 210 will reload their airtime account within the mobile network operator's (MNO's) systems. The subscriber requests to purchase airtime by entering the request via the mobile wallet application or via a mobile wallet web interface. The monetary transaction system 210 then decrements the subscriber's eMoney account (701), while crediting the mFS platform's eMoney account (702). The purchased airtime is then added to the subscriber's airtime balance (703). The monetary transaction system 210 processes the subscriber's request, updates the subscriber's eMoney balances as well as its own eMoney balance, logs the transaction, and sends transaction detail to a mFS platform-specified bank.

[00120] In one embodiment, the monetary transaction system 210 is implemented to top up a prepaid mobile account from a mobile wallet. The communication module 215 of the monetary transaction system 210 receives a subscriber communication over one of a plurality of channels 111 connected to the monetary transaction system (step 710). The subscriber communication indicates that an unbanked subscriber 205 desires to top up a prepaid mobile account by a specified amount using a specified

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1294 of 1360

payment method from the unbanked subscriber's mobile wallet. The transaction processor 216 validates the status of the selected payment method (step 720) and performs a limit check and/or a velocity check on the selected payment method (step 730). The monetary transaction system 210 then debits the specified payment method by the specified amount of funds (step 740) and processes the mobile top-up via a billing system integrator and/or an aggregator (step 750), and notifies the subscriber that the prepaid mobile account was topped up over at least one of the channels connected to the monetary transaction system (step 760).

[00121] Figure 8 illustrates an embodiment where a mFS subscriber pays a bill using a mobile wallet. At least in some embodiments, the company that the subscriber wishes to pay needs to have signed-up to be part of the mFS platform. The mFS platform may publish a list of company names that have registered to be part of the mFS platform. This list of companies may include company IDs so that subscribers can know which company ID to enter in their mobile wallet application. Once the company ID is known, the subscriber can pay a bill by entering the company ID and the amount to be paid. The monetary transaction system 210 then decrements the subscriber's eMoney account (801) and credits the identified company's eMoney account (802). Accordingly, in response to the subscriber's request to pay bill via their mobile wallet application, the monetary transaction system 210 processes the request, updates the bill pay company's and the subscriber's eMoney balances, logs the transaction, and sends transaction details to the mFS platform-specified bank.

[00122] In one embodiment, the monetary transaction system 210 is implemented to pay a bill from a mobile wallet. The communications module 215 of the monetary transaction system 215 receives a subscriber communication over a communication channel 111 connected to the monetary transaction system (step 810). The subscriber

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1295 of 1360

communication indicates that unbanked subscriber 205 desires to pay a bill for a specified amount using a specified payment method from the unbanked subscriber's mobile wallet (e.g. eMoney). The monetary transaction system 210 validates the status of the selected payment method (step 820) and performs a limit check and/or a velocity check on the selected payment method to ensure the eMoney transfer is permissible (step 830). The monetary transaction system then debits the specified payment method by the specified amount of funds (step 840), processes the bill payment via a direct biller connection or a bill pay aggregator (step 850), and notifies the unbanked subscriber that the bill was paid using a communication channel (e.g. SMS) connected to the monetary transaction system (step 860). Thus, in this manner, a subscriber may use a mobile wallet to pay various bills including rent, utility, mortgage, phone, cable, medical and other bills.

[00123] Figure 9 illustrates a mobile wallet subscriber making a retail purchase. Mobile wallet subscribers can make retail purchases at agent branches directly from their mobile device. Agent branches, as explained above, are retail stores or other entities that have registered with the mFS system and are able to accept mobile wallet payments. Accordingly, a subscriber can select the items they wish to purchase, and indicate (via the mobile wallet application) to the agent branch that they wish to pay for the items. The mobile wallet application then communicates with the agent branch and the monetary transaction system to indicate the price of the transaction. The monetary transaction system 210 then debits the subscriber's eMoney account (901) and credits the agent branch's eMoney account (902). The agent branch (and/or the agent manager or agent) receives confirmation that subscriber paid for the purchase. The subscriber may also receive a summary of the retail purchase and may be asked to confirm the purchase by entering a PIN. The monetary transaction system

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1296 of 1360

processes the purchase request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends transaction details to a mFS platform-specified bank.

[00124] In one embodiment, the monetary transaction system 210 is implemented to make a purchase from a mobile wallet. The communications module 215 of the monetary transaction system 210 receives a communication from a subscriber over a communication channels 111 (step 910). The subscriber communication indicates that an unbanked subscriber 205 desires to purchase an item for a specified amount of funds using a specified payment method from the unbanked subscriber's mobile wallet.

[00125] The monetary transaction system 210 then returns a secure, perishable purchase code to the unbanked subscriber over at least one of the channels connected to the monetary transaction system (step 920) and receives a subsequent agent branch communication over a channel indicating that the purchase code has been presented to an agent (branch) (step 930). The monetary transaction system 210 validates the status of the specified payment method (step 940), determines if the specified payment method can accommodate a purchase for the specified amount (step 950), performs a limit check and/or a velocity check on the selected payment method (960), debits the specified payment method by the specified amount of funds (970), returns a notification to the agent branch authorizing the purchase (980) and sends a receipt to the unbanked subscriber over a communication channel. The monetary transaction system 210 may thus be used to make a retail purchase using a mobile wallet.

[00126] Figure 10A illustrates a subscriber requesting a micro-loan. Financial institutions and potentially other mFS program participants may sign up to become money or eMoney lenders. Mobile wallet subscribers may be able to use their mobile

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1297 of 1360

wallets to request micro-loans from these approved lenders. The micro-loans are tracked by the monetary transaction system 210, and repayment reminders, interest and commissions are managed by the monetary transaction system. The subscriber requests a micro-loan from a lender, indicating the amount in the request, as well as other information such as the repayment date and the commission (i.e. interest rate). Potential lenders then have a chance to counter the loan request with their own terms. Once the lender approves the subscriber's request, the lender's eMoney account balance is debited for the specified amount (1001) and the subscriber's eMoney account is credited with the requested amount (1002). The monetary transaction system 210 processes the micro-loan requests, update the lender and subscriber's eMoney balances, sets up repayment schedules and reminders, logs the transaction, and sends transaction detail to a mFS bank. It should also be noted that while the term "micro-loan" is used herein, the loan may be for substantially any amount of money.

[00127] Following on the embodiment described in Figure 10A, Figure 10B illustrates a subscriber repaying a micro-loan. The subscriber may repay the loan using functionality provided in the mobile wallet application or in a similar web interface. Repayments can be made in installments or in full depending on the rules of the micro-loan. The subscriber enters the amount they wish to repay and the loan ID. The subscriber's eMoney account is then debited for the specified amount (1005), while the lender's eMoney account is credited the specified amount (1006). Both the lender and the subscriber may receive confirmation that the loan has been repaid via SMS or some other communication channel. The mFS platform thus processes the subscriber's micro-loan repayment request, updates lender and subscriber's eMoney balances, updates repayment schedule and reminders, logs the transaction, and sends transaction details to a specified mFS platform bank.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1298 of 1360

[00128] Figure 11A illustrates a subscriber receiving a direct deposit from an employer or other entity. Subscribers to the mFS platform have the ability to receive any direct deposit into their eMoney account. Subscribers may be asked by their employers to provide account information in order to set up direct deposit. The employer then submits a direct deposit request using their existing processes (i.e the processes they use for a normal checking or savings bank account). Once the direct deposit is set up and a payday arrives, the employer's bank account is debited for the proper amount (1101) and the employer's mFS account is credited with that amount (1102). Then, once the funds have been received at the mFS platform bank, the mFS platform bank sweeps the employers direct deposit balance (1103) into a mFS platform master account (1104) and notifies the mFS platform of each account to be incremented (including the subscriber's mobile wallet (eMoney) account). The subscriber's eMoney account is then credited with the paycheck amount (1105) upon which the eMoney may be used to pay for goods, pay bills, top up airtime, transfer to other entities or for cash withdrawal.

[00129] The subscriber does not need to have a bank account to participate in direct deposit. The employer's bank can communicate with the mFS platform's bank to perform the necessary steps in directly depositing the subscriber's paycheck in his or her eMoney mobile wallet account. The bank facilitates monetary deposit into the employer's bank account for direct deposit and performs an automated sweep of recent deposits from the employer's bank account into the mFS platform's master bank account. The bank also sends transaction details to the monetary transaction system 210 including transaction logs. The monetary transaction system receives a list of eMoney accounts that are to be credited directly from the employer (or bank), processes the list and requests to establish a direct deposit, updates subscriber's

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1299 of 1360

eMoney balance, log the transaction, and sends transaction details to the mFS platform bank.

[00130] In a similar manner, a subscriber may receive a government welfare payment directly on their mobile device. Figure 11B illustrates a subscriber receiving a government social welfare payment directly into their eMoney account. In some embodiments, subscribers may need to opt-in and register with the government program for which they choose to receive the payment via their mobile wallet. Once the funds have been received, the subscriber can use that eMoney for any goods or services, as described above. Once the direct deposit has been established and a payout has been initiated, the government's welfare account deposits the money (1110) into the government's bank account for welfare payments (1111) and performs an automated sweep of recent deposits from the government's bank account (1112) into the mFS program's master bank account (1113). The bank then sends transaction details to the monetary transaction system 210 regarding the deposit. The subscriber receives a notification that the welfare payment has been credited to their eMoney account (1114). The mFS platform receives an indication of eMoney accounts that are to be credited from the government, processes the welfare payments, updates the subscriber's eMoney balance, logs the transactions, and sends transaction details to the mFS platform bank.

[00131] Figure 12A illustrates an agent administrator distributing eMoney to various recipients. An agent administrator, as explained above, is a person who acts as an agent company's representative. The agent administrator deposits, withdraws, and distributes funds into and out of the agent company's bank account. When an agent administrator deposits cash into an agent company's bank account, it is credited as eMoney to the agent company's account. In order to provide the agent branches with

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1300 of 1360

eMoney, the agent administrator first moves the eMoney from the agent company's account (1201) to the branch accounts (1202). This is performed using the agent administrator's mobile wallet application or portal. In an agent administrator money transfer, the monetary transaction system 210 processes the administrator's eMoney transfer request, updates the agent company and agent branch eMoney balances, logs the transaction, and sends transaction details to the mFS platform bank.

[00132] Figure 12B illustrates an agent company deposit. The agent company has an eMoney account in the monetary transaction system 210 that may also include a corresponding bank account (that may be created automatically upon creation of the agent company's eMoney account). After the agent company's bank account has been set up, the agent administrator can make deposits into that account. As Figure 12B shows, once cash (1205) has been deposited into the bank account (1206), it is transferred to a mFS platform master account (1208) that includes all or a part of the mFS platform's funds. The agent company's bank account is decreased by the deposit amount (1207), while the agent company's eMoney account balance is correspondingly increased (1210). At this time, the agent company account is credited with eMoney. The agent company's bank facilitates a physical cash deposit into the agent company's bank account and performs an automated sweep (1209) of recent deposits from the agent company's bank account into the mFS platform's master bank account. The agent company's bank then sends transaction details to the monetary transaction system 210. The agent administrator physically delivers the cash (or form of money such as a check or money order) to a bank branch for deposit. The monetary transfer system receives transaction details from the agent company's bank about recent transactions (including deposits, as shown in Figure 12B.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1301 of 1360

[00133] Figure 13 illustrates an agent company withdrawal. To make a cash withdrawal for an agent company, the agent administrator requests a withdrawal using the agent administrator mobile wallet application. The monetary transaction system 210 then notifies the bank that a certain amount of eMoney is to be transferred from the master mFS account (1302) to the agent company bank account (1303). When the money is in the agent company bank account, the agent administrator can withdraw the cash by traditional withdrawal means. The mFS master bank receives transaction details from the monetary transaction system 210 about recent transactions (recent withdrawals in this case). The mFS master bank performs an automated sweep (1304) of the mFS platform's master bank account to reflect the recent withdrawal request from agent the agent company (1301). The agent company's eMoney account is reduced by the amount of the withdrawal. The agent company also sends transaction details to the monetary transaction system 210. The agent administrator can request withdrawal via the agent administrator mobile wallet application and physically withdrawal cash (1305) from the agent company's bank branch (1306). The mFS platform processes the agent company's withdrawal request, updates agent company and agent branch eMoney balances, logs the transaction, and sends transaction details to an mFS platform-specified bank.

