(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.

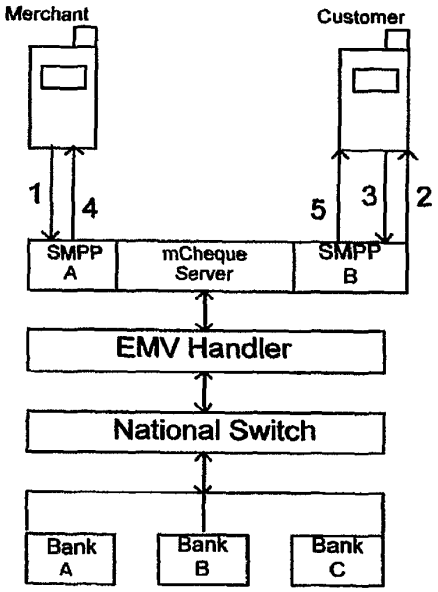
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, 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

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.

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).

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.

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.

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.

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.

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

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.

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.

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.

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.

- **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.

- **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.

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.

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.

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;

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.

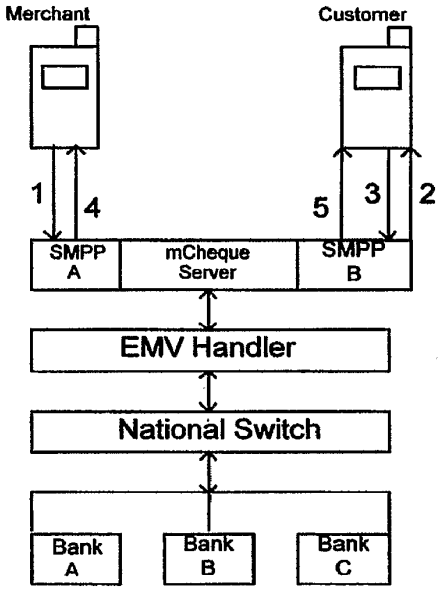

Merchant
Customer
1
4
5
3
2
SMPP A
mCheque Server
SMPP B
EMV Handler
National Switch
Bank A
Bank B
Bank C

Fig. 1.

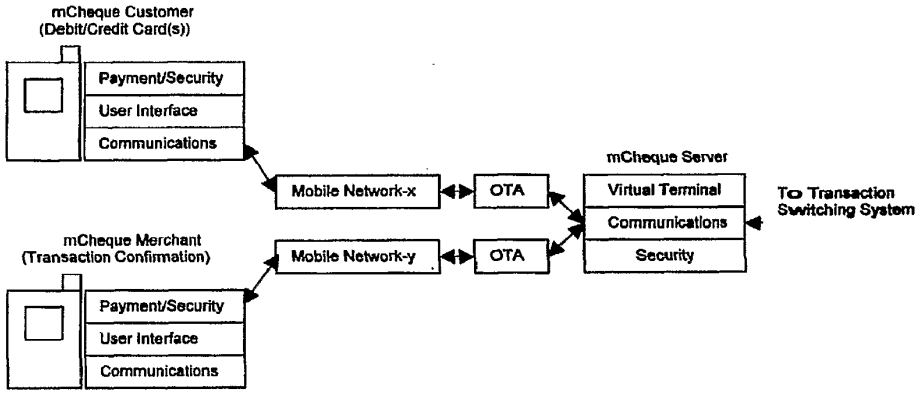

mCheque Customer
(Debit/Credit Card(s))
Payment/Security
User Interface
Communications
Mobile Network-x
OTA
mCheque Server
Virtual Terminal
Communications
Security
To Transaction
Switching System
mCheque Merchant
(Transaction Confirmation)
Mobile Network-y
OTA
Payment/Security
User Interface
Communications

Fig. 2

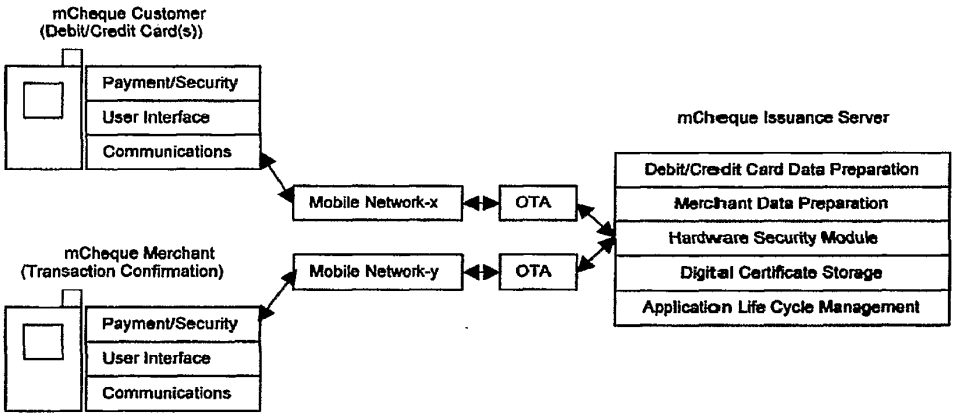

mCheque Customer
(Debit/Credit Card(s))
Payment/Security
User Interface
Communications
mCheque Merchant
(Transaction Confirmation)
Payment/Security
User Interface
Communications
Mobile Network-x
Mobile Network-y
OTA
OTA
mCheque Issuance Server
Debit/Credit Card Data Preparation
Merchant Data Preparation
Hardware Security Module
Digital Certificate Storage
Application Life Cycle Management

Fig. 3

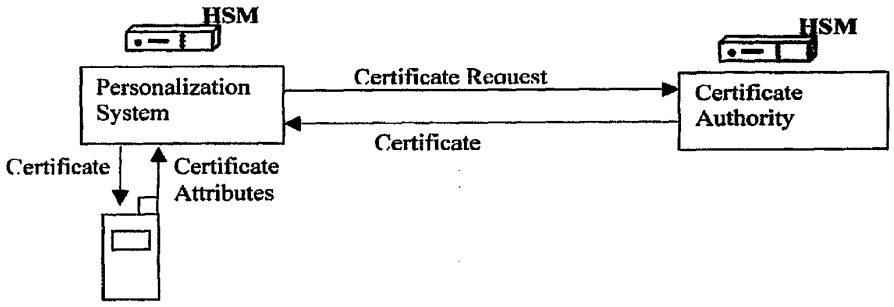

HSM
HSM
Personalization System
Certificate Request
Certificate Authority
Certificate
Certificate
Certificate Attributes

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).

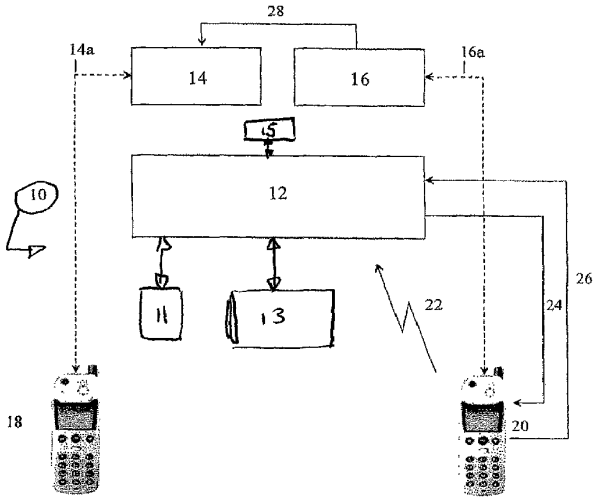
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, 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

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.

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.

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.

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.

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.