[00134] Attention will now be turned to embodiments in which subscribers have bank accounts associated with their mobile wallets. The monetary transaction system 210 provides similar functionality to consumers that have bank or credit union accounts. Although many different transactions are presented herein, many more and varied types of transactions may be processed by the monetary transaction system. In the following figures, "$C" refers to cash balance, "$DC" refers to a debit card (prepaid) balance and "$PIN" refers to a recharge PIN value.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1302 of 1360

[00135] Figure 14 describes a subscriber deposit at an agent branch. The subscriber has a registered and activated (prepaid) debit card at an agent branch location. The prepaid debit card is associated with the mobile wallet application in the subscriber's mobile device. As such, the debit card is linked to the subscriber's account in the monetary transaction system 210. To deposit cash onto the mobile wallet, the subscriber informs the agent that they want to deposit a specified amount of cash (1401). The agent takes the cash and notifies the monetary transaction system 210 of the deposit using their point of sale (POS) system or the agent mobile wallet application (1402), and the monetary transaction system 210 credits the subscriber's mobile wallet account (1403). The funds collected at the cash register typically do not reach a bank account until the reconciliation and settlement of funds occurs between the agent and the mFS owner's bank.

[00136] The subscriber's bank then receives a settlement report from the card processor and receives funds from the agent's bank. The agent or agent manager physically deposits the cash into the subscriber's mobile wallet account via their POS system or agent manager/agent mobile wallet application. The monetary transaction system processes the deposit request, increments the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor increments the subscriber's mobile wallet balance and sends reports to the bank for settlement on a regular (e.g. nightly) basis.

[00137] In one embodiment, the monetary transaction system 210 is implemented to deposit funds into a bank or credit union account using a mobile wallet. The communications module 215 of the monetary transaction system 210 receives communication from an agent branch over a communication channel (step 1410). The agent communication indicates that a subscriber 205 desires to deposit a specified

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1303 of 1360

amount of funds into a bank or credit union account. The transaction processor 216 validates the status of the bank or credit union account (step 1420), determines if the agent branch is authorized to deposit money (step 1430), and performs a limit check and/or a velocity check on the bank or credit union account (step 1440). The monetary transaction system then credits the bank or credit union account with the specified amount of funds (step 1450), returns a notification to the agent branch confirming the deposit (step 1460) and notifies the subscriber that the specified amount of funds was deposited in the bank or credit union account using at least one of the communication channels connected to the monetary transaction system (step 1470). Accordingly, cash may be deposited into a bank or credit union account associated with a subscriber's mobile wallet.

[00138] Figure 15 illustrates a subscriber deposit that is performed with a non-agent. In some economies, subscribers may have the ability to leverage other channels outside of agents to deposit funds onto their card. One deposit method is a PIN-based recharge that allows a subscriber to purchase a PIN worth the deposit value. The PIN can then be redeemed via an interactive voice response (IVR) system or via the subscriber's mobile wallet application. The mobile wallet application will allow the monetary transaction system 210 to deposit the funds onto the subscriber's card. The retailer's bank settles with the PIN card provider's bank and the PIN card provider's bank settles with the mFS platform's bank for the deposit. The subscriber gives cash to the agent (1501) which increases the agent company's physical cash (1502). The subscriber uses IVR or their SIM Application to recharge mobile wallet account using a PIN card (1503). In some cases, an agent may provide the PIN card (i.e. the prepaid debit card) to the subscriber. The monetary transaction system 210 processes the subscriber deposit request, increments the subscriber's mobile wallet balance within

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1304 of 1360

the card processor and logs the transaction. An external card processor decreases the subscriber's PIN card balance (1504), increments the subscriber's mobile wallet balance (1505) and send reports to the mFS platform bank for settlement.

[00139] Figure 16 illustrates a subscriber withdrawal at an agent branch. To withdraw cash at an agent branch from a (prepaid) debit card, a subscriber submits a withdrawal request using the mobile wallet application on their mobile device. The subscriber may also need to enter details about the agent branch that allows the monetary transaction system 210 to determine if the subscriber has sufficient funds on their debit card. The mFS platform then notifies the agent branch that it can give cash to the subscriber. If the subscriber has sufficient funds, the monetary transaction system 210 will decrement the subscriber's funds from their card (1601) and transfer it to the mobile wallet owner's account within the same card processor or bank. The agent branch (1602) then provides the withdrawn cash to the subscriber (1603).

[00140] Accordingly, the subscriber requests a cash withdrawal from their own mobile wallet account via the mobile wallet application. The agent or agent manager verifies the withdrawal request via POS authorization or SMS received on agent's phone and, once verified, gives cash to the subscriber. The monetary transaction system 210 processes the subscriber's withdrawal request, decrements the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor decrements the subscriber's mobile wallet balance and sends reports to the bank for settlement on a periodic basis.

[00141] In one embodiment, the monetary transaction system 210 is implemented to withdraw funds from a bank or credit union account using a mobile wallet. The communication module 215 of the monetary transaction system 210 receives a communication from a subscriber 205 over a communication channel 111 (step 1610).

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1305 of 1360

The subscriber communication indicates that subscriber 205 desires to withdraw a specified amount of funds from a bank or credit union account. The transaction processor validates the status of the bank or credit union account (step 1620), determines if the balance of the bank or credit union account is sufficient to accommodate the requested withdrawal for the specified amount of funds (step 1630) and performs a limit check and/or a velocity check on the bank or credit union account (step 1640).

[00142] The monetary transaction system 210 then returns a secure, perishable withdrawal code to the subscriber 205 over at least one of the communication channels (step 1650) and receives a subsequent agent branch communication indicating that the withdrawal code has been presented to an agent (step 1660). The monetary transaction system 210 then debits the bank or credit union account by the specified amount of funds (step 1670), returns a notification to the agent branch confirming the withdrawal (1680) and notifies the subscriber that the specified amount of funds were withdrawn from the bank or credit union account using at least one of the communication channels connected to the monetary transaction system (step 1690). Accordingly, a subscriber can withdraw cash stored on their mobile wallet from an agent branch or a non-agent branch.

[00143] Figure 17A illustrates a subscriber withdrawal using an automated teller machine (ATM). Subscribers in many countries have access to ATM machines and can use their mobile wallets to perform withdrawals using their (prepaid) debit card at most ATMs. Banks provide ATMs to their customers (typically at no charge) and to non-customers (typically for a small charge). The subscriber requests a cash withdrawal from the subscriber's mobile wallet via the subscriber's debit card that is associated with the mobile wallet. The bank providing the debit card may receive

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1306 of 1360

settlement reports from the card processor and may transfer and/or settle funds from subscriber's account to the ATM network bank. An extern card processor decrements the subscriber's mobile wallet balance (1701) and sends transaction reports to the bank for settlement. Accordingly, once the withdrawal request has been received and the external card processor (e.g. Visa® or MasterCard®) (1702) has debited the debit card account, the ATM (1703) dispenses the withdrawn cash to the subscriber (1704).

[00144] Figure 17B illustrates a subscriber-to-subscriber money transfer. An mFS subscriber (1705) may send money to another mFS subscriber (1706). To do so, subscriber A enters information identifying subscriber B (e.g. a phone number, email address or other identifier). The monetary transaction system 210 determines if there are enough funds to complete the transaction, and if so, the monetary transaction system 210 decrements subscriber A's debit card and credits subscriber B's debit card. The subscriber, accordingly, may request to send money from their own mobile wallet (i.e. money stored on a (prepaid) debit card) account via the subscriber mobile wallet application. The other subscriber receives a notification that the balance of the debit card associated with their mobile wallet has increased. The bank receives a settlement report from the debit card processor and transfers or settles funds from subscriber A's account to subscriber B's account (if necessary). The monetary transaction system 210 processes the transfer request, updates subscriber A's and subscriber B's debit cards that are associated with their mobile wallets and logs the transaction. The external card processor decrements subscriber A's debit card balance, increments subscriber B's debit card balance and sends transaction reports to the mFS platform bank for settlement.

[00145] Figure 17C illustrates subscriber-to-non-subscriber money transfers. In this embodiment, subscriber A (an mFS subscriber) wishes to send money to another

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1307 of 1360

subscriber (a non-mFS subscriber). The transaction is initiated in the same fashion as described above in Figure 17B. However, since subscriber B does not have an mFS account, the monetary transaction system 210 cannot credit them with money. Instead, the monetary transaction system 210 sends a communication (e.g. a SMS) to subscriber B (1708) with an authorization code and instructions for how to pick up the cash. The monetary transaction system 210 puts a hold on subscriber A's debit card for the amount transferred (1707). Subscriber B has a specified time period in which to pick up the cash before the hold expires and the amount is credited back to the debit card associated with subscriber A's mobile wallet account. The agent branch verifies the authorization code via POS or their agent mobile wallet application (1709) and gives the cash to the non-subscriber (1710). (In some countries, an agent network needs to be capable of giving cash to a subscriber based on the money transfer reference number).

[00146] The mFS bank receives a settlement report from the card processor and transfer and settle funds from subscriber A's debit card to the agent's bank (if necessary). The monetary transaction system 210 processes the money transfer request, decrements subscriber A's mobile wallet balance within the card processor, generates a money transfer reference number, authorizes the reference number to be paid out by the agent and logs the transaction. An external card processor decrements subscriber A's mobile wallet balance and sends periodic transaction reports to the bank for settlement. Thus, as seen in Figures 17B and 17C, money may be transferred from subscriber to subscriber and from subscriber to non-subscriber.

[00147] Subscribers may similarly send money internationally to both subscribers and non-subscribers. Figure 18A illustrates a subscriber-to-subscriber international money transfer. In this embodiment, subscriber A wishes to send cash to subscriber B

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1308 of 1360

who resides in another country. As in the embodiments described above where money was transferred internationally, the monetary transaction system 210 may use one or more international money transfer organizations or remittance companies such as MoneyGram® to transfer the money. Subscriber A initiates the international money transfer using his or her phone. Subscriber A's debit card account is decremented by the transfer amount (1801). The money is transferred between countries using an international money transfer organization (1802). In this case, subscriber B has an mFS eMoney account with a foreign mFS platform that is also affiliated with the selected international money transfer organization. That organization can then credit subscriber B's eMoney account directly (1803).

[00148] Thus, subscriber A requests to send money from their debit card account via the subscriber mobile wallet application. Subscriber B receives a notification (including a MoneyGram® Reference Number (MGRN) (or other reference number when other international money transfer organizations are used) and instructions on how to access the eMoney) that their eMoney balance has increased. The mFS bank receives settlement reports from the debit card processor and transfers and/or settles funds from subscriber's account to the international organization's bank. The monetary transfer system 210 processes the transfer request, update subscriber A's and subscriber B's eMoney balances and logs the transaction. An external card processor decrements subscriber A's mobile wallet balance and sends periodic transaction reports to the bank for settlement.

[00149] Figure 18B illustrates a subscriber-to-non-subscriber international money transfer. In this embodiment, subscriber A wishes to send cash to subscriber B who resides in another country. As above, the monetary transaction system 210 uses an international money transfer organization (1806) to transfer the money between

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1309 of 1360

countries. Once the transfer has been initiated by subscriber A, the international money transfer organization debits subscriber A's debit card account (1805) and transfers that money to subscriber B. Subscriber B (1807) receives a notification (e.g. via SMS) with pick up instructions and a transfer ID number. Subscriber B can then go to an agent company (1808), show them the notification (including, perhaps an authorization code), and receive the transferred money (1809).