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 –

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:

```
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

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

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

one embodiment of the invention may be provided in combination with another embodiment of the invention.

5

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;

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.

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

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.

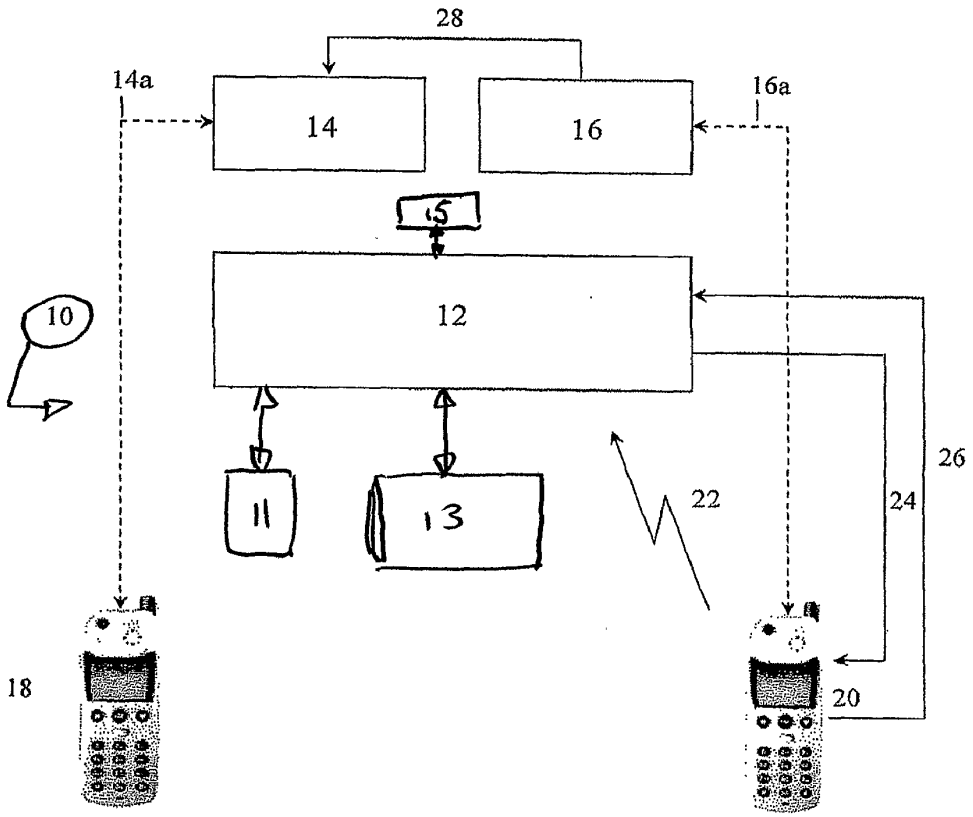


FIG. 1

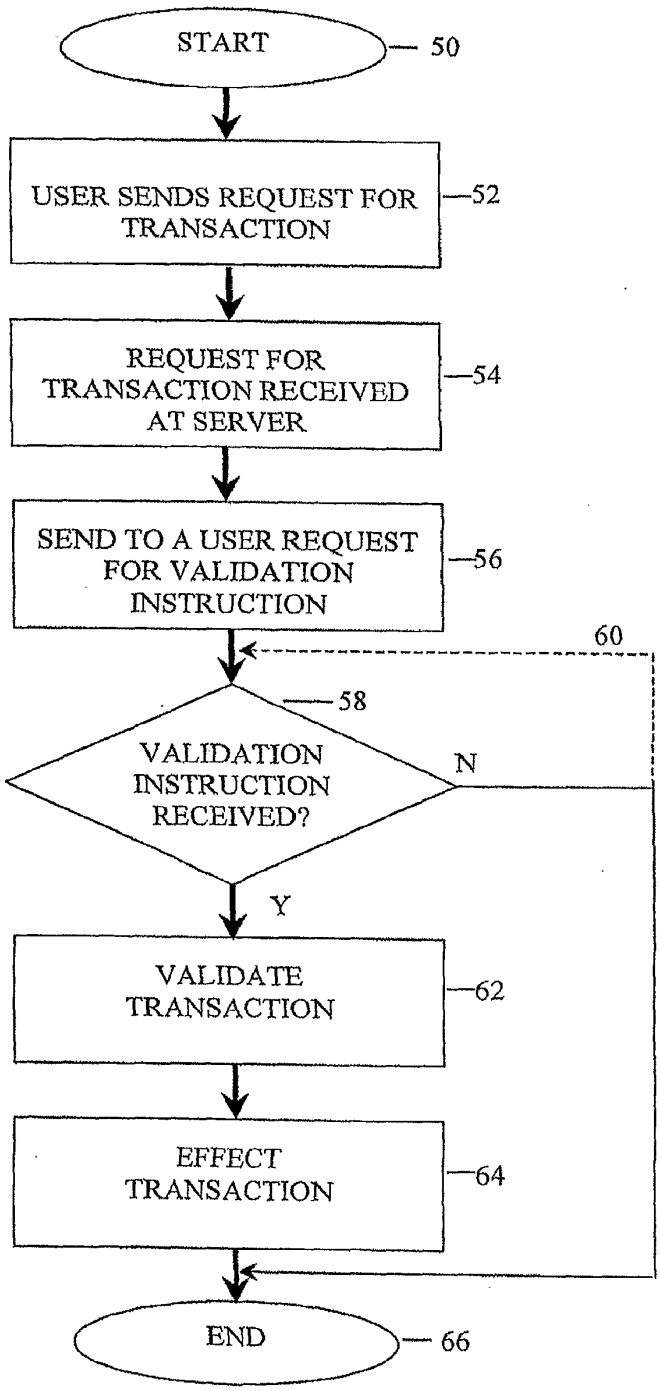

START
50
USER SENDS REQUEST FOR TRANSACTION
52
REQUEST FOR TRANSACTION RECEIVED AT SERVER
54
SEND TO A USER REQUEST FOR VALIDATION INSTRUCTION
56
60
58
VALIDATION INSTRUCTION RECEIVED?
N
Y
VALIDATE TRANSACTION
62
EFFECT TRANSACTION
64
END
66

FIG. 2

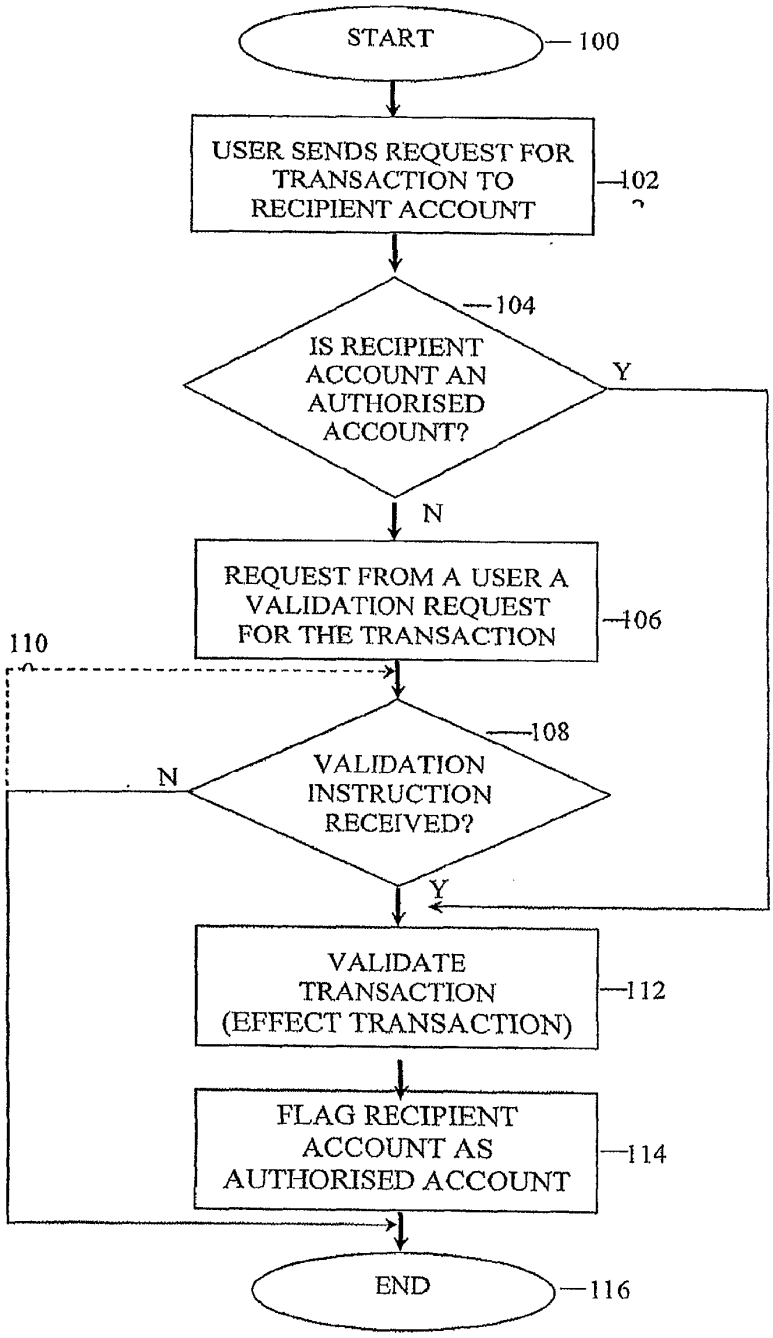

START
100
USER SENDS REQUEST FOR TRANSACTION TO RECIPIENT ACCOUNT
102
104
IS RECIPIENT ACCOUNT AN AUTHORISED ACCOUNT?
Y
N
REQUEST FROM A USER A VALIDATION REQUEST FOR THE TRANSACTION
106
110
108
VALIDATION INSTRUCTION RECEIVED?
N
Y
VALIDATE TRANSACTION (EFFECT TRANSACTION)
112
FLAG RECIPIENT ACCOUNT AS AUTHORISED ACCOUNT
114
END
116

FIG. 3

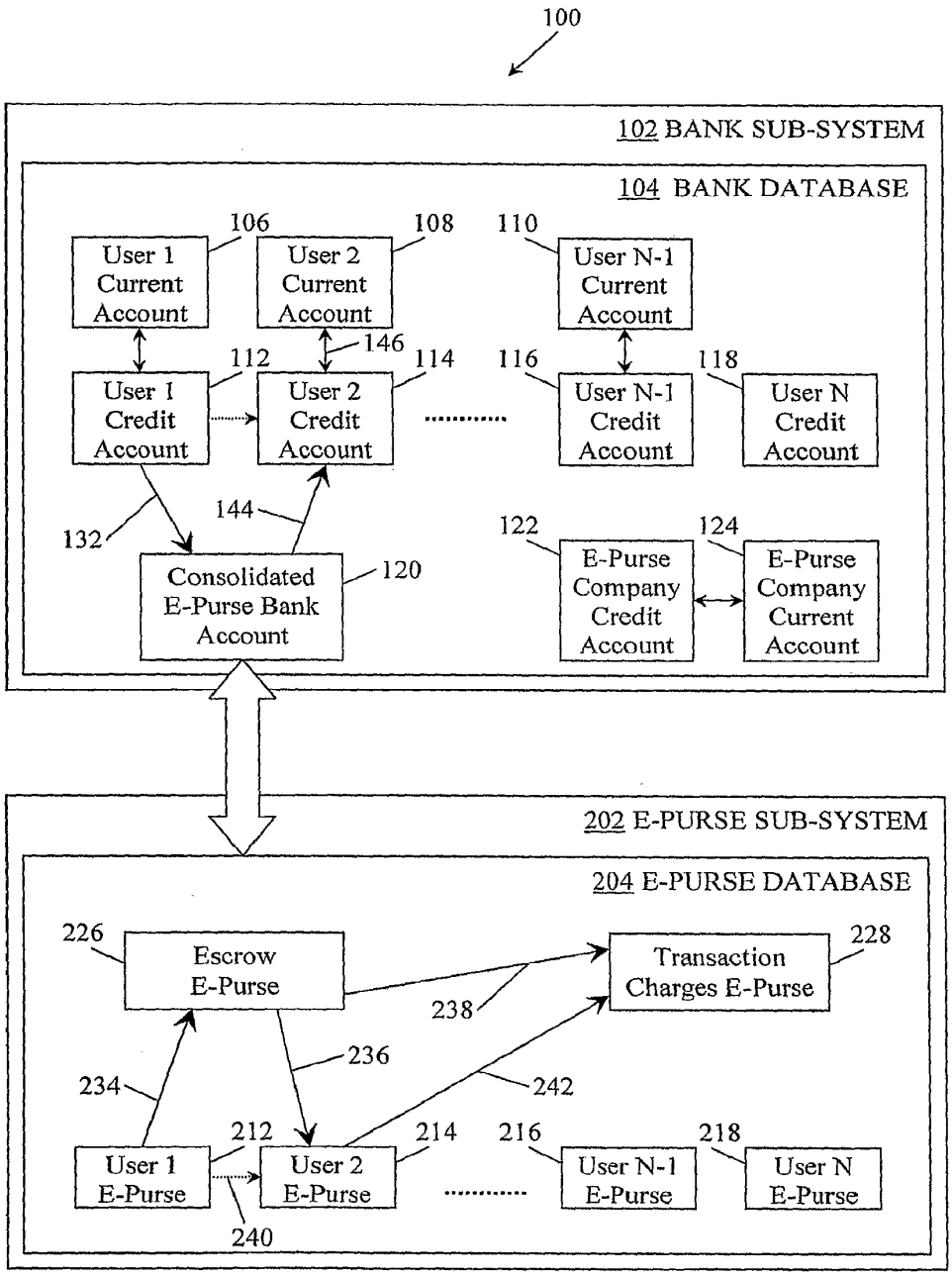

100
102 BANK SUB-SYSTEM
104 BANK DATABASE
106
108
110
User 1 Current Account
User 2 Current Account
User N-1 Current Account
146
112
114
116
118
User 1 Credit Account
User 2 Credit Account
User N-1 Credit Account
User N Credit Account
144
132
122
124
Consolidated E-Purse Bank Account
120
E-Purse Company 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
10 September 2007

Date of mailing of the international search report 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)

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

(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).

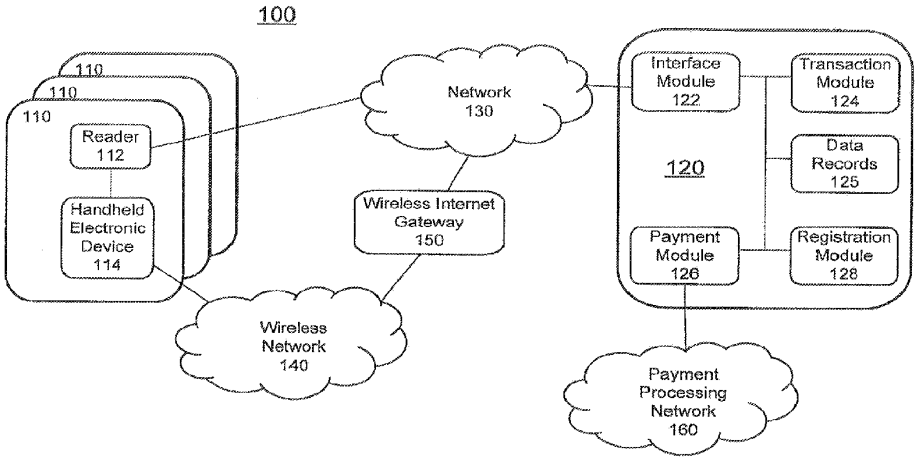
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, 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

TRANSACTIONS USING HANDHELD ELECTRONIC DEVICES BASED ON UNOBTRUSIVE PROVISIONING OF THE DEVICES

INVENTOR(S):
Claeton 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.

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.

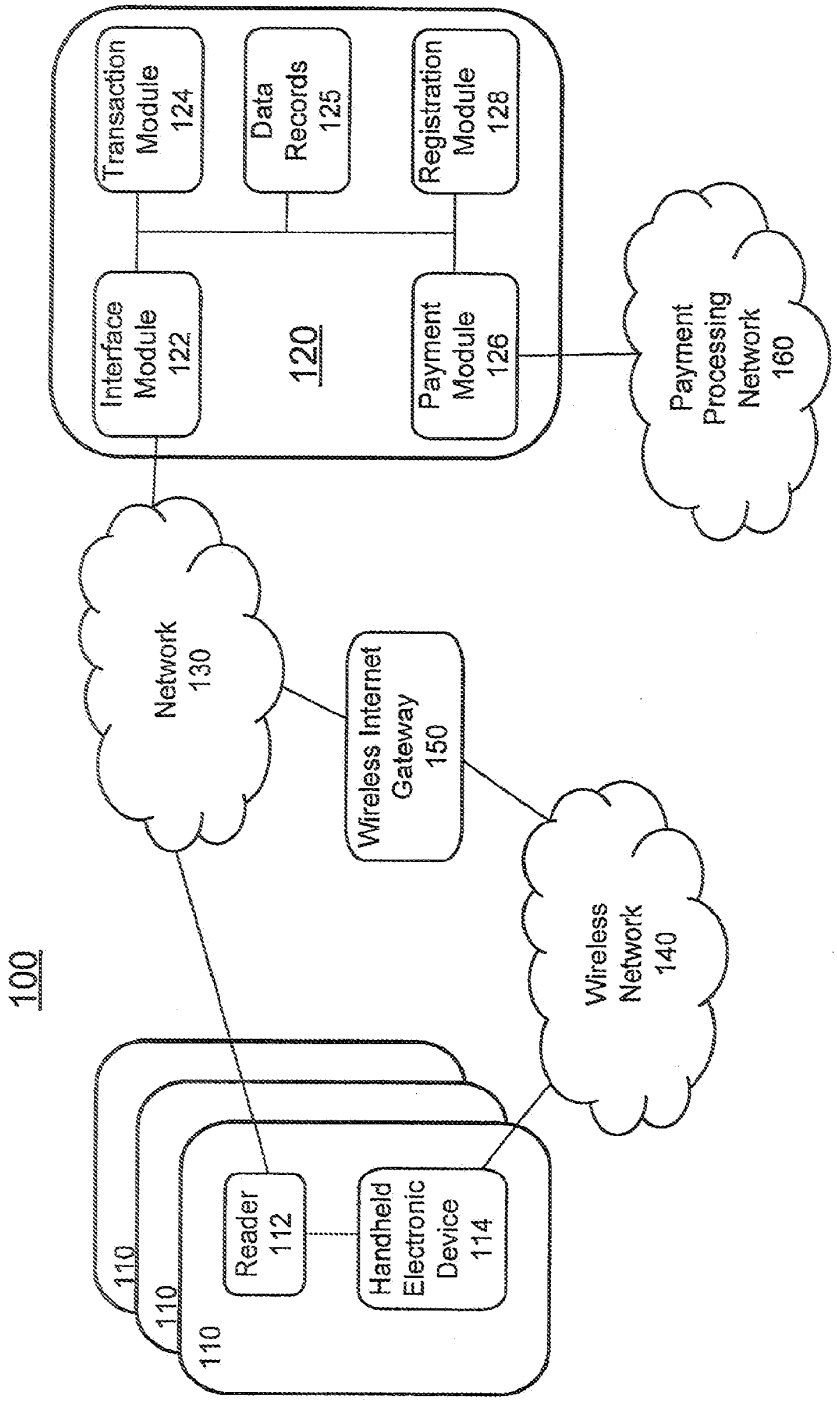

100
110
110
110
Reader 112
Handheld Electronic Device 114
Network 130
Wireless Internet Gateway 150
Wireless Network 140
120
Interface Module 122
Transaction Module 124
Data Records 125
Payment Module 126
Registration Module 128
Payment Processing Network 160

FIG. 1

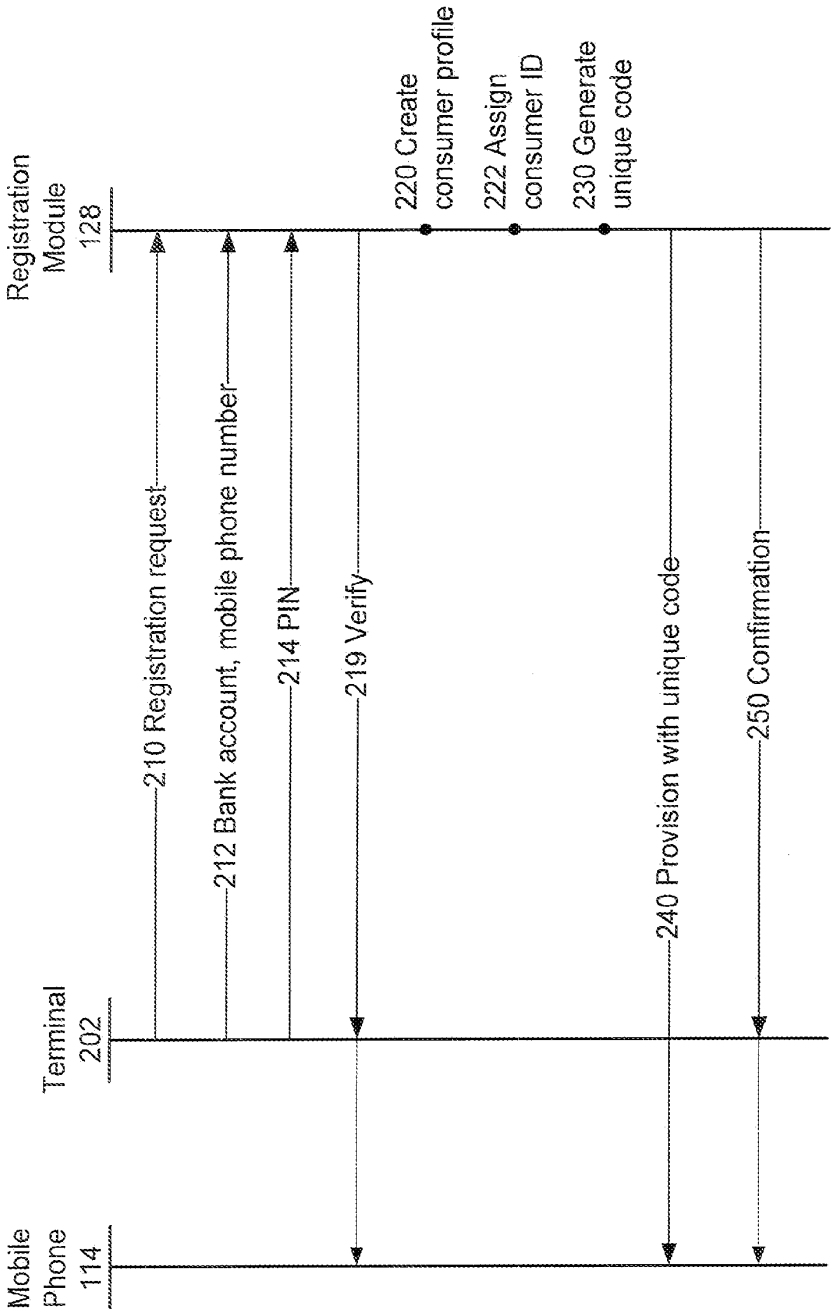

Mobile Phone 114
Terminal 202
Registration Module 128
210 Registration request
212 Bank account, mobile phone number
214 PIN
219 Verify
220 Create consumer profile
222 Assign consumer ID
230 Generate unique code
240 Provision with unique code
250 Confirmation

FIG. 2

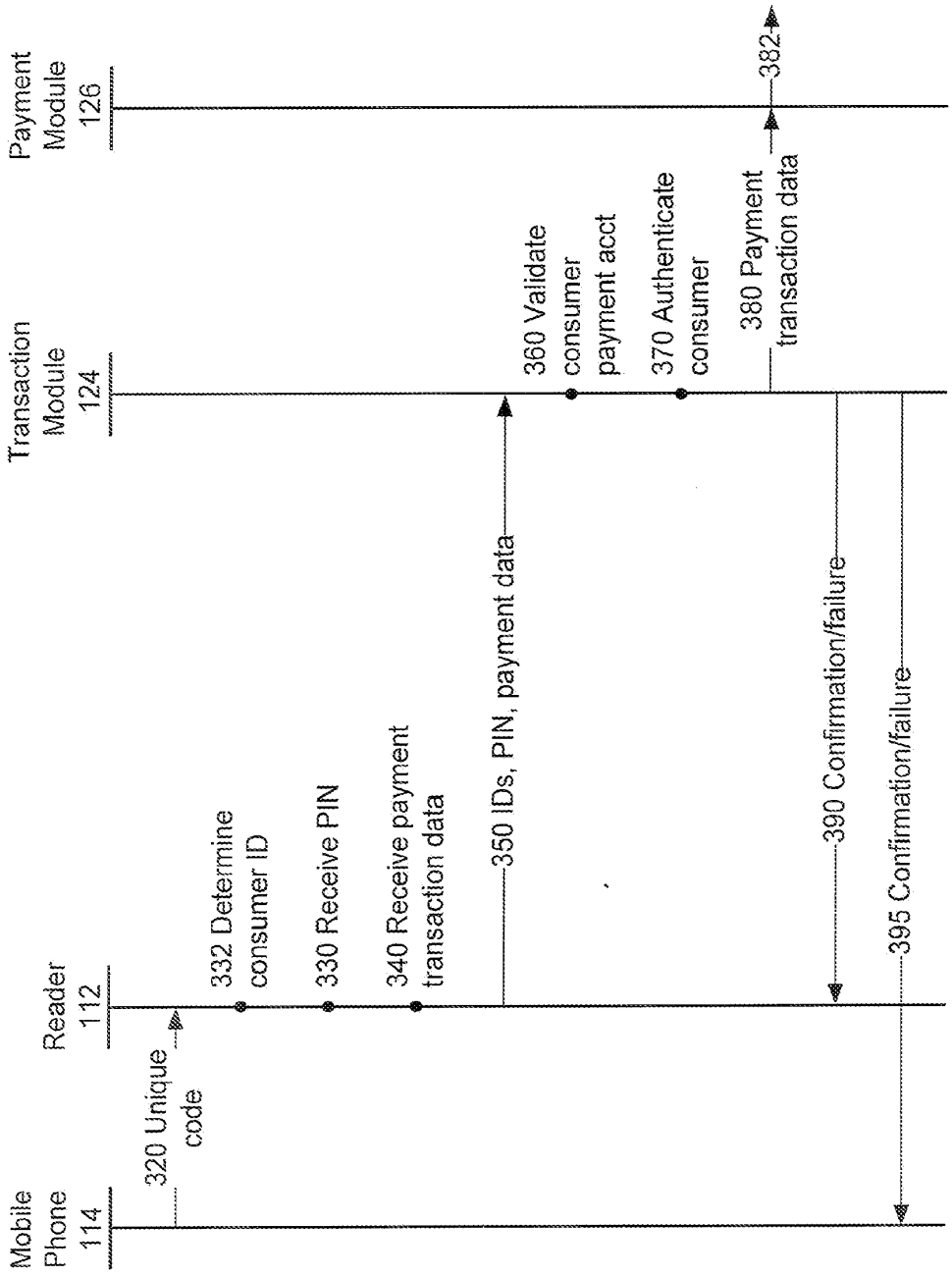

Mobile Phone 114
Reader 112
Transaction Module 124
Payment Module 126
320 Unique code
332 Determine consumer ID
330 Receive PIN
340 Receive payment transaction data
350 IDs, PIN, payment data
360 Validate consumer payment acct
370 Authenticate consumer
380 Payment transaction data
382
390 Confirmation/failure
395 Confirmation/failure

FIG. 3

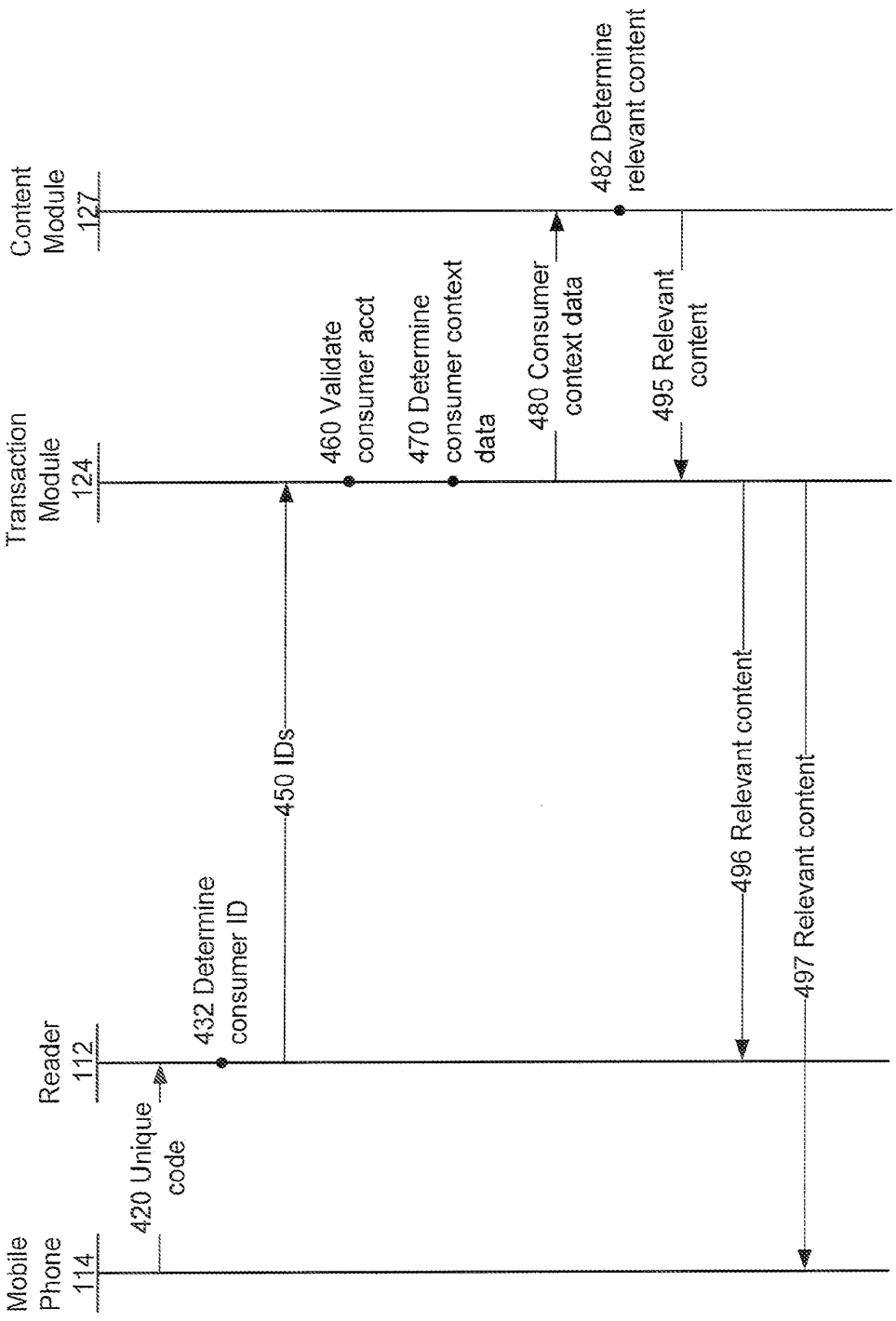

Mobile Phone 114
Reader 112
Transaction Module 124
Content Module 127
420 Unique code
432 Determine consumer ID
450 IDs
460 Validate consumer acct
470 Determine consumer context data
480 Consumer context data
482 Determine relevant content
495 Relevant content
496 Relevant content
497 Relevant content

FIG. 4

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 March 2012 (01.03.2012)

PCT

(10) International Publication Number
WO 2012/025824 A2

(51) International Patent Classification:
G06Q 20/00 (2012.01)

(21) International Application Number:
PCT/IB2011/002046

(22) International Filing Date:
15 June 2011 (15.06.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/355,077 15 June 2010 (15.06.2010) US

(72) Inventors; and
(71) Applicants : **YANG, David** [RU/RU]; 10-5, Bolshoy Kozlovshy Per., Moscow, 107078 (RU). **NALSKY, Max** [RU/RU]; 9 Varshavskoye Shosse, Building 1b, Moscow, 117105 (RU).

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

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

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title**: A CUSTOMER LOYALTY SYSTEM IN RETAIL CHAINS AND RESTAURANTS USING WEB SERVERS, MOBILE COMMUNICATION DEVICES, AND POINT-OF-SALE TERMINALS

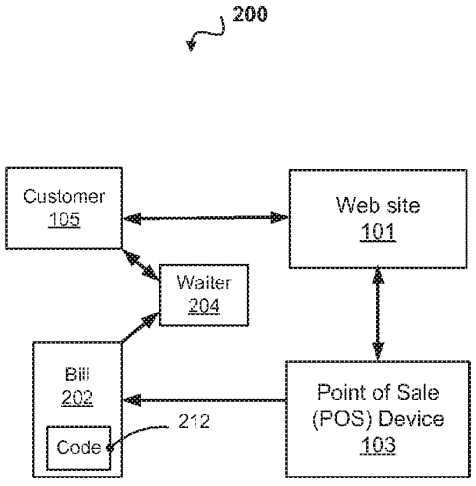


Fig. 2

(57) **Abstract**: A customer loyalty system assists to build and keep a customer base. The system gathers feedback from customers and enables tracking of goods and services. The customer loyalty system rids a customer of multiple loyalty cards by replacing them with one account. A customer account is associated with, for example, a customer cell phone number. A short¬ lived promotional code enables the customer to pay through a virtual wallet and to receive bonus points or rewards. A point of sale (POS) system generates a bill with a short-lived active promotional or activation code. The code identifies the currently ordered or selected goods or services at a particular establishment. The code expires after a few minutes or other relatively short time. Through, for example, a mobile Internet-enabled device, a customer redeems the short-lived code. Redemption may be done in a variety of ways, and may be done before or after payment, but before code expiration.

WO 2012/025824 A2

A CUSTOMER LOYALTY SYSTEM IN RETAIL CHAINS AND RESTAURANTS USING WEB SERVERS, MOBILE COMMUNICATION DEVICES, AND POINT-OF-SALE TERMINALS

CROSS-REFERENCE TO RELATED APPLICATIONS

For purposes of the USPTO extra-statutory requirements, the present application constitutes a continuation-in-part of United States Patent Application No. 61/355,077, titled A METHOD FOR BUILDING A CUSTOMER LOYALTY SYSTEM IN RETAIL CHAINS AND RESTAURANTS USING WEB SERVERS, MOBILE COMMUNICATION DEVICES, AND POINT-OF-SALE TERMINALS CONNECTED TO THE INTERNET, naming David Yan, Max Nalsky and Artyom Yukhin as inventors, filed 15 June 2010.

The United States Patent Office (USPTO) has published a notice effectively stating that the USPTO's computer programs require that patent applicants reference both a serial number and indicate whether an application is a continuation or continuation-in-part. Stephen G. Kunin, Benefit of Prior-Filed Application, USPTO Official Gazette 18 March 2003. The present Applicant Entity (hereinafter "Applicant") has provided above a specific reference to the application(s) from which priority is being claimed as recited by statute. Applicant understands that the statute is unambiguous in its specific reference language and does not require either a serial number or any characterization, such as "continuation" or "continuation-in-part," for claiming priority to U.S. patent applications. Notwithstanding the foregoing, Applicant understands that the USPTO's computer programs have certain data entry requirements, and hence Applicant is designating the present application as a continuation-in-part of its parent applications as set forth above, but expressly points out that such designations are not to be construed in any way as any type of commentary and/or admission as to whether or not the present application contains any new matter in addition to the matter of its parent application(s).

All subject matter of the Related Applications and of any and all parent, grandparent, great-grandparent, etc. applications of the Related Applications is incorporated herein by reference to the extent such subject matter is not inconsistent herewith.

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The invention relates to systems and methods for strengthening customer loyalty in restaurant and retail chains and in other establishments providing goods and services to customers.

RELATED ART

In traditional customer loyalty systems, a customer is usually given a plastic bonus card that the customer then presents when making a payment to a restaurant, restaurant chain, store, retail establishment, wholesale establishment or other similar type company (hereinafter "company"), perhaps one that is a member of a franchise or chain of stores. Upon presentation of the card, the customer may receive bonus points, discounts, and the like.

Typically, customers own many bonus cards issued by different companies. In some companies, the loss of a bonus card by a customer results in the loss of accumulated bonus points and discounts. Additionally, a lost bonus card may be misused be a company's staff or by any other ill-intentioned person that may find it. If the bonus card is associated with a virtual wallet, credits may be lost.

Another drawback of existing customer loyalty systems includes a lack of a means of connecting customers to a social network. Further, loyalty cards do not provide any means for customers to communicate their opinion about the quality of the consumed goods or services directly to the company, and do not enable the company to gather reliable data on consumption of and demand for its specific goods or services.

From the perspective of a company, such company would like to collect certain personal data. Such information might include information to identify and contact customers such as name, phone number, email address, home address or other geographic locator, photograph, date of birth, sex, and identification of friends or relatives who typically accompany the customer, etc. Many companies already collect consumption information such

as what services have been consumed, goods bought, preferences, and details related to each purchase such as the day of week, date of the year, hour of the day, etc. However, a company often cannot connect this information reliably with customers because of the problems associated with loyalty cards.

In terms of applying for a loyalty card, certain existing loyalty systems and companies use paper application forms. Often, a company employee enters the data from the form. Mistakes can be made during data entry assuming that the customer provided correct and legible information. Companies using paper-based forms are saddled with the extra cost of entering or scanning the customer identifying data. Other existing loyalty systems engage and invite customers to fill out an online application form. However, there are many shortcomings with this arrangement. Customers frequently ignore the invitation to do so or forget to do so. When customers do so, the customer does not do so within a reasonable time after a purchase, thus information associated with any recently purchased product or service is lost and unconnectable with a newly issued loyalty card. Further, customers may not enter data in all of the available fields on the online form leaving companies with incomplete customer identification information. As a result, there is a low conversion of customers to known and trackable customers with whom companies can meaningfully engage.

Once a loyalty card has been issued, it is often used at the point of sale by swiping it through a machine to read its magnetic strip or barcode. Frequently, customers complain of having too many loyalty cards to carry in their wallets and thus forget to bring them shopping.

While there may soon be barcodes on screens of mobile devices or devices using near field technology, there are also drawbacks with the use of these devices and technologies. For example, in a restaurant, a customer is required to bring his phone or device near a cash register or point of sale terminal that can detect the device. Customers are not likely to entrust a waiter with their phone! Thus, there is likely to be a low conversion of information gathered

and a low availability of information about a purchase and connectable to an appropriate customer. A dialogue or repeat interaction between such a company and customer is lost.

These and other shortcomings of the current art are overcome by use of the present invention.

SUMMARY

A customer loyalty system, device and method for consumers of goods and services (e.g. guests of restaurants, retail establishments and the like) are disclosed. The customer loyalty system assists to build and keep a customer base. The customer loyalty system enables establishments to gather feedback from customers, to obtain reliable information about the quality of the goods and services offered and about the consumption of goods and services by customers. The customer loyalty system enables establishments to optionally create customer social networks. The customer loyalty system described herein may be implemented with, for example, a Web site and related services, one or more mobile communication devices with Internet access (such as but not limited to cell phones), and point-of-sale (POS) terminals, among others as more fully described herein.

The customer loyalty system, device and method rid a customer of multiple club, bonus, discount, and similar types of cards ("loyalty cards") enabling the customer to receive various privileges from retail outlets, restaurants, gas stations, agencies, etc., by replacing these cards with one account in a loyalty system, the said account being associated with, for example, a customer cell phone number.

The customer loyalty system is able to respond to and interact with registered customers. For example, once the customer enters a code, the loyalty system is able to recognize or acknowledge that the customer is near or otherwise ready to interact with the loyalty system.