[00150] Similar to the transaction described in Figure 18A, the embodiment of 19A illustrates a transaction where a subscriber receives an international money transfer. Subscriber B (1901) initiates a money transfer using their mobile wallet application. The international money transfer organization (1902) debits subscriber B's eMoney account balance. This money is then transferred by the international money transfer organization to subscriber A. Subscriber A receives a notification along with a transfer ID number indicating that their debit card account has been credited with the transferred money (1903).

[00151] Figure 19B illustrates a non-subscriber-to-subscriber international money transfer. This scenario is very similar to that described in Figure 19A from the mFS subscriber's perspective, except that their eMoney account is credited here, and their debit card account was credited in 19A. The initiator, subscriber B (1905), does not have an mFS account and, as a result, takes their cash to an international money transfer organization (e.g. MoneyGram®) or other remittance company's agent (1906) to send it to subscriber A's mobile wallet eMoney account. The international money transfer organization (1907) then transfers the specified amount to subscriber A (1908) and subscriber A's mobile wallet eMoney account is credited with the amount of the transfer. Subscriber A may receive a transaction ID number, along with an indication that the transfer has occurred. The mFS bank may receive settlement

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1310 of 1360

reports from the card processor and settle funds from the international money transfer organization's bank to subscriber A's mobile wallet account. The monetary transaction system processes the money transfer request, updates subscriber A's mobile wallet balance within the card processor and logs the transaction. An external card processor increments subscriber A's mobile wallet balance and sends periodic transaction reports to the mFS bank for settlement.

[00152] Other functionality described above in relation to using an eMoney mobile wallet account may also apply to banked subscribers using a debit card associated with their mobile wallet. Such subscribers may buy airtime for their mobile device, pay bills, make retail purchases, receive direct deposits, and perform other functionality.

[00153] In one embodiment, the monetary transaction system 210 is implemented to add a mobile wallet platform stored value account to a mobile wallet. The stored value account may include eMoney or other monetary credits. In the embodiment, communication module 215 of monetary transaction system 210 may receive subscriber data for an unbanked subscriber 205 over a communication channel. The transaction processor may perform validation checks on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber. The monetary transaction system 210 may then send subscriber data to another entity (such as a third party verification system) for identification of the unbanked subscriber. The monetary transaction system 210 receives results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber, creates a stored value account for the unbanked subscriber that maintains a recorded balance for the created stored value account, adds the stored value account to the unbanked subscriber's mobile

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1311 of 1360

wallet and notifies the unbanked subscriber of the addition of the stored value account over at least one communication channel connected to the mobile wallet platform.

[00154] In another embodiment, the monetary transaction system 210 is implemented to add a third party stored value account to a mobile wallet. The monetary transaction system 210 receives unbanked subscriber data, including account details, over a communication channel. The transaction processor 216 performs a validation check on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber. If the validation check is ok, the monetary transaction system 210 sends subscriber data to a third party verification system for identification of the unbanked subscriber. In some cases, validating the status of the sender or the recipient includes performing a check on the specified sender or recipient to comply with the office of foreign assets control. The monetary transaction system 210 then receives results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber, and submits the unbanked subscriber's account details to a third party account processor. The monetary transaction system 210 receives an indication from the third party account processor that third party account processor created a third party stored value account for the subscriber. The transaction processor maintains a link between the subscriber data and the third party stored value account and adds the third party stored value account to the unbanked subscriber's mobile wallet. The monetary transaction system 210 then notifies the unbanked subscriber of the addition of the third party stored value account over a communication channels connected to the monetary transaction system.

[00155] In another embodiment, the monetary transaction system 210 is implemented to add a bank or credit union account to a mobile wallet. The

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1312 of 1360

communication module 215 receives subscriber data, including bank or credit union account details, over a communication channel 111. The transaction processor 216 performs validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber and sends subscriber data to a third party verification system for identification of the subscriber. The communication module then receives results from the third party verification system indicating that the subscriber data appropriately identifies the subscriber. Upon receiving these results, the monetary transaction system 210 submits bank or credit union account details for validation by the transaction processor, receives an indication that the bank or credit union account details correspond to a valid bank or credit union account, maintains a link between the subscriber data and the bank or credit union account and notifies the subscriber of the bank or credit union account validation over a communication channel.

[00156] In still another embodiment, the monetary transaction system is implemented to add a debit or credit card account to a mobile wallet. The communication module 215 receives subscriber data, including a debit or credit card account number, over a communication channel 111 connected to the monetary transaction system. The transaction processor performs validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber. The communication module sends subscriber data to a third party verification system for identification of the subscriber and receives results from the third party system indicating that the subscriber data appropriately identifies the subscriber. The monetary transaction system 210 securely stores the debit or credit card account number for access by the mobile wallet (e.g. in memory 217 or transaction database 225), adds the debit or credit card account number to the

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1313 of 1360

subscriber's mobile wallet, and notifies the subscriber of the addition of the debit or credit card account number. It should be noted that many other transactions can take place over the monetary transaction system, and that the embodiments described herein should not be read as limiting.

[00157] Embodiments of the invention can adhere to Know Your Customer (KYC) rules in the US by performing Customer Identification Program (CIP) checks as required by the Bank Secrecy Act and US PATRIOT Act. A minimum amount of information can be gathered about a customer, such as, for example, first name, last name, date of birth, government ID Type, government ID number and address. The CIP processes are designed to validate customer identity against government blacklists and assists in the prevention of money laundering and terrorist financing. A combination of non-documentary and documentary verification can be used to ensure beyond a reasonable doubt the identity of the customer.

[00158] Non-documentary verification can occur through the presentment of the information that was collected from the user to an external third party, such as, for example, Lexis Nexis(R). Documentary verification can occur if non-documentary verification fails, then the user is asked to present an unexpired government ID. Various differ forms of identification including driver's license, passport, alien identification (e.g., green card or work visa), and Mexican Consular identification card, can be accepted.

[00159] Embodiments of the invention can perform Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) checks. AML and CFT checks can be performed using transaction monitoring methods to flag names and suspicious transactions for further investigation. The mobile wallet platform can perform AML and CFT checks on all electronic financial transactions to ensure that

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1314 of 1360

electronic funds are not being used for money laundering or terrorism. Transaction limits can be placed on user accounts. The transaction limits are fully configurable for each particular use case, channel and payment method that allows maximum flexibility to restrict higher risk use cases. Velocity checks can also be performed. Velocity Checks ensure that subscribers are not abusing the mobile wallet platform within the allowable limits.

[00160] The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1315 of 1360

CLAIMS

We claim:

1. A monetary transaction system for conducting monetary transactions between unbanked subscribers and other entities, the system comprising:

a mobile device configured to run a monetary transaction system application;

an unbanked monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the unbanked subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;

a monetary transaction system processor that performs the one or more transactions specified by the unbanked subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile; and

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system.

2. The monetary transaction system of claim 1, wherein the monetary transaction system application provides a web interface that allows subscribers to perform the same functions provided by the monetary transaction system application.

3. The monetary transaction system of claim 1, wherein the monetary transaction system application is provided on a prepaid or postpaid phone.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1316 of 1360

4. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to enroll a user for a mobile wallet, including the following steps:

receiving a subscriber-initiated transaction over one of a plurality of channels connected to the monetary transaction system;

prompting for and receiving enrollment information for the unbanked subscriber over at least one of the plurality of channels;

sending activation instructions over a second channel to activate the unbanked subscriber and create a subscriber account for the unbanked subscriber;

generating a mobile wallet for the unbanked subscriber; and

presenting the unbanked subscriber's account data associated with the mobile wallet to the unbanked subscriber.

5. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to add a mobile wallet platform stored value account to a mobile wallet, including the following steps:

receiving subscriber data over one of a plurality of channels connected to the mobile wallet transaction system;

performing one or more validation checks on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber;

sending subscriber data to the at least one entity for identification of the unbanked subscriber, wherein the entity comprises a third party verification system;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1317 of 1360

receiving results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber;

creating a stored value account for the unbanked subscriber, wherein the monetary transaction system processor maintains a recorded balance for the created stored value account;

adding the stored value account to the unbanked subscriber's mobile wallet; and

notifying the unbanked subscriber of the addition of the stored value account over at least one other of the plurality of channels connected to the mobile wallet platform.

6. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to add a third party stored value account to a mobile wallet, including the following steps:

receiving unbanked subscriber data, including account details, over one of a plurality of channels connected to the monetary transaction system;

performing one or more validation checks on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber;

sending subscriber data to the at least one entity for identification of the unbanked subscriber, wherein the entity comprises a third party verification system;

receiving results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1318 of 1360

submitting one or more of the unbanked subscriber's account details to a third party account processor;

receiving an indication from the third party account processor that third party account processor created a third party stored value account for the subscriber;

maintaining a link between the subscriber data and the third party stored value account;

adding the third party stored value account to the unbanked subscriber's mobile wallet; and

notifying the unbanked subscriber of the addition of the third party stored value account over at least one other of the plurality of channels connected to the monetary transaction system.

7. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to deposit funds at an agent branch through a mobile wallet, including the following steps:

receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system , the agent communication indicating that the unbanked subscriber desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account;

validating the status of the unbanked subscriber's mobile wallet account;

determining if the agent branch is authorized to receive deposited money;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1319 of 1360

performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account;

crediting the unbanked subscriber's mobile wallet account with the specified amount of funds;

returning a notification to the agent branch confirming the deposit; and

notifying the subscriber that the specified amount of funds was deposited in the unbanked subscriber's mobile wallet account over at least one of the plurality of channels connected to the monetary transaction system.

8. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to withdraw funds at an agent branch using a mobile wallet, including the following steps:

receiving a communication from the unbanked subscriber over one of a plurality of channels connected to the monetary transaction system, the communication indicating that the unbanked subscriber desires to withdraw a specified amount of funds from the unbanked subscriber's mobile wallet account at the agent branch;

validating the status of the unbanked subscriber's mobile wallet account;

determining if the balance of the unbanked subscriber's mobile wallet account is sufficient to accommodate the requested withdrawal for the specified amount of funds;

performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1320 of 1360

returning a secure, perishable withdrawal code to the subscriber over at least one of the plurality of channels connected to the monetary transaction system;

receiving subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system , the agent branch communication indicating that the withdrawal code has been presented to the agent branch;

debiting the unbanked subscriber's mobile wallet account by the specified amount of funds;

returning a notification to the agent branch confirming the withdrawal; and

notifying the subscriber that the specified amount of funds was withdrawn from the unbanked subscriber's mobile wallet account over at least one of the channels connected to the monetary transaction system.

9. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to pay a bill from a mobile wallet, including the following steps:

receiving a subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to pay a bill for a specified amount using a specified payment method from the unbanked subscriber's mobile wallet;

validating the status of the selected payment method;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1321 of 1360

performing one or more of a limit check and a velocity check on the selected payment method;

debiting the specified payment method by the specified amount of funds;

processing the bill payment via at least one of a direct biller connection and a bill pay aggregator; and

notifying the unbanked subscriber that the bill was paid over at least one of the plurality of channels connected to the monetary transaction system.

10. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to buy airtime on a prepaid mobile account from a mobile wallet, including the following steps:

receiving subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to top up a prepaid mobile account by a specified amount using a specified payment method from the unbanked subscriber's mobile wallet;

validating the status of the selected payment method;

performing at least one of a limit check and a velocity check on the selected payment method;

debiting the specified payment method by the specified amount of funds;

processing the mobile top-up via at least one of a billing system integrator and an aggregator; and

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

notifying the subscriber that the prepaid mobile account was topped up over at least one of the plurality of channels connected to the monetary transaction system.

11. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to transfer money between mobile wallets, including the following steps:

receiving subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to transfer a specified amount of funds to specified recipient using a specified payment method from the subscriber's mobile wallet;

validating the status of the selected payment method;

performing at least one of a limit check and a velocity check on the selected payment method;

validating the status of the specified recipient to ensure the specified recipient has a valid mobile wallet account;

debiting the specified payment method by the specified amount of funds;

transferring the specified amount of funds to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system;

notifying the unbanked subscriber that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1323 of 1360

12. The monetary transaction system of claim 11, wherein validating the status of the specified recipient comprises performing a check on the specified recipient to comply with the office of foreign assets control.

13. The monetary transaction system of claim 11, wherein the money is transferred internationally between the mobile wallets.

14. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to make a purchase from a mobile wallet, including the following steps:

receiving a communication from a subscriber over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to purchase an item for a specified amount of funds using a specified payment method from the unbanked subscriber's mobile wallet;

returning a secure, perishable purchase code to the unbanked subscriber over at least one of the plurality of channels connected to the monetary transaction system;

receiving subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system, the agent branch communication indicating that the purchase code has been presented to an agent;

validating the status of the specified payment method;

determining if the specified payment method can accommodate a purchase for the specified amount;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

performing at least one of a limit check and a velocity check on the selected payment method;

debiting the specified payment method by the specified amount of funds;

returning a notification to the agent branch authorizing the purchase; and

sending a receipt to the unbanked subscriber over at least one of the plurality of channels connected to the monetary transaction system.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1325 of 1360

15. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising:

a mobile device configured to run a monetary transaction system application;

a monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;

a monetary transaction system processor that performs the one or more transactions specified by the subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile; and

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system.

16. The monetary transaction system of claim 15, wherein the monetary transaction system is implemented to add a bank or credit union account to a mobile wallet, including the following steps:

receiving subscriber data, including bank or credit union account details, over at least one of a plurality of channels connected to the monetary transaction system;

performing one or more validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber;

sending subscriber data to a third party verification system for identification of the subscriber;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1326 of 1360

receiving results from the third party system indicating that the subscriber data appropriately identifies the subscriber;

submitting bank or credit union account details for validation by the transaction processor;

receiving an indication that the bank or credit union account details correspond to a valid bank or credit union account;

maintaining a link between the subscriber data and the bank or credit union account; and

notifying the subscriber of the bank or credit union account validation over at least one of the plurality of channels connected to the monetary transaction system.

17. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to add a debit or credit card account to a mobile wallet, including the following steps:

receiving subscriber data, including a debit or credit card account number, over one of a plurality of channels connected to the monetary transaction system;

performing one or more validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber;

sending subscriber data to a third party verification system for identification of the subscriber;

receiving results from the third party system indicating that the subscriber data appropriately identifies the subscriber;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1327 of 1360

securely storing the debit or credit card account number for access by the mobile wallet;

adding the debit or credit card account number to the subscriber's mobile wallet; and

notifying the subscriber of the addition of the debit or credit card account number over at least one of the plurality of channels connected to the monetary transaction system.

18. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to deposit funds into a bank or credit union account using a mobile wallet, including the following steps:

receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system, the agent communication indicating that a subscriber desires to deposit a specified amount of funds into a bank or credit union account;

validating the status of the bank or credit union account;

determining if the agent branch is authorized to deposit money;

performing one or more of a limit check and a velocity check on the bank or credit union account;

crediting the bank or credit union account with the specified amount of funds;

returning a notification to the agent branch confirming the deposit; and

notifying the subscriber that the specified amount of funds was deposited in the bank or credit union account over at least one of the plurality of channels connected to the monetary transaction system.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1328 of 1360

19. The monetary transaction system of claim 1, wherein the monetary transaction system is implemented to withdraw funds from a bank or credit union account through a mobile wallet, including the following steps:

receiving communication from a subscriber over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that a subscriber desires to withdraw a specified amount of funds from a bank or credit union account;

validating the status of the bank or credit union account;

determining if the balance of the bank or credit union account is sufficient to accommodate the requested withdrawal for the specified amount of funds;

performing at least one of a limit check and a velocity check on the bank or credit union account;

returning a secure, perishable withdrawal code to the subscriber over at least one of the plurality of channels connected to the monetary transaction system;

receiving subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system, the agent branch communication indicating that the withdrawal code has been presented to an agent;

debiting the bank or credit union account by the specified amount of funds;

returning a notification to the agent branch confirming the withdrawal; and

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1329 of 1360

notifying the subscriber that the specified amount of funds were withdrawn from the bank or credit union account over at least one of the plurality of channels connected to the monetary transaction system.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1330 of 1360

20. A monetary transaction system, comprising:

a mobile wallet application configured to perform one or more of the following: process incoming and outgoing transactions, authenticate transaction system subscribers, manage subscriber profiles, and manage interactions between monetary transaction system components;

a monetary transaction processor configured to perform one or more of the following: manage account balances for mobile wallet subscribers, manage mobile wallet agent accounts, process balance inquiries, account credits, account debits, and transaction roll-backs;

a mobile wallet rules engine that manages and applies rules and policies that are defined for transactions as the transactions are processed on the mobile wallet transaction system including rules that control at least one of the following: transaction fees, transaction limits, transaction velocity limits, commissions, mobile transaction system roles and permissions;

a mobile wallet integration module that manages interaction between the mobile wallet transaction system and one or more external transaction systems including at least one of a wireless service provider's billing platform and a program partner bank;

a mobile wallet database that stores mobile wallet transaction data used in mobile wallet transactions including one or more of the following: subscriber profiles, subscription data, transaction data, transaction logs, mobile wallet application configuration data and mobile wallet application runtime data; and

a mobile wallet wireless service that interfaces with the wireless service provider's network to allow communication between the mobile wallet application

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1331 of 1360

and other mobile wallet transaction system components via the wireless service provider's network.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1332 of 1360

ABSTRACT

Embodiments are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one scenario, the monetary transaction system includes a mobile device that runs a monetary transaction system application. The monetary transaction system also includes a subscriber that has a profile with the system. The subscriber indicates a transaction that is to be performed with the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber including communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile. The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity..

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

PayPal - Exhibit 1002
PayPal v. Fintiv - IPR2023-00744
Page 1333 of 1360

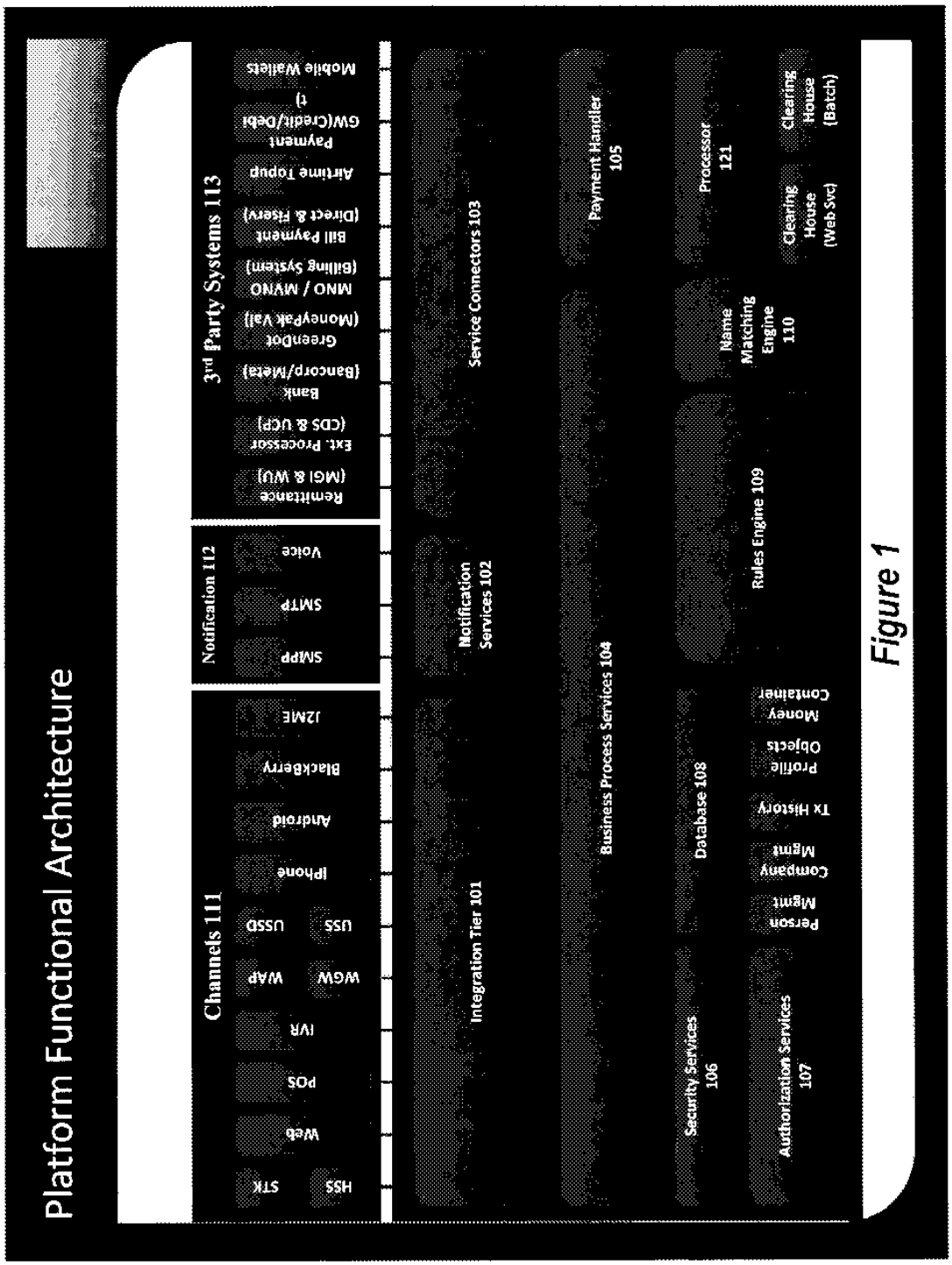

Platform Functional Architecture
Channels 111
HSS
STK
Web
POS
IVR
WGW
WAP
USS
USSD
iPhone
Android
BlackBerry
J2ME
Notification 112
SMPP
SMTP
Voice
3rd Party Systems 113
Remittance (MGI & WU)
Ext. Processor (CDS & UCP)
Bank (Bancorp/Meta)
GreenDot (MoneyPak Val)
MNO / MVNO (Billing System)
Bill Payment (Direct & Fiserv)
Airtime Topup
Payment GW(Credit/Debit)
Mobile Wallets
Integration Tier 101
Notification Services 102
Service Connectors 103
Business Process Services 104
Payment Handler 105
Security Services 106
Database 108
Rules Engine 109
Processor 121
Name Matching Engine 110
Authorization Services 107
Person Mgmt
Company Mgmt
Tx History
Profile Objects
Money Container
Clearing House (Web Svc)
Clearing House (Batch)
Figure 1