In one implementation, a short-lived active promotional code enables the customer to pay for goods and services from his account in the system (such as through a "virtual wallet") and to accumulate bonus points on this account. An establishment or company is able to aggregate consumption data and correlate or connect with data associated with a registered customer. A point of sale (POS) system prints a bill with the short-lived active promotional code or activation code. This short-lived active promotional code identifies the currently

ordered or selected goods or services at the particular establishment. Further, the POS system or device uploads, stores, transmits or sends a corresponding list of goods, services or goods and services of the bill (and provided to the customer) and associates the list with a particular short-lived active promotional code. The POS system may upload, store, transmit or send the entire list of goods, services or goods and services, an identifier of the bill, or other code that can be used to match one or more of the goods, services or goods and services with the promotional code. The POS system or device may be loaded or pre-loaded with a certain number of promotional codes and thus may operate offline. When re-connected, the POS system or device may then be accessed or directed to divulge its bills, lists of goods and services, associated information and promotional codes that were used and unused.

The short-lived active promotional code expires after a few minutes or a relatively short time (e.g., seconds, minutes, hours, days, or weeks depending on the needs or desires of a particular company or business). A customer receives the bill with the short-lived active promotional code. Through, for example, a mobile Internet-enabled device, a customer redeems the short-lived active promotional code. Redemption may be done in a variety of ways, and may be done before or after payment, but before code expiration.

After expiration of the code, a customer may also access the loyalty system from any mobile communication device or computer connected to the Internet or other network by authenticating with the customer loyalty system. The customer may then access his one or more virtual wallets. In one implementation, each virtual wallet is associated with a separate establishment or chain of similarly named establishments.

This Summary introduces a non-exclusive selection of concepts and aspects of the customer loyalty system, device and method in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key or essential features of the claimed subject matter, and it is not intended to be used to limit the scope of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the subject matter are set forth in the appended claims. Throughout, like numerals refer to like parts with the first digit of each numeral generally referring to the figure which first illustrates the particular part. The subject matter and a preferred mode of use are best understood by reference to the following Detailed Description of illustrative implementations when read in conjunction with the accompanying drawings.

FIG. 1 is a diagram of an exemplary implementation of a customer loyalty system.

FIG. 2 is a diagram of another exemplary implementation of a customer loyalty system.

FIG. 3 is a diagram of an exemplary computer system or hardware and/or software with which a customer loyalty system may be implemented.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is directed to a customer loyalty system (herein "system" or "loyalty system") for consumers of goods and services (e.g. guests of restaurants, retail establishments, gas stations, agencies, and the like – herein "companies") aimed to build and keep a customer base. The customer loyalty system enables such restaurants, retail establishments and the like to gather feedback from customers and to obtain reliable information about the quality of the goods and services offered and about the consumption of goods and services by customers. The customer loyalty system enables companies to expand a customer base, and to, optionally, create customer social networks and participate in existing customer networks using the techniques described herein. The customer loyalty system described herein may be implemented with, for example, a Web site, database, Web or other server, one or more mobile communication devices with Internet access (such as but not limited to cell phones), and point-of-sale (POS) terminals, among others as more fully described herein.

The customer loyalty system rids a customer of multiple club, bonus, discount, and similar types of cards ("loyalty cards") enabling the customer to receive various privileges from companies by replacing one or more cards with an account in a loyalty system, the said account being associated with, for example, a customer's cell phone number.

One feature of the customer loyalty system is the ease of access to the loyalty system. For example, once a customer registers with the system, the system is able to recognize the customer automatically or in a programmatic way. For example, once the customer enters a code, then the loyalty system is able to recognize or acknowledge that the customer is near or otherwise ready to interact with the loyalty system.

In an exemplary implementation, an active promotional code enables the customer to pay for goods and services from his account in the system (such as through a "virtual wallet") and to accumulate bonus points, reward points, frequently flyer miles, etc. on this account.

The customer may also access the loyalty system from any mobile communication device or computer connected to the Internet or other network by authenticating with the system – for example, entering a login and password or other credential – in which case the customer gets access to his one or more virtual wallets. In the exemplary implementation, each virtual wallet is associated with a separate establishment or a chain connected to or participating in the loyalty system. However, for compatibility with earlier or other systems, the use of previously issued plastic cards may be supported.

Referring now to the figures, implementations of the invention are described in detail. In referring to the figures, like numerals refer to like parts.

FIG. 1 is a diagram of an exemplary implementation of a customer loyalty system illustrating some of its aspects in a scenario involving a restaurant. FIG. 1 shows some of the technical means that may be used to implement such a customer loyalty system. With reference to FIG. 1, the system itself may be accessible as an Internet resource (such as a Web site) hosted on one or more Web or other type of servers 101 (hereinafter "Web server"). The Web server 101 hosts or is electronically in communication with a database (Card Server) (not shown) of customers, which contains information about the customers, their virtual wallets, orders, history of visits, etc. The Web site is accessed from one or more point-of-sale terminals 103 and from customer mobile communication devices (e.g., cell phones, tablets, smart phones, laptops) 105, or from any other device connectable to the Internet or through another means or protocol. While not shown, a point-of-sale terminal 103 may also be connected to or in communication with a server that operates a restaurant management system. Such restaurant management server stores and manages information about orders, their origins, availability of tables, active promotional codes, etc.

Communications 102 between customers 105 and the Web server 101 enable the customers 105 to access their virtual wallets and the promotional codes of their meal or other orders (goods or services). Via one or more communications 102, customers optionally may

order additional dishes, ask for their bill, pay all or part of their bill using their virtual wallet, receive a bonus (e.g., receive a discount on the current or future order), buy a dish for a friend, and rate the dishes, the establishment, the waiter, the information services, etc.

In an exemplary scenario, a customer who has previously registered with the system and provided information regarding a bank account or credit card, upon receiving a promotional code (either electronically or on paper), enters the promotional code into an application or user interface of a portable electronic device, which was also previously registered, recorded or associated with the customer. The customer activates or sends the promotional code through a communication 102 to the Web server 101. The promotional code alone may trigger a subsequent communication 102 to the customer, as long as the promotional code was activated within the limited time. The subsequent communication 102 requests authorization from the customer to pay the bill (for the order) by charging the bill to the customer's credit card or bank account associated with the customer or account with the restaurant. Activation of the promotional code alone may trigger payment if the customer has configured such action to take place. Alternatively, if the customer has agreed or configured his account in the system accordingly, activation of the promotional code automatically charges the bill to the account, credit card or virtual wallet. After the limited time, there is no such prompt and no such automatic payment. The limited time may be just a few minutes in such a scenario, or may be longer depending on the desires of the administrator or company using the system. In this scenario, the system may prompt a customer 105 to confirm his identity, confirm an amount to be paid, ask if an additional gratuity (tip) is to be added to the amount paid, etc. If the promotional code is activated by an unregistered device, the system may prompt for the identity of the customer activating the promotional code and allows one customer to pay for an order of another customer. Thus, while a first customer initiated the order with a waiter, another or second customer may use the promotional code to pay for the order. A promotional code may be passed from device to device, and from customer to

customer in a peer-to-peer fashion. Any of the customers may then activate the promotional code. Once a promotional code has been activated, the system expires the promotional code, at least for payment purposes, and may or may not expire the promotional code in terms of granting of a discount or other promotional offer.

In another implementation, customers may receive and accumulate reward points associated with a particular company for purchasing goods, services or goods and services from the particular company. One company may opt to allow exchanges of these points for cash or for exchange for reward points of another company. Through the Website 101, a customer may exchange points such as from one account to another or from one virtual wallet to another. Companies can set exchange rates and may do so through the system Website 101. In another implementation, participating companies may set exchanges rates for traditional currencies so that they could offer, for example, a two percent discount to customers who pay through their virtual wallet or through the reward system, virtual wallet and use of promotional codes. In another implementation, customers may exchange reward points with each other in a peer-to-peer fashion. For example, a single member of a family may aggregate reward points from other members of the family so that a single member of the family may receive a free meal at a participating restaurant. In principle, each company, business or participating establishment can have its own currency. The amount of money in this currency is effectively its liability to its customers. Thus, a company's liabilities can be traded, traditional cash payments may be eliminated or reduced.

Communications 102 facilitate interactions between customers via the Web server 101. Such customers 105 may be customers that are currently consuming or have recently consumed restaurant goods and/or services (such as within a few minutes, hours, days, etc.). According to another aspect, customers 105 may interact with any other customer having an account in the system and who have patronized a particular establishment. Further, the Web server 101 enables customers 105 to engage in an online text or voice chat with each other.

Communications 104 between a point-of-sale terminal 103 or an administrator terminal (not shown) accessible by a waiter and a device used by a customer 105 enable printing, downloading or otherwise accessing or saving of a receipt. For example, a customer 105 may download a copy of the receipt to his cellular phone. In a preferred implementation, the receipt includes a promotional code as described more fully herein and below.

Other communications 106 transfer information between the Web server(s) 101 and one or more point-of-sale terminals 103. Such other communications 106 may include information about, for example, payment of customer bills (and optionally bonus points granted), completed orders and bonuses, rewards or discounts issued during a particular period, food or service rankings assigned by customers, customer preferences, etc.

FIG. 2 shows another exemplary implementation of a customer loyalty system 200 illustrating some of its aspects. With reference to FIG. 2, a guest or customer 105 joins the loyalty system 200 as follows. During his or her first visit to a restaurant or other establishment, the customer 105 receives a bill 202 from a waiter or cashier for goods or services purchased or consumed. In such implementation, the bill 202 includes an invitation to join the loyalty system 200 to thereby become eligible to receive a discount on the current order, a first order or a subsequent order. As another example, by use of a promotional code, a registering customer receives a free dessert or other reward including an instant reward.

To join the loyalty system 200, the customer 105 visits the Web site 101 of the loyalty system 200, enters requested information and submits this information via a registration function or user interface element. Such may be done through a smartphone or other Web enabled device (not shown). Preferably, registration occurs while the customer is still in the restaurant.

Alternatively, for registration, a customer 105 sends an SMS text message from his cellular phone that corresponds ideally with the cellular phone number assigned to that device. In a preferred implementation, the SMS text message includes a promotional code

212 that was printed or otherwise made available on or through the bill 202. Thus, the promotional code 212 is associable or connected with the goods or services ordered and itemized on the bill 202. The customer cell phone number serves as an authentication mechanism such as a login, user identification, account name, account identifier or authentication scheme.

As one example, the promotional code 212 is a short sequence of letters and/or digits, e.g. a 2, 3, 4, 5, 6 or other-length-digit, character sequence, number or the like. The promotional code 212 may also be a two- or three-dimensional code, picture, etc. For example, a promotional code may be a quick response code or QR code, a bar code or non-human readable code. The promotional code 212 may also be printed with a non-human-visible ink or other material that is detectable by a consumer device. Thus a near field detector, RFID detector and the like may be used to detect, access and use such a promotional code 212. In a preferred implementation, the promotional code 212 is generated by the POS terminal or device 103 using one or more algorithms. In one particular implementation, one of the one or more algorithms involves random number generation to generate a promotional code 212. In another implementation, the Web site 101 generates promotional codes 212. Use of a promotional code may involve manually entering an alphanumeric code, resending an electronically delivered promotional code or may involve scanning or photographing a promotional code.

The promotional code 212 serves as a unique ID of the order in a given restaurant and, preferably, must be activated by the customer within a short period of time after the customer receives the promotional code 212 or a short time after generation of the promotional code 212. Otherwise, the promotional code 212 is or may be recycled. A promotional code 212, or a combination of promotional code 212 and one or more other numbers or digits, may be used to uniquely identify, for example, the following: an order at a particular establishment, an order and patron at a particular establishment, an order across all

establishments registered with the system, etc. Such unique identity is for a particular time interval. A time interval may be just a few minutes, a few hours, a few days, a few weeks, etc. Thus, a promotional code 212 may be unique across all establishments or may be semi-unique in the system 200 across all times or within a time interval.

Activating the promotional code 212 provides a discount on the order or bonus points for the order, or some other benefit or combination of benefits. All promotional codes 212 activated by or put in use by establishments (a variety of retailers, restaurants, etc.) connected to or registered with the loyalty system are known to the system 200 (e.g., to the Web server 101).

Upon joining the loyalty system 200, a customer 105 is registered with the system 200, and the system 200 uses the customer cell phone number (for example) as his account identifier or login. After registration, the customer 105 gets access to his account in the loyalty system 200 and can enter additional personal data, review and change it and supervise one or more virtual wallets. Subsequently, when a customer 105 accesses the loyalty system 200, the system recognizes each customer 105 by his cell phone number, which is likely a unique number in the loyalty system 200. Alternatively, an email-address, unique nickname or one or more other personal data may be used to identify a customer account in the loyalty system 200.

In a subsequent visit to the restaurant, a customer 105 who already has an account in the loyalty system 200 may get immediate access to information about his order by asking the waiter 204 for the promotional code 212 of the newly created food order. The waiter 204 or an employee that registers orders provides the customer 105 with the promotional code 212 generated upon creating the order. The customer 105 may access the information about his order through his smart phone (such as through an application operating on the smart phone, via SMS text message or some other way), Internet enabled device, traditional phone or other device. For example, after entering or otherwise using the promotional code 212, the

customer 105 may access his order from his device by seeing or receiving a status indicator (e.g. "in progress" or "ready"). Through the use of the promotional code 212, the customer 105 may order additional items if desired (dishes, goods, services, etc.), because the promotional code 212 remains active during a period of time after its creation, for example, 20 minutes, one hour, two hours, several hours, one day, etc. The delivery of a promotional code 212 may be done with or without delivery of a customer's receipt or bill, and may be delivered on paper or electronically such as through an SMS text message, email message, through an application operating on a customer's smart phone or voice message to a traditional phone. A customer 105 may use the loyalty system 200 to discover how much money he has in his virtual wallet, and pay his bill from this virtual wallet, by credit card, or by using another method of payment.

Further, once registered with a loyalty system, a customer may view a menu of a restaurant where he is currently at and may view current promotional offers that are available from the restaurant that are only offered to registered members of the loyalty system 200. If the customer orders an item via the restaurant's Web site 101 or loyalty system 200 (instead of through a waiter or other traditional means), the customer may receive bonus points and discounts on the entire order, possibly in addition to any promotion or discount offered for connecting with or using the loyalty system.

In another implementation of the loyalty system 200, a member or customer 105 may also receive additional bonus points by attracting new customers (e.g. friends, family) to a restaurant M at which the customer 105 is registered. In one exemplary scenario to attract a new customer, an existing customer 105 authenticates with restaurant M's Web site 101 or system 200, pays for a dish or drink, and specifies that the dish or drink is intended for a customer with a particular cell phone number N. The recipient or person associated with cell phone number N receives an SMS text message at the cell phone number N inviting him to restaurant M, and notifying him of the dish or drink that has been bought for him there. The

SMS text message may contain the special promotional code of the order. The new prospective customer is required to visit restaurant M, register with the loyalty system 200, and enter the special promotional code into the loyalty system 200. Once the promotional code is accepted, the new customer will see his active pre-paid order. Bonus points for customers who invite their friends to the restaurant may be calculated, for example, as a percentage of the sums of orders subsequently placed by the invitees. Bonus points and rewards are awarded for friends and other persons that subsequently sign up. In yet a further implementation, rewards for attracting and promoting the registration of friends of friends may be given in a fashion akin to pyramid selling rewards. Thus, a first registered customer may accumulate substantial rewards for referring new customers to a particular establishment through the loyalty system 200.

Management of a particular restaurant may issue special promotional codes to grant bonus points to its registered customers or may raise their bonus priorities. To this end, a restaurant's waiter or employee enters one or more parameters and causes the POS terminal or device 103 to issue a particular, special bonus (such as a number of bonus points or a bonus percentage). The special bonus may include a time to live prior to activation, a bonus time to live after activation, etc. A generated promotional code may be printed on a printer and handed over to a customer or may be delivered electronically to the particular customer. When the patron or customer enters or uses the special promotional code associated with the loyalty system, he receives the granted bonuses after fulfilling any particular requirements (if any). This type of promotional code may be granted for free or may require purchase of a good or service or require a customer to purchase this type of promotional code. This type of promotional code may be generated in batches so that, for example, all customers in a particular restaurant in a block of time receive or are eligible for a particular special promotion, promotional code or special bonus. For example, a special batch of codes may be generated and be active for a Happy Hour event at a restaurant.

Additionally, a customer may access the loyalty system without entering a promotional code if the customer is currently not on the premises of a participating establishment, an establishment that is a member of the loyalty system. The customer is still able to view the statuses of his virtual wallets, see promotional offers from the loyalty system restaurants and stores, and possibly, depending on the customer's current location or the location specified by the customer as a preferred destination, see the menus of the corresponding restaurants, the availability of tables to be booked, etc. For example, the customer may book a table and order a dish for a certain time and pay for it from the virtual wallet. At any moment, the customer will be able to see the rankings of the loyalty system restaurants as entered by other members of the loyalty system community. Additionally, the customer may view his restaurant-going history, e.g. which restaurants he visited and when and what dishes he ordered there, and his history of "gifts" to and from friends. Upon making a payment for an order, a customer may have a small questionnaire sent to his account such as to his mobile or other registered device.

In another implementation, if a customer makes certain information about himself known to the loyalty system, for example his name, his photo, or a code word, the customer will be rewarded with extra features. For example, one of these features is the ability to make payments from one or more of his virtual wallets without using a promotional code.

In fast-food restaurants or in a store where payments are made at a POS terminal, the system will automatically detect the customer if his cell phone is turned on using near field technology, a cellular telephone technology, a GPS technology, etc. If the customer expresses his wish to pay from his virtual wallet and/or to receive the applicable discount, the cashier will only need to authenticate the customer by his name, photo, code word or using other suitable information.

Additionally, the use of the loyalty system may prevent fraudulent actions by third parties and, in particular, by employees of the establishments. In traditional customer loyalty

systems, a lost bonus card may often be used by any person that finds it without any authentication or cross reference to other information. The loyalty system requires that the user not only knows the right promotional code, but also owns or possesses the customer device (e.g., cell phone) or provides an identifier (e.g., cell phone number) that was used to register with the loyalty system at this specific place. To further prevent fraud, a location of the given cell phone may be checked by using a geo-location technology, such as GPS, A-GPS or SBAS. The cell phone numbers of restaurant staff are usually known and may be blocked in the loyalty system, at least when the cell phones of the restaurant staff are in physical proximity to the restaurant and when the restaurant staff are working. In case of doubt, one or more additional checks or authentication mechanisms may be applied based on the supplied credentials—for example, additional questions may be sent to the customer by SMS or an account verification may be made through a partnership with a respective mobile carrier (provider).

The loyalty system 200 may also be configured to build, maintain and facilitate a customer social network. The social network may include such functions as Internet Relay Chat (IRC) or other type of chat, a blog, or a customer review forum, recommendation forum, "check-in" tallies and the like. When a registered customer engages with the loyalty system at a participating restaurant, the customer may receive or access a current status indicator for each of his friends or for each of any other registered customer that is also participating at the participating restaurant. Alternatively, the registered customer be able to receive or access a current status indicator for any other registered customer that is in the vicinity of the registered customer. There is provided an option whereby a registered customer's status is set to "invisible" such that other registered customers are not updated as t a registered customer's location or participation at a particular restaurant. Participating customers may be able to send other registered customers personal messages, or make a posting on a common bulletin board for the particular establishment. In this manner, a registered customer may notify his