FIG. 1

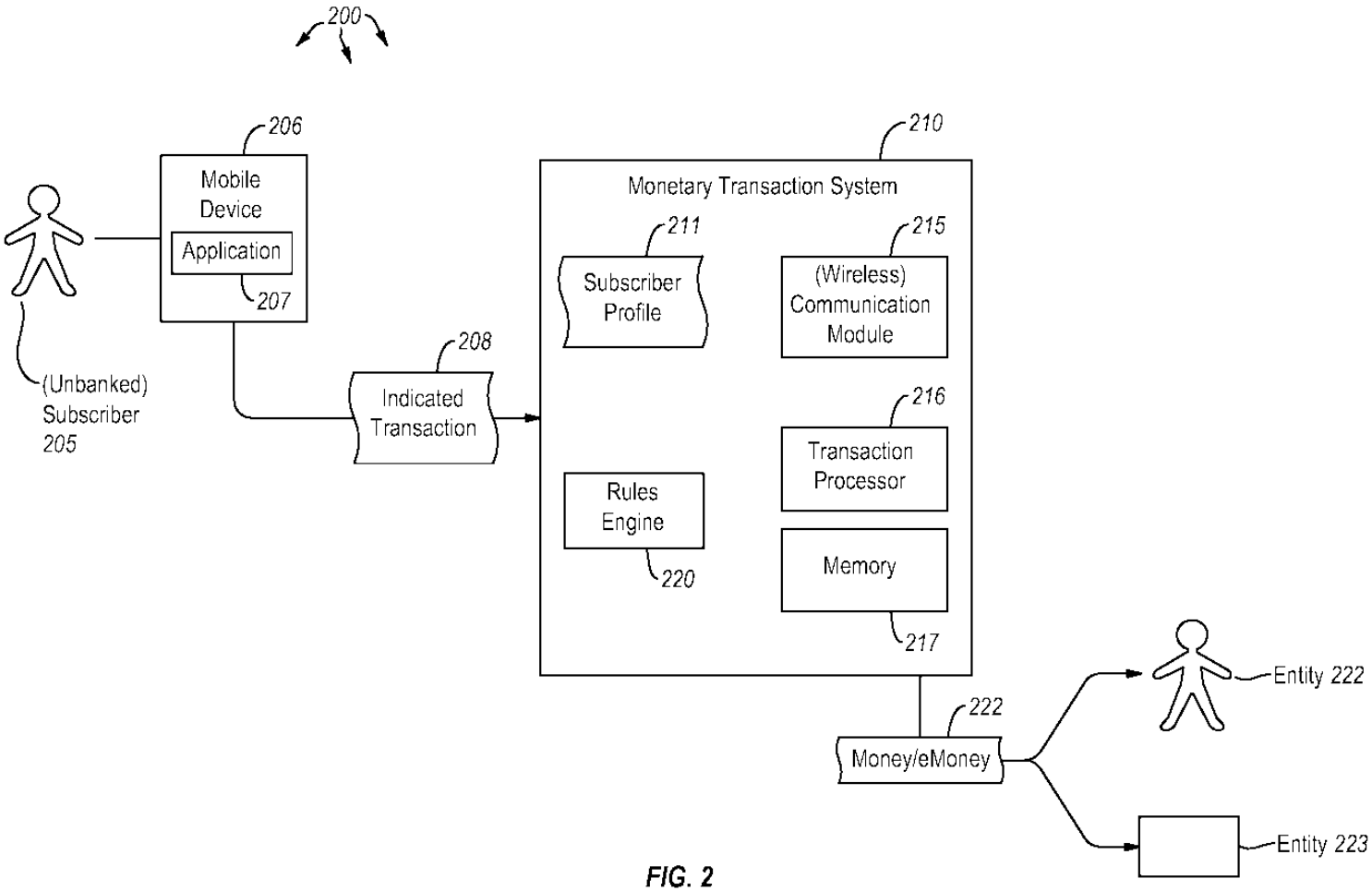
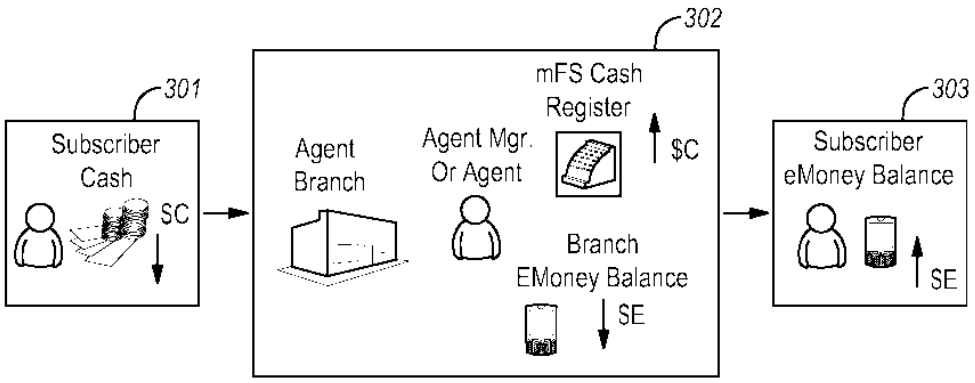

200
206
Mobile Device
Application
207
(Unbanked) Subscriber 205
208
Indicated Transaction
210
Monetary Transaction System
211
Subscriber Profile
215
(Wireless) Communication Module
216
Transaction Processor
Rules Engine
220
Memory
217
222
Money/eMoney
Entity 222
Entity 223

FIG. 2


301
Subscriber Cash
SC
302
Agent Branch
Agent Mgr. Or Agent
mFS Cash Register
$C
Branch EMoney Balance
SE
303
Subscriber eMoney Balance
SE

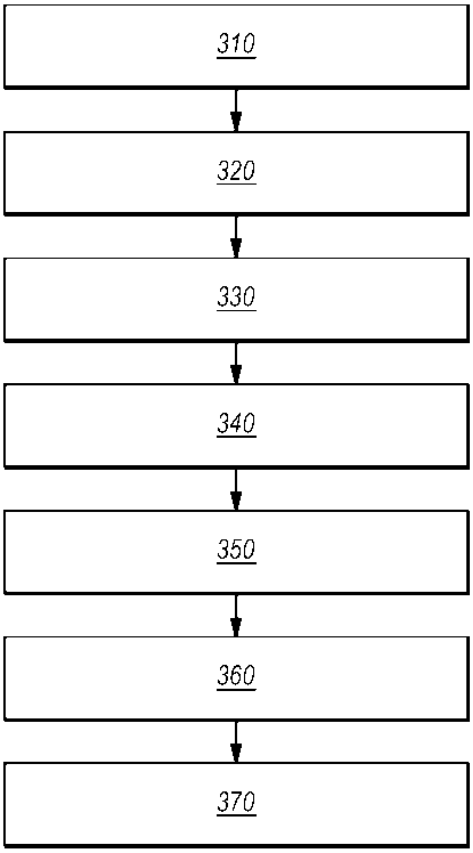
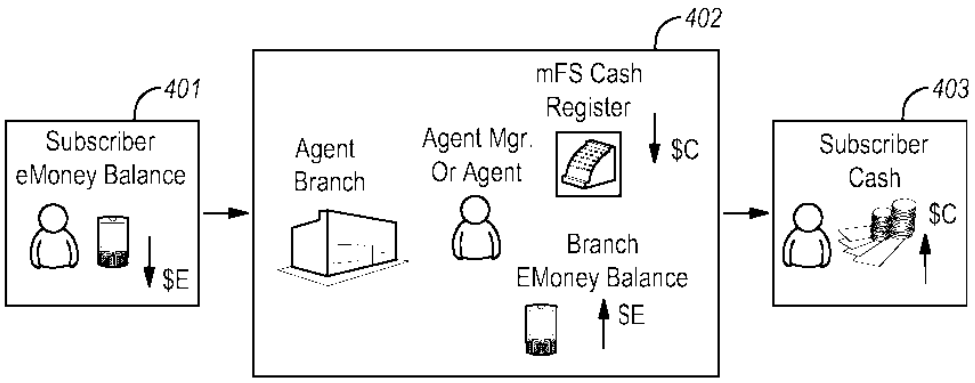

Subscriber Deposit
310
320
330
340
350
360
370

FIG. 3



Subscriber Withdrawal

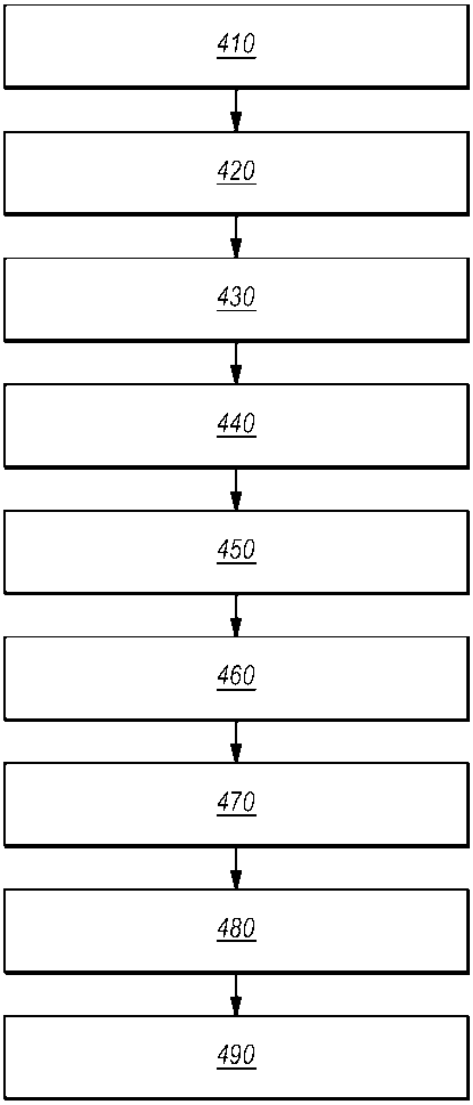
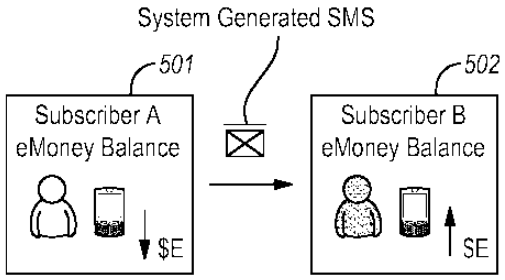
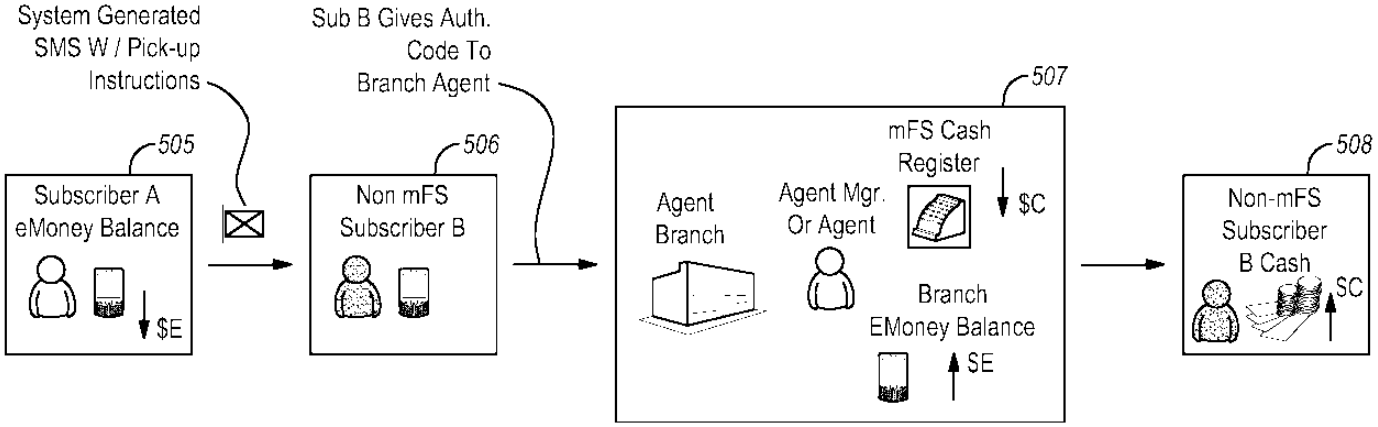


FIG. 4



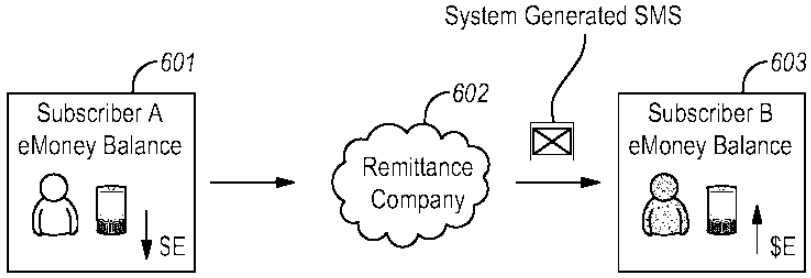
Subscriber -To- Subscriber
eMoney Transfer