friends or other members of the loyalty system community about his intention to make a future visit to a particular restaurant.

The loyalty system enables companies to gather accurate information about their customers such as their gender, age, occupation, frequency of visits, preferences, and other participating restaurants visited. Using such data, a loyalty system may provide a company information that a company could use to determine how the company ranks among other similar establishments, get reliable data about the quality of work of his employees (bartenders, waiters, chefs), and learn what customers liked and what customers disliked.

Exemplary Device

FIG. 3 of the drawings shows an exemplary hardware 300 or device that may be used to implement the present invention. Referring to FIG. 3, the hardware 300 typically includes at least one processor 302 coupled to a memory 304. The processor 302 may represent one or more processors (e.g. microprocessors), and the memory 304 may represent random access memory (RAM) devices comprising a main storage of the hardware 300, as well as any supplemental levels of memory, e.g., cache memories, non-volatile or back-up memories (e.g. programmable or flash memories), read-only memories, etc. In addition, the memory 304 may be considered to include memory storage physically located elsewhere in the hardware 300, e.g. any cache memory in the processor 302 as well as any storage capacity used as a virtual memory, e.g., as stored on a mass storage device 310.

The hardware 300 also typically receives a number of inputs and outputs for communicating information externally. For interface with a user or operator, the hardware 300 may include one or more user input devices 306 (e.g., a keyboard, a mouse, imaging device, scanner) and a one or more output devices 308 (e.g., a Liquid Crystal Display (LCD) panel, a sound playback device (speaker)).

For additional storage, the hardware 300 may also include one or more mass storage devices 310, e.g., a floppy or other removable disk drive, a hard disk drive, a Direct Access

Storage Device (DASD), an optical drive (e.g. a Compact Disk (CD) drive, a Digital Versatile Disk (DVD) drive) and/or a tape drive, among others. Furthermore, the hardware 300 may include an interface with one or more networks 312 (e.g., a local area network (LAN), a wide area network (WAN), a wireless network, a cellular network (not shown) and/or the Internet among others including all of the devices or equipment necessary to carry out network communication) to permit the communication of information with other computers or devices coupled to the networks. It should be appreciated that the hardware 300 typically includes suitable analog and/or digital interfaces between the processor 302 and each of the components 304, 306, 308, and 312 as is well known in the art.

The hardware 300 operates under the control of an operating system 314, and executes various computer software applications, components, programs, objects, modules, etc., to implement the techniques described above. In particular, the computer software applications may include a client application, in the case of the client user device or smart phone 302. Moreover, various applications, components, programs, objects, etc., collectively indicated by reference 316 in FIG. 3, may also execute on one or more processors in another computer coupled to the hardware 300 via a network 312, e.g. in a distributed computing environment, whereby the processing required to implement the functions of a computer program may be allocated to multiple computers over a network.

In general, the routines executed to implement the embodiments of the invention may be implemented as part of an operating system or a specific application, component, program, object, module or sequence of instructions referred to as "computer programs." The computer programs typically comprise one or more instruction sets at various times in various memory and storage devices in a computer, and that, when read and executed by one or more processors in a computer, cause the computer to perform operations necessary to execute elements involving the various aspects of the invention. Moreover, while the invention has been described in the context of fully functioning computers and computer

systems, those skilled in the art will appreciate that the various embodiments of the invention are capable of being distributed as a program product in a variety of forms, and that the invention applies equally regardless of the particular type of computer-readable media used to actually effect the distribution. Examples of computer-readable media include but are not limited to recordable type media such as volatile and non-volatile memory devices, floppy and other removable disks, hard disk drives, optical disks (e.g., Compact Disk Read-Only Memory (CD-ROMs), Digital Versatile Disks (DVDs), flash memory, etc.), among others. Another type of distribution may be implemented as Internet downloads.

Systems, devices and methods have been described for facilitating the display or use of displaying or using text and other information in a format that substantially appears as originally displayed or found on or in a medium (e.g., screen, television, paper, book, newspaper, fax, sign, photograph, magazine, etching, sculpture). Throughout, for sake of simplicity in explanation, reference is made to text and/or words. However, text and words refer generally to any information that is capable of being perceived, identified, recognized or used and may be found in or on any medium. While a smart phone is referred to herein, it is merely exemplary. It is to be understood that "smart phone" refers to any device that cannot display an actual sized representation of the menu 202 or to a device with a relatively small display (e.g., tablet, laptop, appliance).

While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative and not restrictive of the broad invention and that this invention is not limited to the specific constructions and arrangements shown and described, since various other modifications may occur to those ordinarily skilled in the art upon studying this disclosure. In an area of technology such as this, where growth is fast and further advancements are not easily foreseen, the disclosed embodiments may be readily modifiable in arrangement and detail as

facilitated by enabling technological advancements without departing from the principals of the present disclosure.

While the invention has been described with respect to a preferred implementation, other implementations are possible. The concepts disclosed herein apply equally to other non-described systems, devices and methods for displaying or using text (and information generally) in a format that substantially appears as originally displayed or found on or in a medium. Furthermore, the concepts applied herein apply more generally to displaying or using text and breaking adjacent text at word and other logical boundaries such as at, near or around a character or element. The invention is described below with reference to the accompanying figures.

The foregoing discussion has been presented for purposes of illustration and description. Various features from one implementation can be combined with other features from other implementations. The description is not intended to limit the invention to the form or forms disclosed herein. Consequently, variation and modification commensurate with the above teachings, within the skill and knowledge of the relevant art, are within the scope of the present invention. The implementations described herein and above are further intended to explain the best mode presently known of practicing the invention and to enable others skilled in the art to use the invention as such, or in other implementations, and with the various modifications required by their particular application or uses of the invention. It is intended that the appended claims be construed to include alternate implementations to the extent permitted.

CLAIMS

We claim:

1. A method for providing a customer loyalty reward to a customer, the method comprising:

generating a promotional code that is active for a limited time;

associating the promotional code with an order for goods or services;

sending the promotional code that is active for the limited time;

receiving an indication of use of the promotional code within the limited time; and

sending an indication of a customer loyalty reward to the customer after receiving an indication of use of the promotional code within the limited time.

2. The method of claim 1 wherein the method for providing a customer loyalty reward to a customer further comprises:

automatically charging a financial account associated with the customer after receiving the indication of use of the promotional code within the limited time.

3. The method of claim 1 wherein the sending the promotional code that is active for the limited time includes sending the promotional code in an electronic form to an account associated with the customer.

4. The method of claim 1 wherein the sending the promotional code is electronically sending the promotional code to a device accessible by the customer.

5. The method of claim 1 wherein the sending the promotional code is sending a paper to the customer.

6. The method of claim 1, wherein the method for providing a customer loyalty reward to a customer further comprises:

generating a bill for goods or services, wherein the promotional code is associated with the bill for goods or services or with an identifier of at least one of the goods or services.

7. The method of claim 1 wherein the promotional code is a series of digits, and wherein the promotional code is unique for the limited time across all customer orders for a company associated with the customer loyalty reward.

8. The method of claim 1 wherein the promotional code is a series of digits, and wherein the promotional code is unique for the limited time across all customer orders for all participating companies.

9. The method of claim 1 wherein the promotional code is a series of digits, and wherein the promotional code is unique for the limited time across all customer orders for all participating companies.

10. The method of claim 1, wherein sending the promotional code that is active for the limited time includes sending the promotional code to a social network account of the customer, the account being part of a social network.

11. The method of claim 1, wherein the promotional code is associated with a business, and wherein the customer loyalty reward is dependent on a number of times that the customer has interacted with the business.

12. The method of claim 11, wherein the customer loyalty reward is dependent on an amount of money that the customer has transacted with the business over a period of time or in a current transaction.

13. The method of claim 11, wherein the customer loyalty reward is dependent on a number of other customers that transacted money with the business since a last visit to the business by the customer in response to a previous promotional code shared by the customer with the other customers.

14. The method of claim 1, wherein the promotional code is associated with a current transaction with a business or company.

15. The method of claim 14, wherein receiving the indication of use of the promotional code within the limited time is done before payment by the customer.

15. The method of claim 14, wherein receiving the indication of use of the promotional code within the limited time is done after payment by the customer.

16. The method of claim 1 wherein the associating the promotional code with the order for goods or services includes associating the promotional code with information associated with the device accessible by the customer.

17. The method of claim 1 wherein the method for providing a customer loyalty reward to a customer further comprises:

sending the promotional code that is active for the limited time to a server after generating the promotional code, wherein the generating the promotional code is done by a point of sale device; and

sending information identifying the goods or services of the order to the server after generating the promotional code.

18. A device configured to provide a service to a plurality of customers, the device comprising:

a promotional code generator that is capable of generating a promotional code that is active for a limited time, each promotional code corresponding to a customer;

an interface service capable of sending and receiving information to and from a point of sale device;

an authenticator configured to receive promotional codes and to activate a reward corresponding to a respective promotional code when the promotional code is sent electronically to the authenticator within the limited time; and

a recorder configured to record information associated with each promotional code sent to the authenticator.

19. The device of claim 18 wherein the promotional code generator is configured to generate a promotional code in response to the interface service receiving a request from the point of sale device.

20. The device of claim 18 wherein the recorder is further configured to record information related to a consumer redeeming a promotional code.

21. A system comprising:

circuitry for generating a promotional code that is active for a limited time;

circuitry for sending to a device, the device accessible to a customer, the promotional code that is active for the limited time;

circuitry for receiving the promotional code within the limited time; and