FIG. 5A



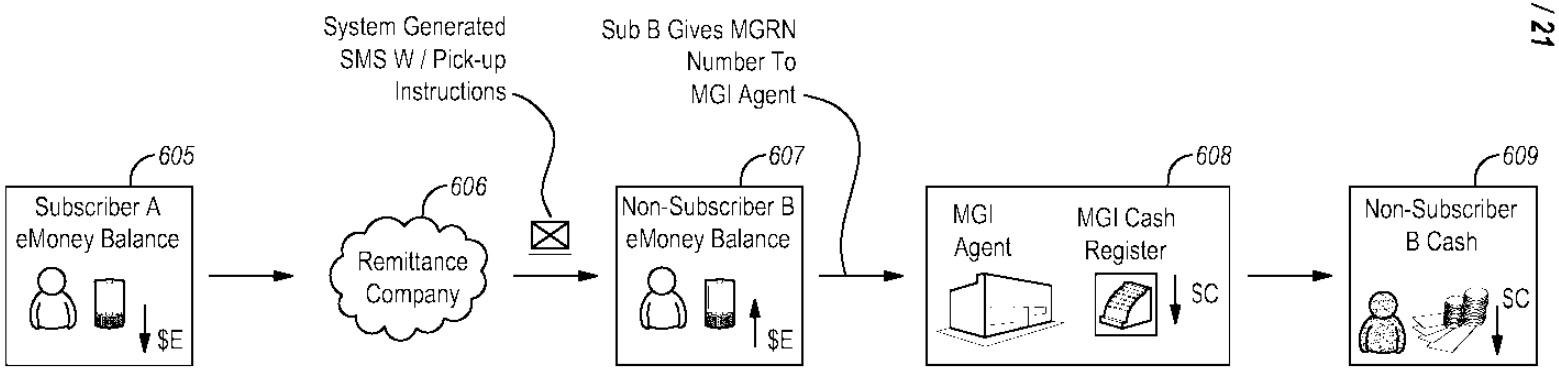
Subscriber -To- Non Subscriber
eMoney Transfer

FIG. 5B



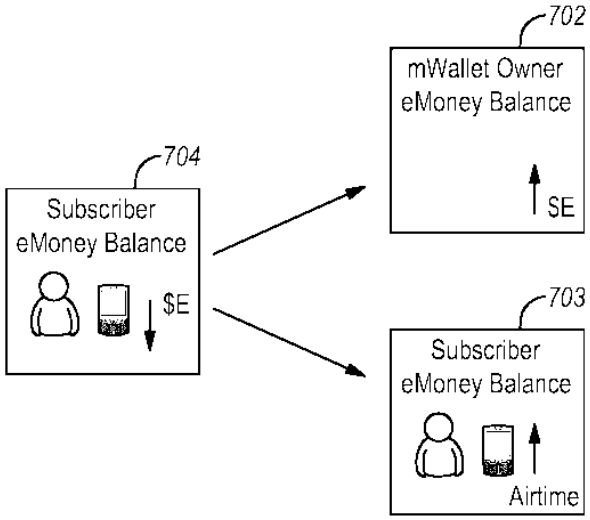
Subscriber -To- Subscriber
International eMoney Transfer

FIG. 6A



Subscriber -To- Non Subscriber
International eMoney Transfer

FIG. 6B



Subscriber Buys Airtime

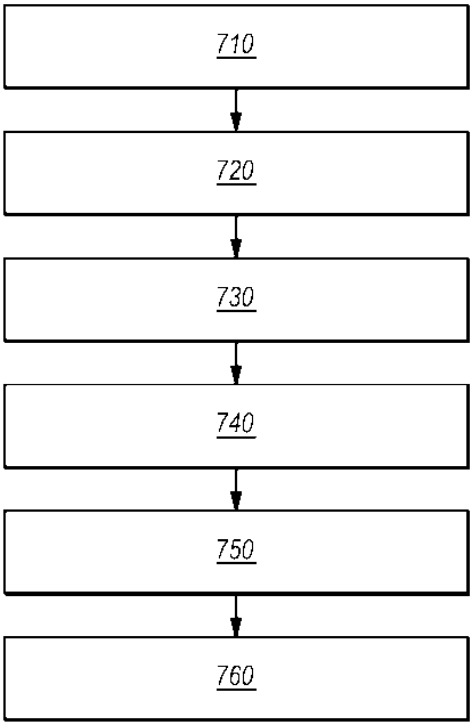
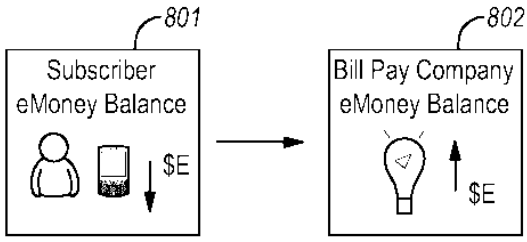


FIG. 7



Subscriber Pays Bill

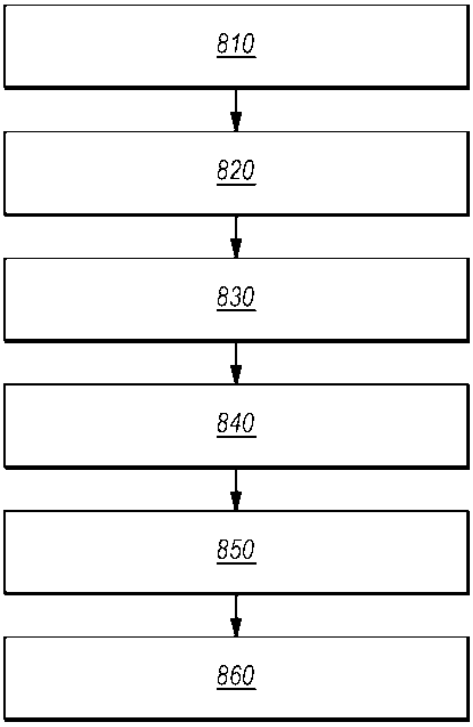
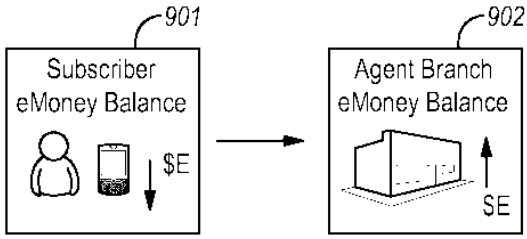


FIG. 8



Subscriber Makes Retail Purchase

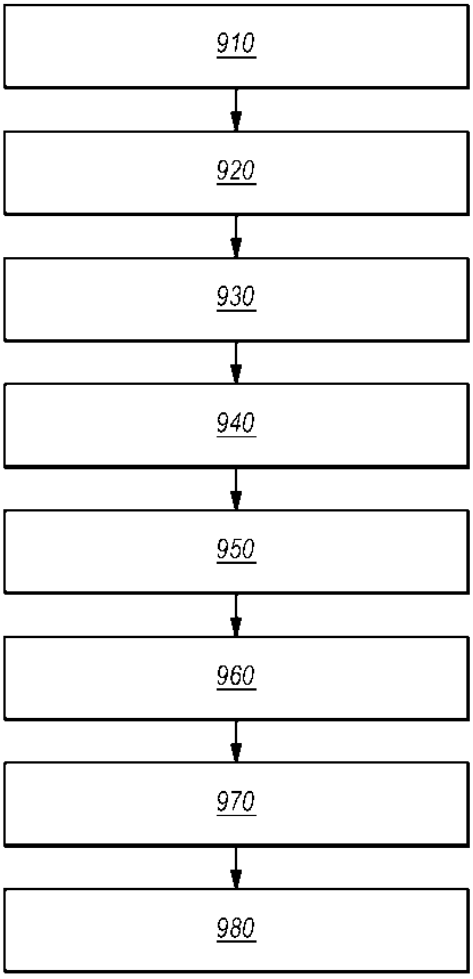
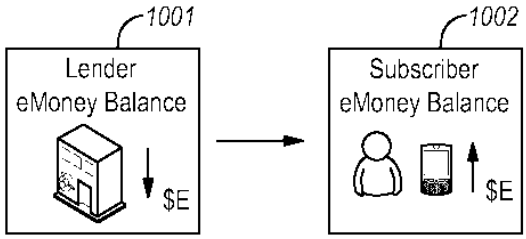
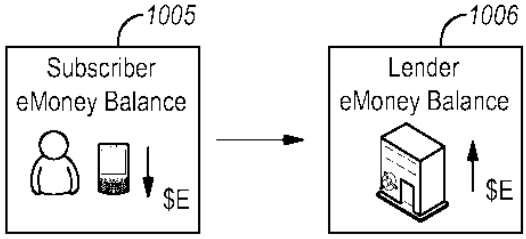


FIG. 9



Subscriber Requests Micro-Loan

FIG. 10A



Subscriber Repays Micro-Loan

FIG. 10B

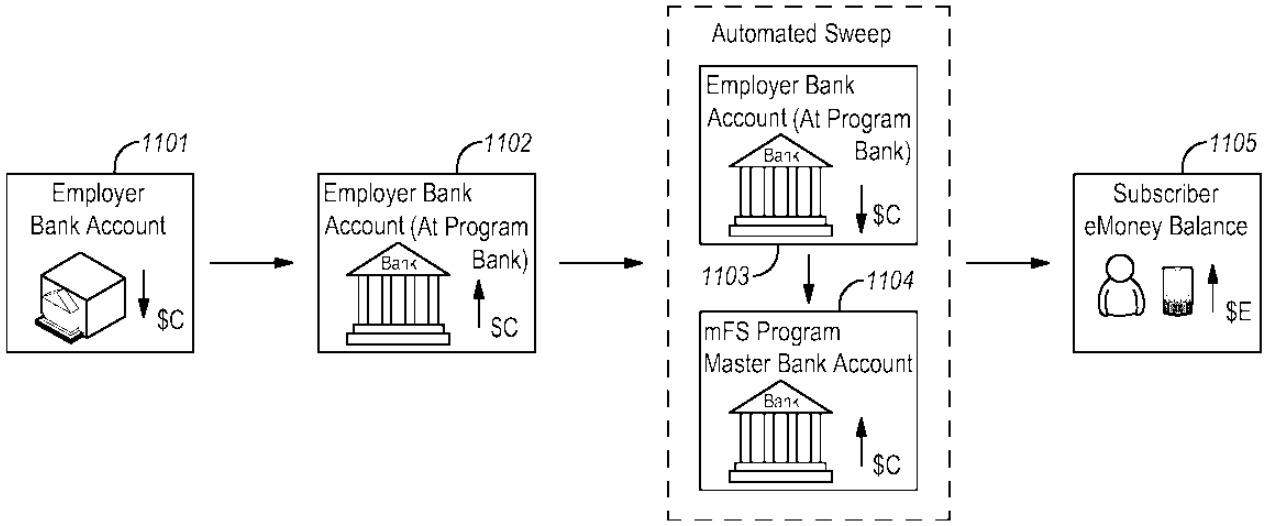
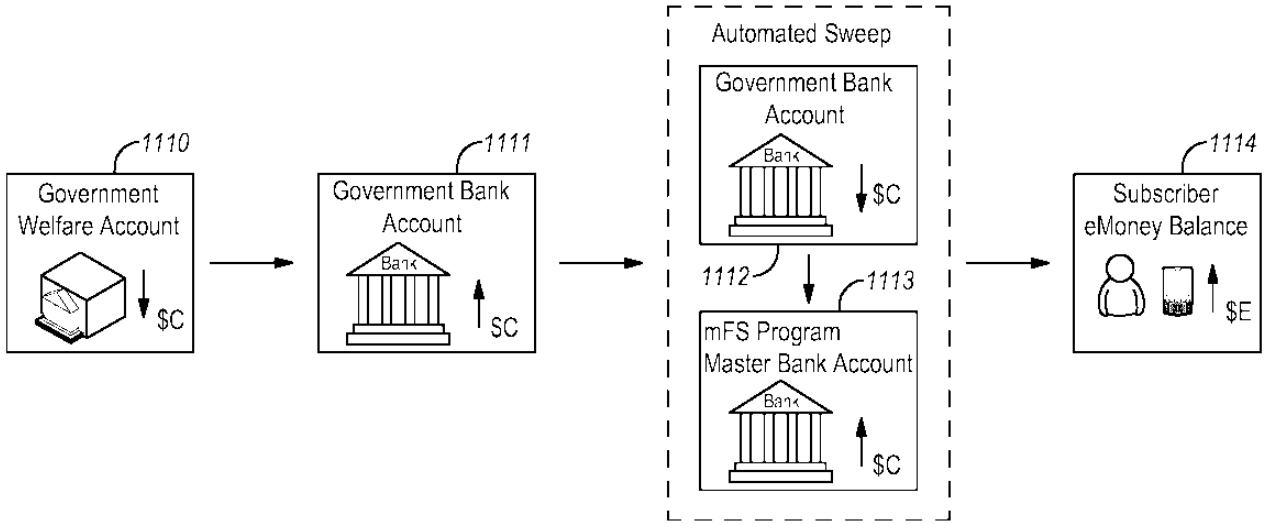
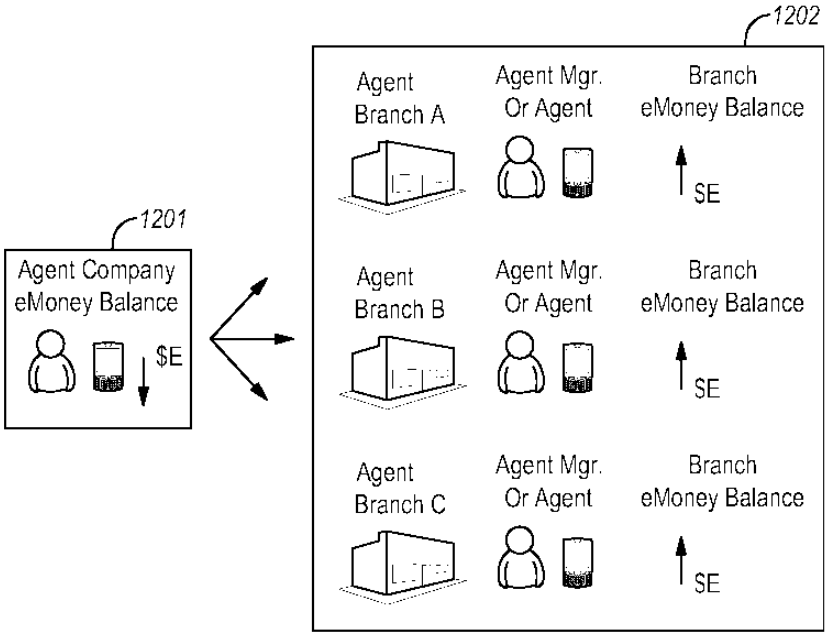