circuitry for delivering an indication of a customer loyalty reward to the customer after receiving an indication of use of the promotional code within the limited time.

22. The system of claim 21, wherein the circuitry for generating the promotional code that is active for the limited time is configured to re-issue the promotional code after the limited time.

23. The system of claim 21, wherein the circuitry for receiving the promotional code within the limited time is configured to receive identifying information from the device accessible to the customer, the identifying information corresponding to the device accessible to the customer, the customer or both the device accessible to the customer and the customer.

24. The system of claim 21, wherein the indication of the customer loyalty reward includes information that may be used to acquire the customer loyalty reward.

25. A computer program product comprising one or more tangible computer accessible storage media configured with instructions for executing the following process:

generating a promotional code that is active for a limited time;

sending the promotional code that is active for the limited time to the customer;

receiving an indication of use of the promotional code within the limited time; and

sending an indication of a customer loyalty reward to the customer after receiving an indication of use of the promotional code within the limited time.

26. The computer program product of claim 25, wherein the limited time is variable and the promotional code is active for as long as the customer is within a predetermined geographical area associated with the customer loyalty reward.

27. The computer program product of claim 25, wherein the limited time is variable and the promotional code is active for as long as the customer is within a predetermined geographical area associated with a business location.

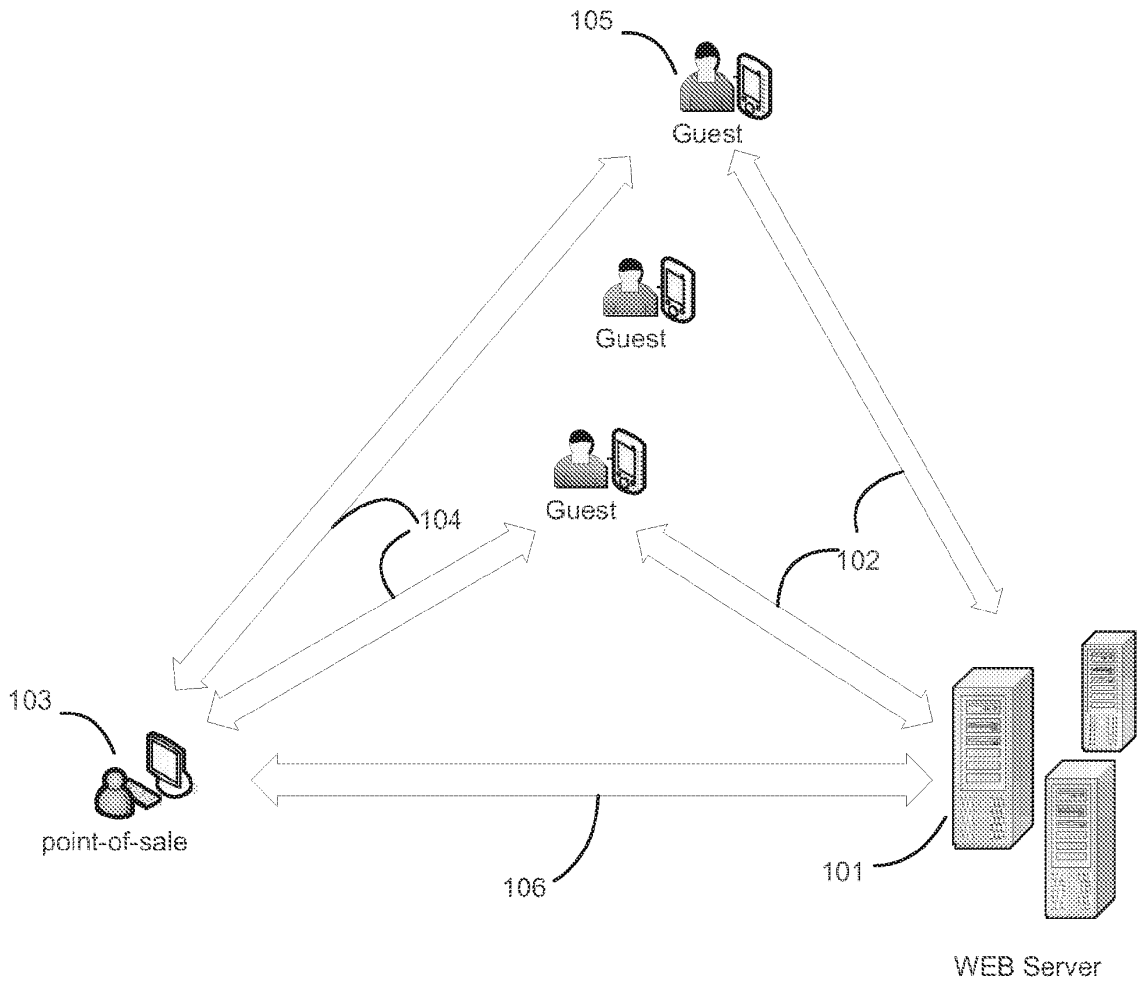

105
Guest
Guest
Guest
104
102
103
point-of-sale
106
101
WEB Server

Figure 1

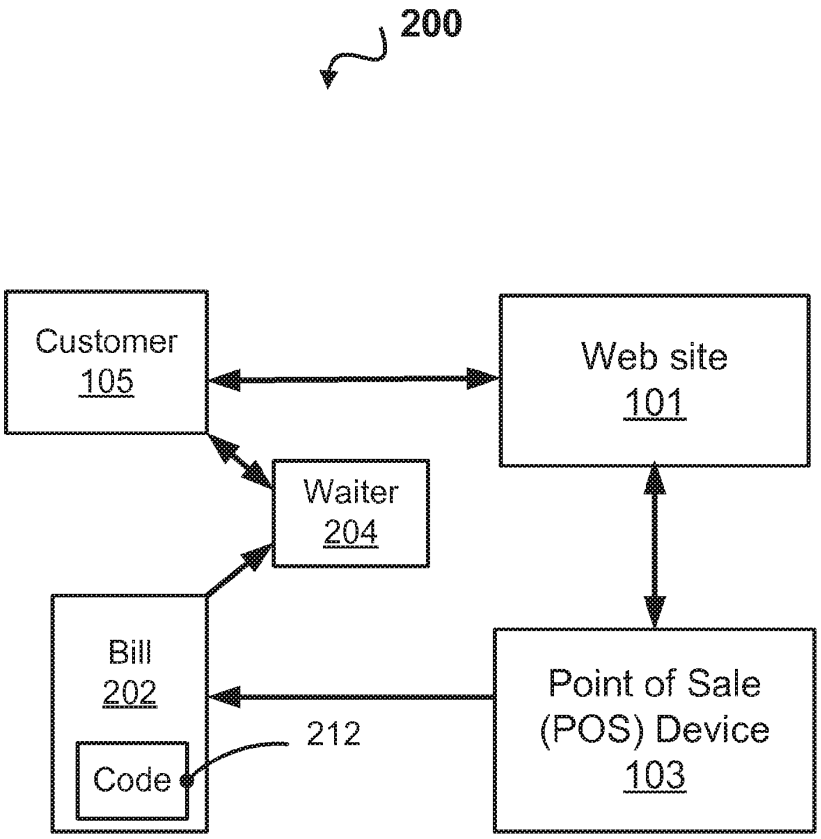

200
Customer
105
Web site
101
Waiter
204
Bill
202
212
Code
Point of Sale
(POS) Device
103

Fig. 2

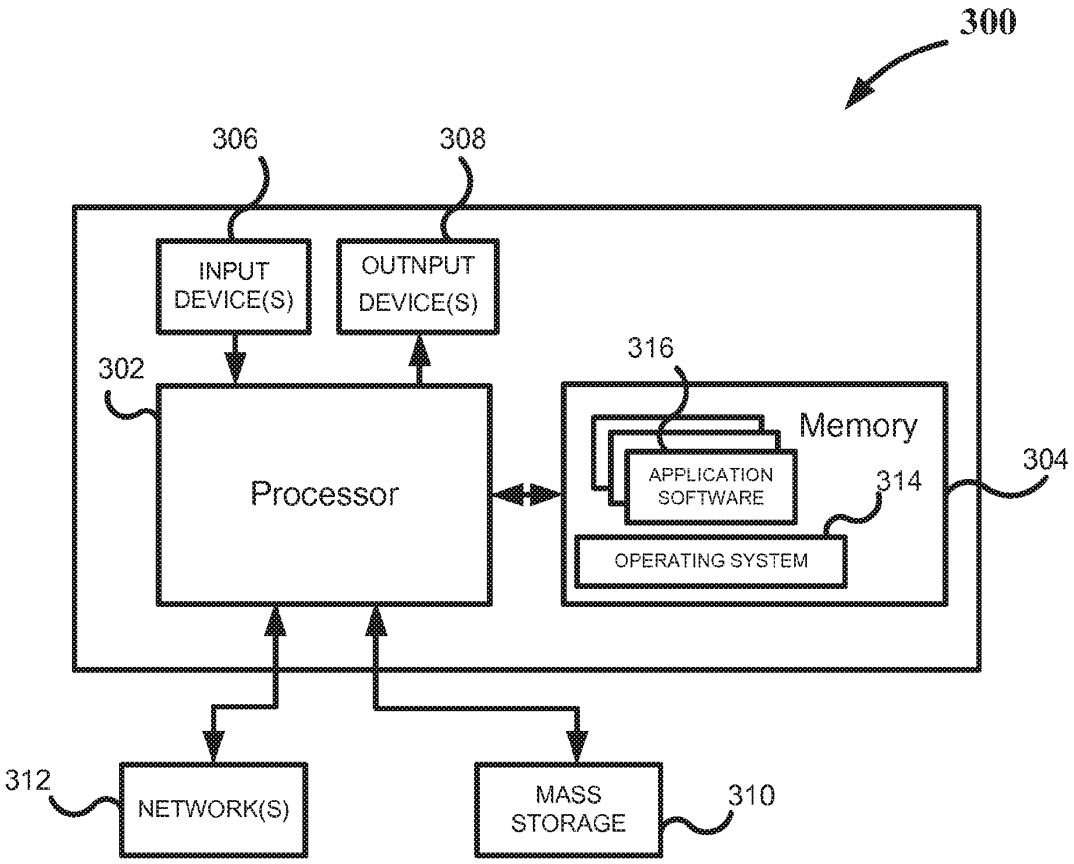

300
306
308
INPUT DEVICE(S)
OUTNPUT DEVICE(S)
316
302
Memory
APPLICATION SOFTWARE
314
304
Processor
OPERATING SYSTEM
312
NETWORK(S)
MASS STORAGE
310

Fig. 3

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2013 (17.01.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/009444 A1

(51) International Patent Classification:
G06Q 20/00 (2012.01)

(21) International Application Number:
PCT/US2012/043321

(22) International Filing Date:
20 June 2012 (20.06.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/498,957	20 June 2011 (20.06.2011)	US
61/522,099	10 August 2011 (10.08.2011)	US
13/484,199	30 May 2012 (30.05.2012)	US
13/527,466	19 June 2012 (19.06.2012)	US

(71) Applicant *(for all designated States except US)*: **MOZIDO, LLC** [US/US]; 1950 Stemmons Freeway, Suite 6040, Dallas, TX 75207 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LIBERTY, Michael, A.** [US/US]; 5373 Isleworth Country Club Drive, Windemere, FL 34786 (US).

(74) Agents: **STRINGHAM, John, C.** et al.; 60 East South Temple, Suite 1000, Salt Lake City, UT 84111 (US).

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

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

Published:

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

(54) **Title**: BUSINESS TO BUSINESS MOBILE VAULT

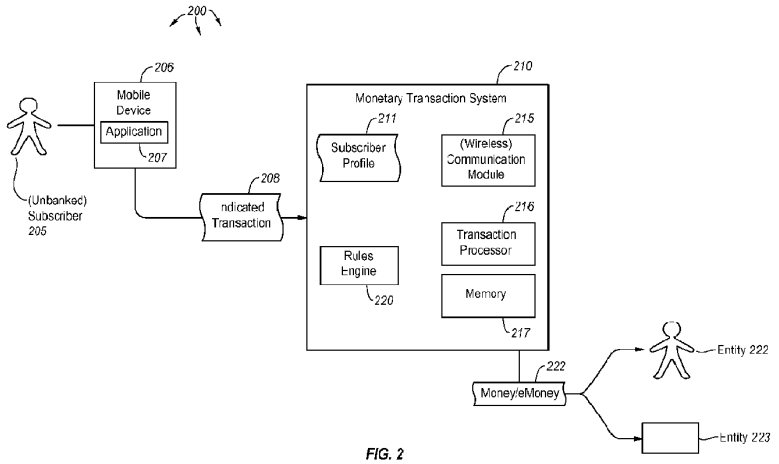


FIG. 2

(57) **Abstract**: Embodiments extend to methods, systems, and computer program products for a business to business mobile vault. Embodiments allow retailers to pay distributors electronically through the use of a mobile device such as a mobile phone. Electronic payment through a mobile phone is more efficient than a currency transaction and reduces the amount of currency that delivery and distributor personnel handle. Further, mobile phone communication is available in many geographic locations, and in some geographic locations is the only form of communication available. Thus, electronic payment through a mobile phone can often be used even when other computer systems and specialized equipment such as point of sale terminals are not available or are not used, and when other types of data connections are not available.

WO 2013/009444 A1

BUSINESS TO BUSINESS MOBILE VAULT

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to and the benefit of U.S. Utility Patent Application Ser. No. 13/527,466, filed on June 19, 2012, entitled "Business to Business Mobile Vault, and also claims priority to and the benefit of U.S. Provisional Patent Application Ser. No. 61/498,957, filed on June 20, 2011, entitled "Business to Business Mobile Vault," and which are incorporated by reference herein in their entirety. This application further claims priority to and the benefit of U.S. Patent Application Ser. No. 13/484,199, entitled "Monetary Transaction System", filed on May 30, 2012, which itself claims priority to U.S. Provisional Application Ser. No. 61/522,099, filed on August 10, 2011, entitled "Mobile Wallet Platform", and U.S. Provisional Application Ser. No. 61/493,064, filed on June 3, 2011, entitled "Mobile Wallet Platform". Each of the aforementioned applications is incorporated by reference herein in its entirety.

BACKGROUND

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 actions 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).

BRIEF SUMMARY

Embodiments of the present invention extend to methods, systems, and computer program products for a business to business mobile vault. Embodiments allow retailers to pay distributors (vendors) electronically through the use of a mobile device such as a mobile phone, tablet or other electronic device. Electronic payment through a mobile device is more efficient than a currency transaction and reduces the amount of currency that delivery and distributor personnel handle. Further, mobile communication is available in many geographic locations, and in some geographic locations is the only

form of communication available. Thus, electronic payment through a mobile device can often be used even when other computer systems and specialized equipment (e.g., point of sale terminals) are not available or are not used, and when other types of data connections are not available.

Embodiments described herein include mobile devices such as mobile phones or tablets interoperating with an electronic payment system to invoice, pay for, and track the payment for delivered goods. A merchant mobile device runs a mobile wallet application that interacts with a merchant mobile wallet at the electronic payment system. A delivery personnel mobile phone runs an invoicing application that interacts with a distributor mobile vault. Embodiments of the invention can be used to both speed up the delivery personnel/merchant transaction (allowing more deliveries per day) and reduce the amount of currency handled by delivery personnel and distributors.

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.

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.

BRIEF DESCRIPTION OF THE DRAWINGS

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:

Figure 1 illustrates a monetary transaction system architecture in which embodiments described herein may operate.

Figure 2 illustrates an alternate example embodiment of a monetary transaction system.

Figures 3A and 3B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber eMoney transfers via a mobile wallet, respectively.

Figure 4 illustrates a monetary transaction system architecture in which embodiments including business to business mobile transactions may take place.

Figure 5 illustrates an example data flow for allowing a merchant to pay a distributor for delivered goods using an electronic payment system.

DETAILED DESCRIPTION

Embodiments of the present invention extend to methods, systems, and computer program products for a business to business mobile vault. Embodiments allow retailers to pay distributors (vendors) electronically through the use of a mobile device such as a mobile phone, tablet or other electronic device. Electronic payment through a mobile device is more efficient than a currency transaction and reduces the amount of currency that delivery and distributor personnel handle. Further, mobile communication is available in many geographic locations, and in some geographic locations is the only form of communication available. Thus, electronic payment through a mobile device can often be used even when other computer systems and specialized equipment (e.g., point of sale terminals) are not available or are not used, and when other types of data connections are not available.

Embodiments described herein include mobile devices such as mobile phones or tablets interoperating with an electronic payment system to invoice, pay for, and track the payment for delivered goods. A merchant mobile device runs a mobile wallet application that interacts with a merchant mobile walled at the electronic payment system. A delivery personnel mobile phone runs an invoicing application that interacts with a distributor mobile vault. Embodiments of the invention can be used to both speed up the delivery personnel/merchant transaction (allowing more deliveries per day) and reduce the amount of currency handled by delivery personnel and distributors.

Embodiments 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.

Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change 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.

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.

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.

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.

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.

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 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.

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.

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.

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.

Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a 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.

Various terminology will be used herein to describe the monetary transaction system (also referred to as a "mobile wallet platform", "mobile wallet program", "mobile wallet transaction system", "mobile financial services (mFS) platform" or "electronic payment system"). The term "agent" is used to refer to an individual with 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.

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 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.

The mobile wallet platform may also include a mobile vault (such as distributor mobile vault 426 in Figure 4). The mobile vault may include a mobile wallet as well as other items including invoicing data. A mobile vault may be used by merchants, distributors or other users to store value (e.g. on the mobile wallet) or other important information such as invoicing data. The mobile vault allows cash (and its corresponding logistical problems) to be replaced with mobile-enabled payment collection and digital invoicing, as well as providing a mobile point of sale (mPOS) for distributors (as will be described further below).

As used herein, a mobile wallet application is a mobile wallet application installed on a mobile device, in some cases on the device's SIM card. The mobile wallet application of a merchant may interact with the mobile wallet of a distribotro distributor which is stored in the distributor's mobile vault. 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.

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. 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.

In some embodiments, the mFS platform application and/or the mobile vault 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 mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

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.

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.

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.

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 distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

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.

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".

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. 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. In some embodiments, the mFS agent manager

application itself be a mobile vault providing business-to-business cashless transactions, including other functions. In other embodiments, the mFS agent manager application may provide mobile wallet application functions and/or mobile vault functions. System-specific permissions may dictate which functions are available on each mFS agent manager application.

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. 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.

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.

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".

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.

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.

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 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.

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.

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 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.

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.

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.

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 the external processor. A Clearing House subsystem of transaction processor 121 can be used to exchange the financial information with a bank.