1101
Employer
Bank Account
$C
1102
Employer Bank
Account (At Program
Bank)
Bank
SC
Automated Sweep
Employer Bank
Account (At Program
Bank)
Bank
$C
1103
1104
mFS Program
Master Bank Account
Bank
$C
1105
Subscriber
eMoney Balance
$E
Subscriber Receives Direct Deposit

FIG. 11A



Subscriber Receives Government Welfare Payment

FIG. 11B



Agent Administrator Distributes eMoney

FIG. 12A

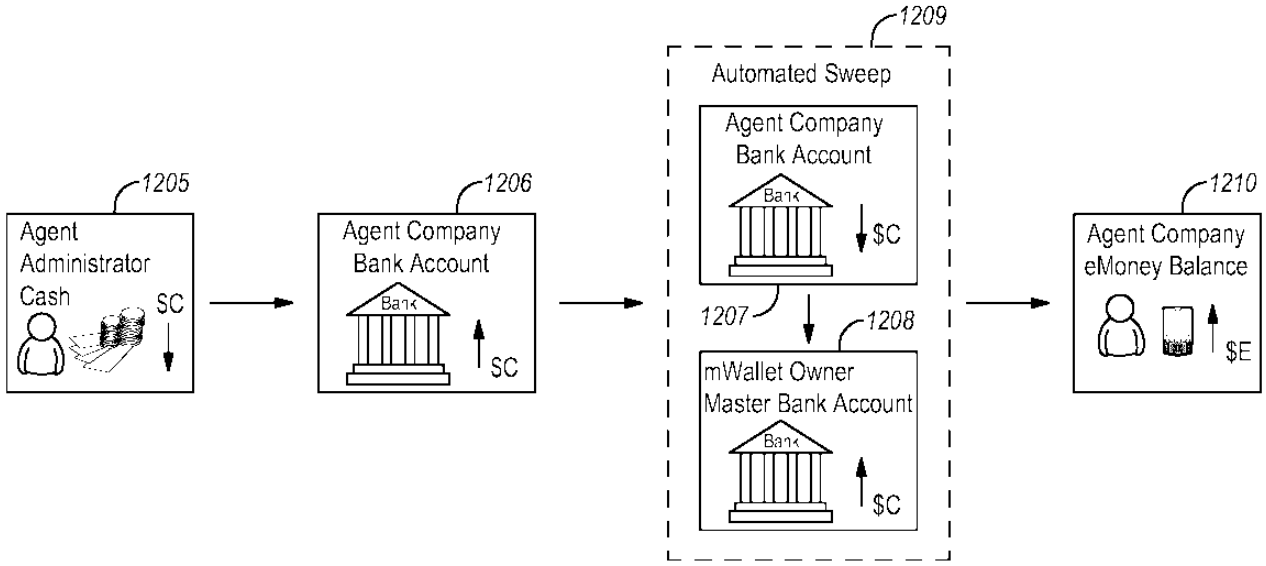

1209
Automated Sweep
Agent Company Bank Account
Bank
$C
1207
1208
mWallet Owner Master Bank Account
Bank
$C
1205
Agent Administrator Cash
SC
1206
Agent Company Bank Account
Bank
SC
1210
Agent Company eMoney Balance
$E
Agent Company Deposit

FIG. 12B

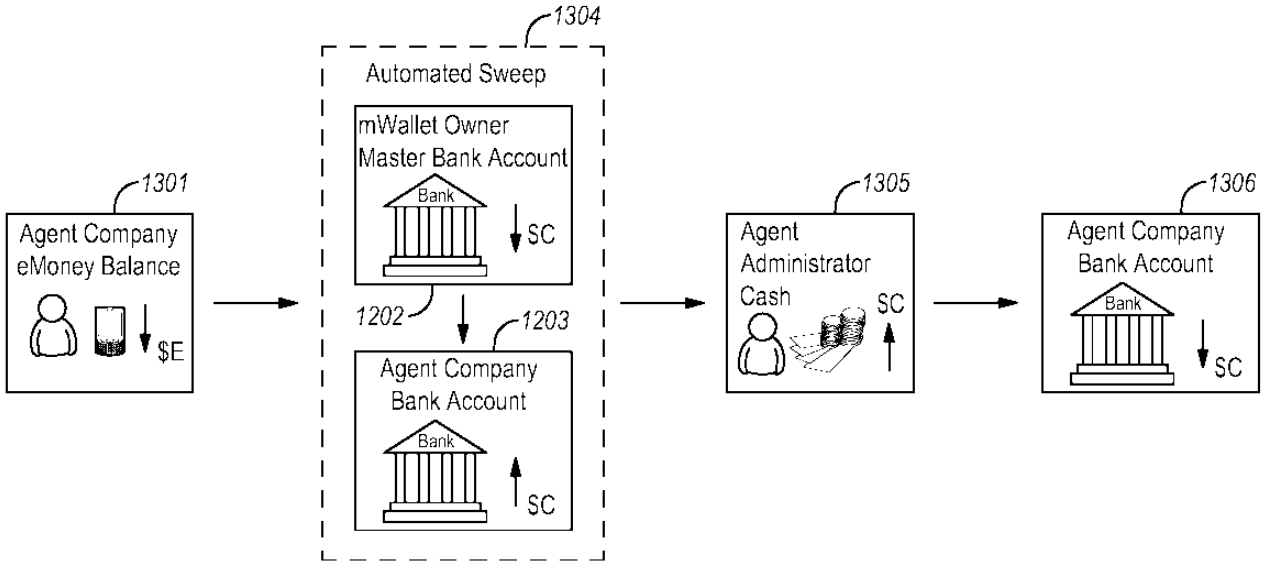
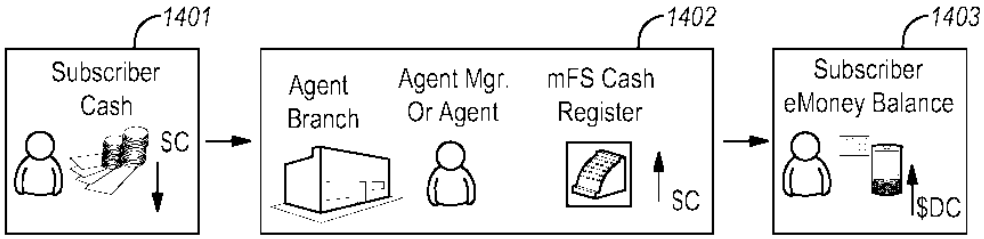

1304
Automated Sweep
mWallet Owner
Master Bank Account
Bank
SC
1301
Agent Company
eMoney Balance
$E
1202
1203
Agent Company
Bank Account
Bank
SC
1305
Agent
Administrator
Cash
SC
1306
Agent Company
Bank Account
Bank
SC
Agent Company Withdrawal

FIG. 13



Subscriber Deposit At Agent Branch

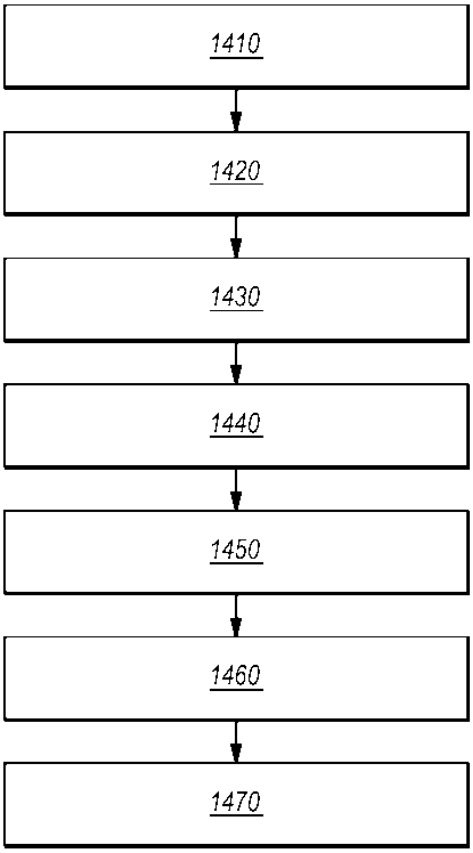
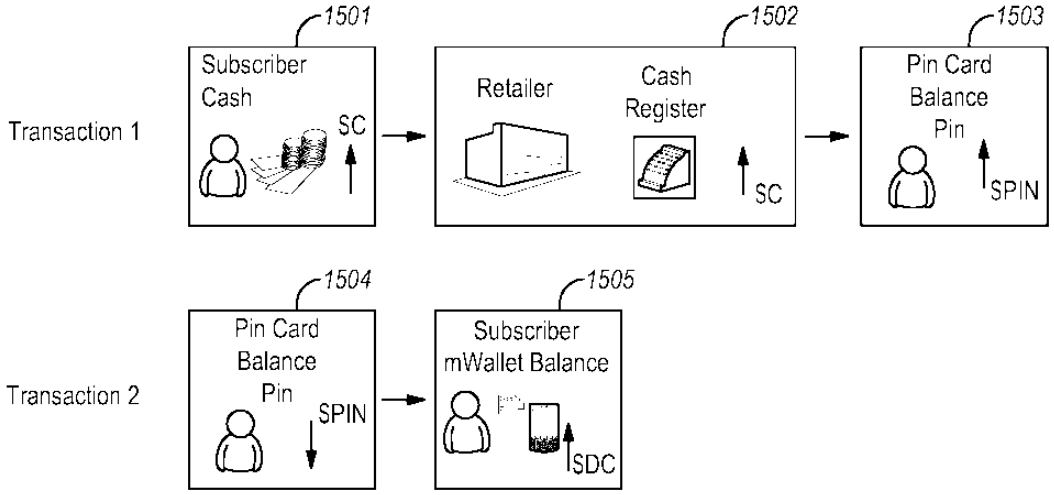
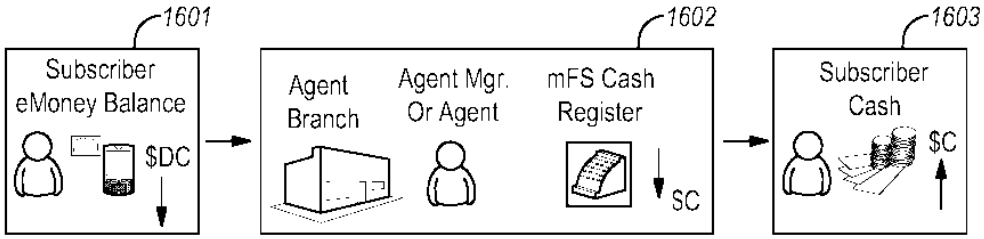