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.

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.

Figure 2 depicts a monetary transaction system 200 similar to that described in Figure 1. The monetary transaction system 200 may provide a more 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 know your customer (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.

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.

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 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).

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.

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.

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.

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 an electronic payment system or a third party), adding a bank/credit union account to a mobile wallet, adding a debit/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, making in store purchases from a mobile wallet, or transferring money or eMoney from one business account to another business account (i.e. from one business's mobile vault to another business's mobile vault, as will be shown in Figure 4).

Figure 3A depicts a subscriber-to-subscriber eMoney transfer. In a merchant and distributor scenario, either or both of the merchant and the distributor (including any delivery personnel) may be subscribers. To perform such a transfer, subscriber A (301) 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 (302). 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.

Figure 3B illustrates a subscriber-to-non-subscriber eMoney transfer. Accordingly, as mentioned above, either or both of the merchant and the distributor may be non-subscribers. In graphic 305, 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 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 (306). 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.

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 (307) and the user leaves with the cash in hand (308). 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.

Figure 4 depicts a physical environment and corresponding computer system architecture 400 for paying using mobile wallets to pay for delivered products.

As depicted in Figure 4, delivery vehicle 404 physically delivers goods 403 from distribution center 401 to retail location 402 (i.e. to merchant 407). It should be noted that retail location 402 may include any location to which goods are distributed including stores, homes, business offices or other locations. Distribution center 401 may be one of a number of distribution centers owned and/or controlled by distributor 462. Delivery of goods 403 to retail location 402 can be part of delivery route that includes deliveries to one or more other retail locations. Thus, before arriving at retail location 402, delivery vehicle 404 may have already made other stops to deliver other goods to one or more other retail locations. Likewise, after leaving retail location 402, delivery vehicle 404 may make additional other stops to deliver other goods to one or more additional retail locations.

After arriving at retail location 402, goods 403 are removed from delivery vehicle 404 (e.g., by one or more of: merchant 403, merchant 403's employees, and delivery

personnel 406) and left at retail location 402 for subsequent sale to patrons of the retail location.

Merchant 407 can use merchant mobile phone 408 (or another mobile device) for wireless (telephonic) communication, as well as running software applications, such as, for example, mobile wallet application 411. Delivery personnel 406 can use delivery mobile phone 409 for wireless telephonic communication as well as running software applications, such as, for example, invoicing application 412. Merchant mobile phone 408 and delivery mobile phone 409 can communicate wirelessly with (e.g., send data to, receive data from, issue commands to, etc.) electronic payment system 421 to utilize the functionality of electronic payment system 421 (i.e. monetary transaction system 210). Wireless communication can occur over a wide area wireless network, such as, for example, a cellular network. Collectively, electronic payment system 421, merchant mobile phone 408, and delivery mobile phone 409 represent a mobile payment platform (i.e. 210). Within this platform, the merchant may be an agent, and the retail location may be an agent company, and thus provide the appertaining functionality (described above) to subscribers and non-subscribers.

As depicted, electronic payment system 421 includes payment processor 422 (e.g., a payment processor used by payment handler 105), an invoice processor 423, merchant mobile wallet 424, and distributor mobile vault 426. Merchant mobile wallet 424 corresponds to merchant 407. Distributor mobile vault 426 further includes distributor mobile wallet 427 and distributor invoicing data 428. Distributor invoicing data 428 defines an invoicing formation for distributor 462. Distributor mobile vault 426 corresponds to distributor 462. Merchant mobile wallet 424 and distributor mobile vault 426 can be stored in a database (e.g., database 108).

Although not depicted, various other modules from the architecture of Figures 1 and/or 2 can also be included electronic payment system 421. The modules expressly depicted in Figure 4 can interoperate with these other modules as appropriate to facilitate desired functionality.

Delivery personnel 406 can use invoicing application 412 to interact with electronic payment system 421 in a limited way on behalf of distributor 462. Upon delivery of goods 403 to retail location 402, delivery personnel can also deliver an invoice to merchant 407. In some embodiments, the invoice is a paper invoice, such as,

for example, invoice 461. Invoice 461 indicates that goods 403 were purchased for amount 463.

In other embodiments, the invoice is an electronic invoice. For example, delivery personnel 406 can use invoicing application 412 to send invoice submission data 429 to invoice processor 423. (Alternatively, the invoice submission data 429 may be sent via a batch file from distributor 462). Invoice processor 423 can receive invoice submission data 429 from invoicing application 412. Invoice submission data 429 can indicate that goods 403 are valued at a specified amount and were physically delivered retail location 402. Invoice processor 423 can refer to distributor invoicing data 428. Invoice processor 423 can generate electronic invoice 431 based on the invoice submission data 429 and the distributor invoicing data 428. Invoice processor 423 can submit electronic invoice 431 to merchant mobile phone 408 on behalf of distributor 462. Electronic invoice 431 indicates that goods 403 were purchased for amount 463. Invoice processor 423 can record generation of invoice 431 in distributor mobile vault 426.

Mobile wallet application 411 can receive invoice 431 from electronic payment system 421. In response to receiving invoice 431, mobile wallet application 411 can indicate receipt of invoice 431 at a user-interface (e.g., display screen) of merchant mobile phone 408.

Upon receiving an invoice (whether it be a paper invoice or an electronic invoice) merchant 407 can log into electronic payment system 421 and access merchant mobile wallet 424 through mobile wallet application 411. Merchant 407 can enter commands through a user-interface (e.g., touch screen or keypad) to request that the invoice (e.g., invoice 461 or invoice 431) be paid partially or in full. Mobile wallet application 411 can send payment instructions 432 to payment processor 422. Payment instructions 432 indicate that amount 463 is to be paid from merchant 407 to distributor 462. Payment processor 422 can validate that the balance of funds in merchant mobile wallet 424 is sufficient to pay amount 463. When the balance of funds is sufficient, payment processor 422 s debits 441 amount 463 from merchant mobile wallet 424 and credits 442 amount 463 to distributor mobile wallet 427.

Payment processor 422 indicates to invoice processor 423 that invoice 431 or invoice 461 was paid as appropriate. Invoice processor 423 receives the indication that invoice 431 or invoice 461 was paid. Invoice processor 423 records the indication that invoice 431 or invoice 461 was paid in the distributor mobile vault 426. Payment

processor 422 (or a separate notification module) can send payment received notification 434 (e.g., a receipt) to mobile wallet application 411. Mobile wallet application 411 can present payment received notification 434 to merchant 407 through a user-interface (e.g., a display screen). Accordingly, merchant 407 is provided verification when an invoice is paid.

Payment processor 422 (or the separate notification module) can send payment received notification 433 to invoicing application 412. Invoicing application 412 can present payment received notification 433 to delivery personnel 406 through a user-interface (e.g., a display screen). Accordingly, delivery personnel 406 are provided verification when an invoice is paid. In response to seeing presentation of payment received notification 433, delivery personnel 406 can leave retail location 402 and delivery other goods to a next delivery stop or return to distribution center 401. The transaction is efficient and saves time relative to a currency based transaction. Accordingly, delivery personnel 406 can makes more deliveries in a specified time period (e.g., a shift or a day).

The features of mobile telephone applications, such as, for example, mobile wallet application 411 and invoice application 412, can be adjusted for mobile telephone capabilities. For example, a lower function, "basic" mobile wallet application may be configured to work on lower capability mobile phones. The basic mobile wallet application can be used for merchant mobile wallet payment for goods. The basic application can provide electronically time-stamped authentication and authorization of payment and automatic deposit.

An "enhanced" mobile wallet application can be configured to work on higher capability mobile phones such as smart phones and tablets. In addition to features of the basic application, the enhanced application also has the capability to tie into a distributor's inventory to produce other features, including: automatic notification to merchant of pending delivery, automatic notification of delays, real-time inventory adjustments that re-calculate the amount due, and automatically close out accounts receivable ("A/R") account upon completion of a transaction.

In addition to linking existing bank accounts to the mobile wallet, the electronic payment system 421 maintains a stored value account for real-time payment of services. For at least some implementations, the electronic payment system may partner with a local bank to provide pre-paid stored value accounts for each mobile wallet (including the

distributor's mobile wallet, the delivery person's mobile wallet (which may be the same as or an extension of the distributor's mobile wallet), and the merchant's mobile wallet. These stored value accounts provide the basis for the exchange of funds between each of the program participants, whether they are distributors, merchants, consumers, agents, or companies providing services on the platform.

A partner bank is used to hold all of the stored value accounts and support settlements between the accounts. Agents deposit funds into and withdraw funds from the bank directly. Distributors, merchants, and consumers interact with agents to deposit and withdraw funds. Integration into a partner bank supports the activation and maintenance of each of the stored value accounts. While the electronic payment system 421 manages the real-time balance of each end-user stored value account, the platform interacts with the bank to move funds from one account to the other as a means of settling the transactions. The partner bank also supports settlement with program participants who don't have an account with the partner bank. The partner bank may support settlements with payment gateways, bill payment providers, and international remittance providers.

Other financial service providers such as bill payment aggregators and international remittance providers are also integrated into the electronic payment system 421. These service providers offer end-users the ability to pay their bills and send money to others. The recipients don't necessarily need to be subscribers to the program to receive their funds (as explained above with regard to Figure 3B). International remittance providers support the ability to both send money as well as receive money transfers in real time into the stored value accounts.

A reconciliation report may be generated and accessible through a portal provided by the electronic payment system 421 to ensure delivery personnel invoices (431) and receipts (433) are reconciled with merchant orders and inventory. The electronic payment system 421 also allows users to view the account balance and transaction history of the driver account and distribution center stored value accounts. Delivery personnel/distributors are able to receive and process payments for client products from merchants using cash, credit cards, debit cards, or a mobile wallet stored value account. Delivery personnel/distributors have the ability to deposit cash in nearby banks or with program agents in order to limit the amount of cash on hand as they complete their deliveries.

Merchants establish a stored value account with their mobile wallet 411 that can be used to make mobile payments to distributors or receive payments from consumers using cash, credit cards, debit cards, or a mobile wallet platform stored value account. The mobile wallet application 411 allows merchants to make electronic bill payments or transfer money from their mobile phone on behalf of customers who have not registered for the client mobile wallet stored value account.