FIG. 14



Subscriber Deposit (Non-Agent)

FIG. 15



Subscriber Withdrawal (Agent)

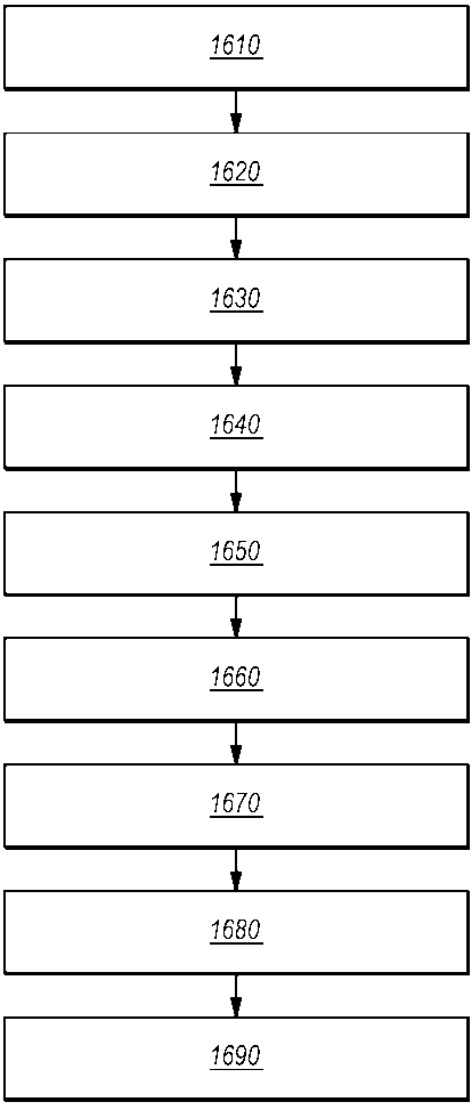
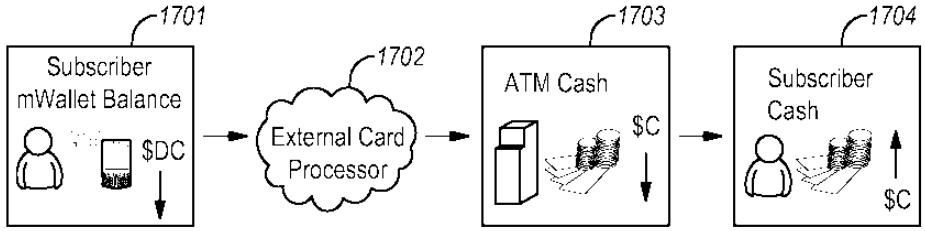
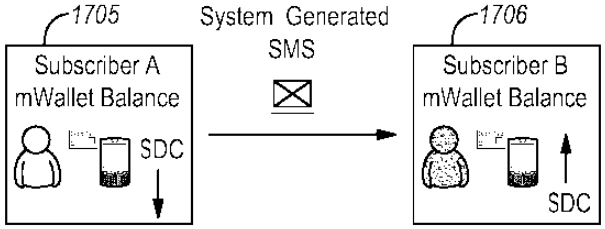


FIG. 16



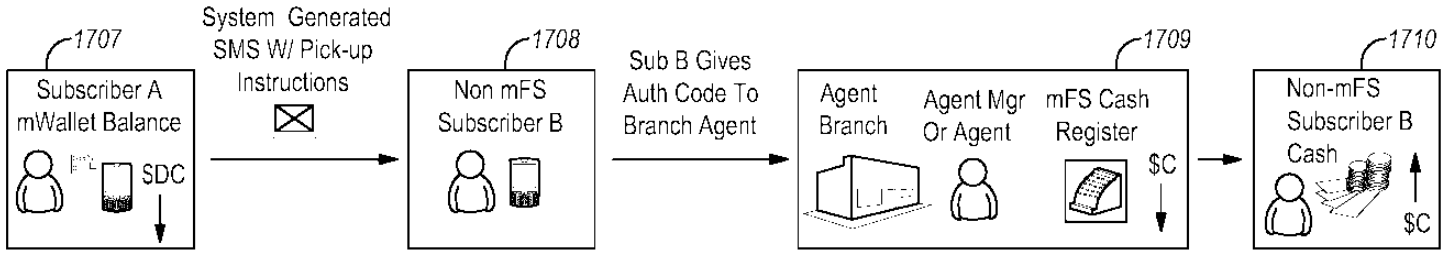
Subscriber Withdrawal (ATM)

FIG. 17A



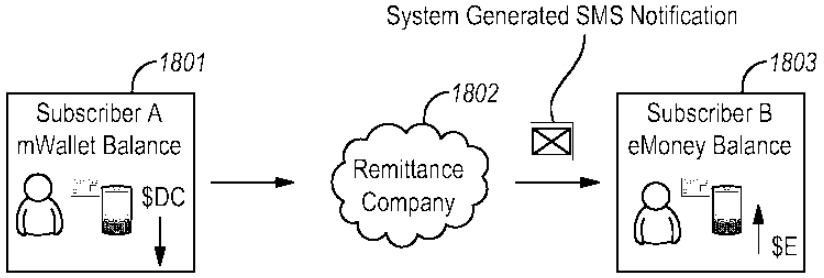
Subscriber To Subscriber Money Transfer

FIG. 17B



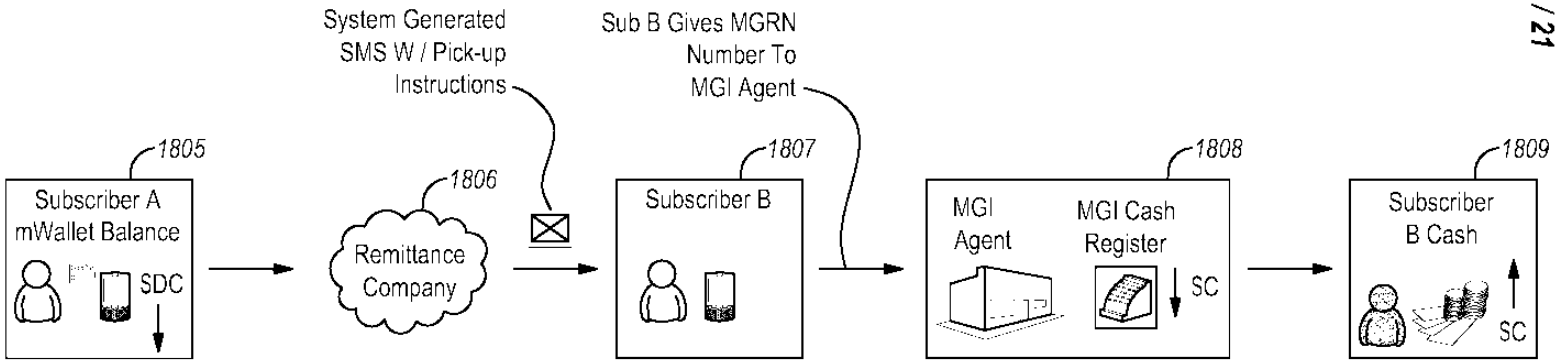
Subscriber To Non-Subscriber Money Transfer

FIG. 17C



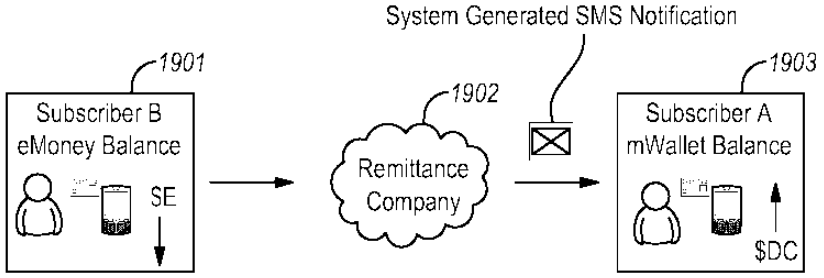
Subscriber -To- Subscriber
International Money Transfer

FIG. 18A



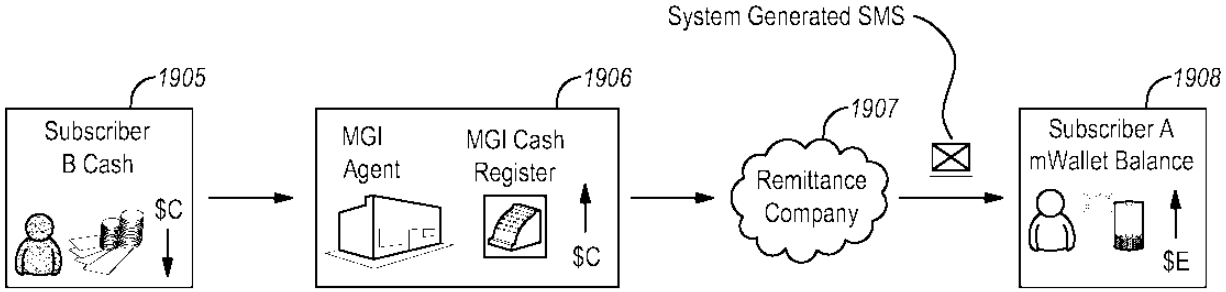
Subscriber -To- Non Subscriber
International Money Transfer

FIG. 18B



Subscriber -To- Subscriber
International Money Transfer

FIG. 19A



Non-Subscriber -To- Subscriber
International Money Transfer

FIG. 19B

Electronic Patent Application Fee Transmittal	
Application Number:	
Filing Date:	
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Filer:	GREGORY LUNT
Attorney Docket Number:	18756.8.1.1
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	1250

Electronic Acknowledgement Receipt	
EFS ID:	12897045
Application Number:	13484199
International Application Number:	
Confirmation Number:	5095
Title of Invention:	MONETARY TRANSACTION SYSTEM
First Named Inventor/Applicant Name:	Michael A. Liberty
Customer Number:	22913
Filer:	GREGORY LUNT/dee so
Filer Authorized By:	GREGORY LUNT
Attorney Docket Number:	18756.8.1.1
Receipt Date:	30-MAY-2012
Filing Date:	
Time Stamp:	20:10:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1250
RAM confirmation Number	13799
Deposit Account	233178
Authorized User	LUNT,GREGORY
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 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	Transmittal Letter	Transmittal-Utility-Application.pdf	156051 [illegible]	no	2
Warnings:					
Information:					
2	Application Data Sheet	Application-Data-Sheet.pdf	96839 [illegible]	no	4
Warnings:					
Information:					
3		18756-8-1-1 Utility-Application.pdf	71361 [illegible]	yes	77

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	59
Claims	60	76
Abstract	77	77

Warnings:					
Information:					
4	Drawings-other than black and white line drawings	18756-8-1-1 Drawings.pdf	2336290 [illegible]	no	21
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	32606 [illegible]	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	4206457		

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.

DocCode - SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 13484199 Document Date: 5/30/2012

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface using the Supplemental Content tab.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces using the Supplemental Content tab.

Form Revision Date: May 1, 2009