In addition to processing financial transactions, the merchant's mobile wallet account applications allow them to manage their user profile including the linking and unlinking of payment instruments such as credit cards and checking accounts, updating their personal information including address, password and PIN, and methods by which the platform sends receipts, alerts and reminders. Changes made on any channel are updated and stored in the subscriber profile and are applied to each channel (i.e. – a password update on a mobile wallet application applies also to the Web client or USSD client).

The electronic payment system 421 works with all of the program participants to manage fraud and unauthorized access to data on the platform. Every transaction on the electronic payment system 421 is considered an auditable event and is stored with the account information of the person executing the transaction, a unique transaction ID, and time stamp. This data is aggregated on a centralized logging server where it is indexed and made available for reporting and fraud research. Likewise, periodic (e.g. daily) reports are generated to highlight suspicious activity based on patterns, thresholds, and velocities. The electronic payment system 421 also utilizes real-time transactions monitoring and filtering by validating transaction limits and velocities of every transaction to diminish fraudulent usage.

In one embodiment, as described in the flowchart 500 of Figure 5, a computer system is provided. The computer system may be any type of computing device that has one or more processors and some type of memory. The computer system also includes a computer-readable medium that has computer-executable instructions stored on it that, when executed by the one or more processors, causes the computer system to perform a method for allowing a merchant to pay a distributor for delivered goods using an electronic payment system. The method includes receiving a payment instruction 432 from a merchant 407 in step 510. The payment instruction indicates that a distributor's invoice for a specified amount 463 is to be paid from the merchant's mobile wallet 411.

The invoice is generated for goods 403 that were physically delivered from the distributor 462 to the merchant 407. At least in this embodiment, both the merchant and the distributor have mobile wallets (411 and 427, respectively). In other embodiments, one or the other may not be subscribers to the electronic payment system 421 and may not have a mobile wallet.

The electronic payment system 421 validates that the merchant's mobile wallet 411 has a balance of funds sufficient to pay the amount 463 specified in the invoice 431 in step 520, and debits the merchant's mobile wallet by the specified amount of funds in step 530. The electronic payment system 421 then credits the distributor's mobile wallet by the specified amount of funds in step 540 and sends a notification 433 to the distributor indicating that the invoice has been paid in step 550. Accordingly, a business may be able to pay an invoice using a mobile wallet quickly and seamlessly. The delivery person / distributor thus does not have to deal with cash (at least in this transaction), and can avoid the logistical hassles of physical cash.

Thus, in general, a mobile vault and corresponding applications, enable a distributor to accept mobile wallet payments from merchants, increasing the number of merchants drivers can reach within a day while reducing the amount of cash transactions per route. Moreover, a merchant mobile wallet can be used for additional services such as remittances, bill payments, airtime top-up and purchases.

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, 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.

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. 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.

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 electronic payment system can perform AML and CFT checks on all electronic financial transactions to ensure that 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 electronic payment system within the allowable limits.

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.

CLAIMS

What is claimed:

1. A computer system comprising the following:

one or more processors;

system memory;

one or more computer-readable storage media having stored thereon computer-executable instructions that, when executed by the one or more processors, causes the computing system to perform a method for allowing a merchant to pay a distributor for delivered goods using an electronic payment system, the method comprising the following:

receiving a payment instruction from a merchant, the payment instruction indicating that a distributor's invoice for a specified amount is to be paid from the merchant's mobile wallet, the invoice being generated for one or more goods physically delivered from the distributor to the merchant, the merchant and the distributor both having mobile wallets;

validating that the merchant's mobile wallet has a balance of funds sufficient to pay the amount specified in the invoice;

debiting the merchant's mobile wallet by the specified amount of funds;

crediting the distributor's mobile wallet by the specified amount of funds; and

sending a notification to the distributor indicating that the invoice has been paid.

2. The computer system of claim 1, wherein the merchant's payment instruction is received from the merchant's mobile device using wireless communication.

3. The computer system of claim 2, further comprising sending a payment received notification to the merchant's mobile device.

4. The computer system of claim 1, wherein the indication sent to the distributor is sent to the distributor's mobile device using wireless communication.

5. The computer system of claim 1, wherein the distributor's invoice is submitted to the merchant's mobile device by a delivery person on behalf of the distributor.

6. The computer system of claim 5, further comprising, prior to receiving the payment instruction from the merchant mobile device, receiving invoice submission data from the delivery person's mobile device using wireless communication, the invoice submission data indicating that the merchant is to be invoiced in the specified amount for the physically delivered goods.

7. The computer system of claim 6, further comprising sending an electronic invoice to the merchant's mobile device in response to receiving a request from the merchant and in response to receiving the invoice submission data from the delivery person on behalf of the distributor, the electronic invoice indicating that the merchant owes the distributor the specified amount for the physically delivered goods.

8. The computer system of claim 7, wherein receiving a payment instruction from a merchant mobile device using wireless communication comprises receiving a payment instruction indicating that the electronic invoice is to be paid from the merchant's mobile wallet.

9. The computer system of claim 7, wherein receiving a payment instruction from the merchant mobile device using wireless communication comprises receiving a payment instruction indicating that a paper invoice is to be paid from the merchant's mobile wallet.

10. The computer system of claim 1, further comprising sending the merchant an additional notification notifying the merchant of a pending delivery.

11. The computer system of claim 10, wherein the additional notification indicates a delivery date and time window in which the deliver is to occur.

12. The computer system of claim 11, wherein subsequent notifications are sent to the merchant automatically upon the occurrence of a delay.

13. The computer system of claim 1, further comprising sending the merchant a real-time inventory adjustments notification that indicates the merchant's newly received goods.

14. The computer system of claim 1, further comprising automatically closing out a merchant accounts receivable (A/R) account upon completion of the transaction.

15. The computer system of claim 1, wherein the electronic payment system utilizes an internal processor to maintain individual merchant mobile wallet balances in addition to distributor mobile wallet balances.

16. A mobile payment platform, the mobile payment platform including:

an electronic payment system, the electronic payment system including one or more computer storage devices having stored thereon computer executable instructions representing a payment processor, an invoice processor, a merchant mobile wallet, and a distributor mobile vault, the distributor mobile vault including a distributor mobile wallet and distributor invoicing data, the merchant mobile wallet for a merchant, the distributor mobile vault for a distributor;

a distributor mobile device, the distributor mobile device including one or more computer storage devices having stored thereon computer executable instructions representing an invoicing application; and

an merchant mobile device, the merchant mobile device including one or more computer storage devices having stored thereon computer executable instructions representing a mobile wallet application; and

wherein the invoice processor is configured to:

receive invoice submission data from the distributor's mobile device, the invoice submission data indicating that goods valued at a specified amount were physically delivered to the merchant;

generate an electronic invoice based on the invoice submission data;

submit the generated electronic invoice to the merchant's mobile device;

record generation of the electronic invoice in the distributor's mobile vault;

receive an indication that an electronic invoice has been paid; and

record the indication that the electronic invoice has been paid in the distributor's mobile vault.

17. The mobile payment platform of claim 16, wherein the payment processor is configured to:

receive a payment instruction from a merchant, the payment instruction indicating that a distributor's invoice for a specified amount is to be paid from the merchant's mobile wallet, the invoice being generated for one or more goods physically delivered from the distributor to the merchant, the merchant and the distributor both having mobile wallets;

validate that the merchant's mobile wallet has a balance of funds sufficient to pay the amount specified in the invoice;

debit the merchant's mobile wallet by the specified amount of funds;

credit the distributor's mobile wallet by the specified amount of funds; and

send a notification to the distributor indicating that the invoice has been paid.

18. The mobile payment platform of claim 16, wherein the generated electronic invoice is submitted to the merchant's mobile device by a delivery person on behalf of the distributor.

19. The mobile payment platform of claim 16, the merchant uses the mobile payment platform for performing at least one of the following in addition to making payments for received goods: bill payments, remittances, mobile phone airtime top-up and retail purchases.

20. A mobile payment platform, the mobile payment platform including:

an electronic payment system, the electronic payment system including one or more computer storage devices having stored thereon computer executable instructions representing a payment processor, an invoice processor, a merchant mobile wallet, and a distributor mobile vault, the distributor mobile vault including a distributor mobile wallet and distributor invoicing data, the merchant mobile wallet for a merchant, the distributor mobile vault for a distributor;

a distributor mobile device, the distributor mobile device including one or more computer storage devices having stored thereon computer executable instructions representing an invoicing application; and

an merchant mobile device, the merchant mobile device including one or more computer storage devices having stored thereon computer executable instructions representing a mobile wallet application; and

wherein the invoice processor is configured to:

receive invoice submission data from the distributor's mobile device, the invoice submission data indicating that goods valued at a specified amount were physically delivered to the merchant;

generate an electronic invoice based on the invoice submission data;

submit the generated electronic invoice to the merchant's mobile device;

record generation of the electronic invoice in the distributor's mobile vault;

receive an indication that an electronic invoice has been paid; and

record the indication that the electronic invoice has been paid in the distributor's mobile vault; and

wherein the payment processor is configured to:

receive a payment instruction from a merchant, the payment instruction indicating that a distributor's invoice for a specified amount is to be paid from the merchant's mobile wallet, the invoice being generated for one or more goods physically delivered from the distributor to the merchant, the merchant and the distributor both having mobile wallets;

validate that the merchant's mobile wallet has a balance of funds sufficient to pay the amount specified in the invoice;

debit the merchant's mobile wallet by the specified amount of funds;

credit the distributor's mobile wallet by the specified amount of funds; and

send a notification to the distributor indicating that the invoice has been paid.

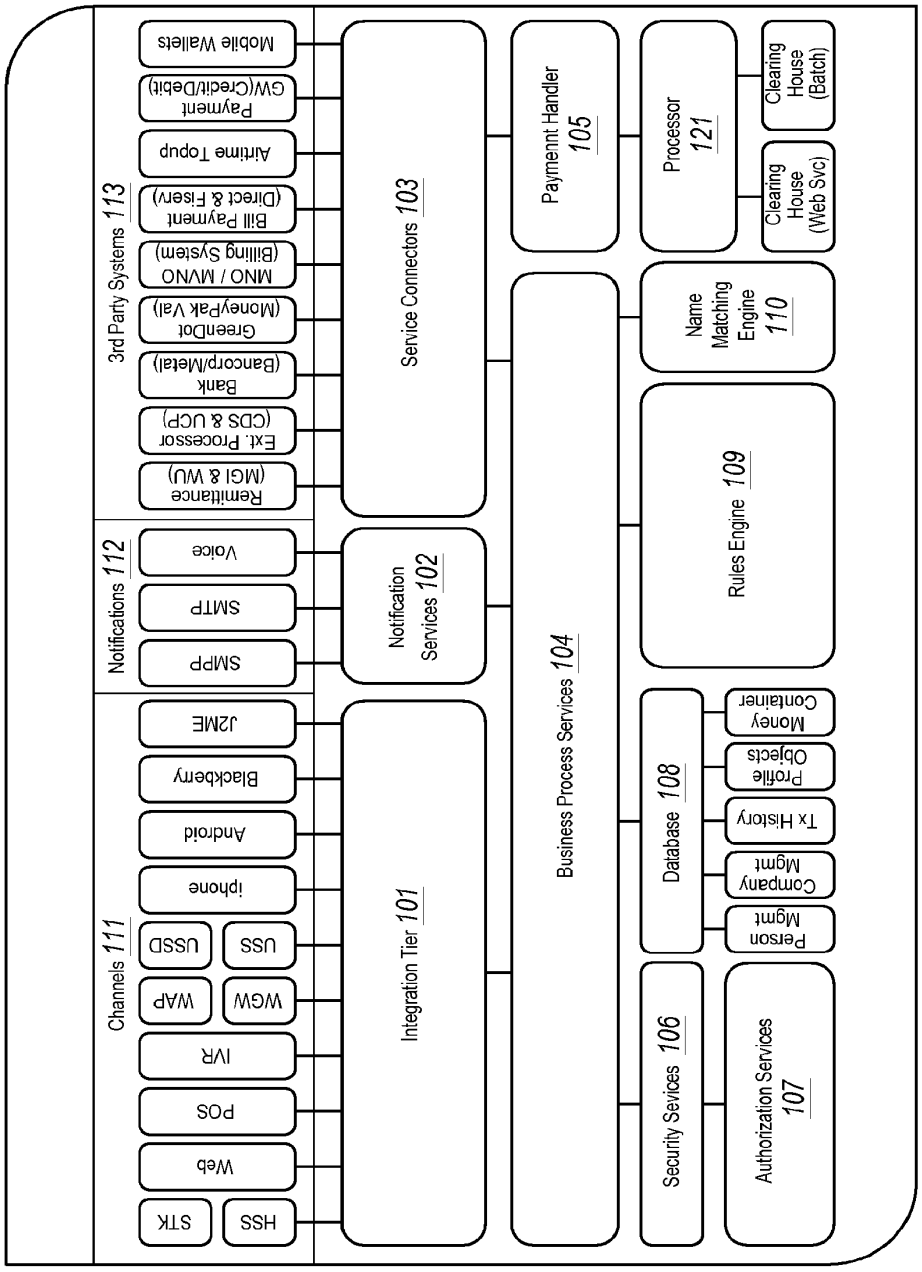

Platform Functional Architecture
Channels 111
HSS
STK
Web
POS
IVR
WGW
WAP
USS
USSD
iphone
Android
Blackberry
J2ME
Notifications 112
SMPP
SMTP
Voice
3rd Party Systems 113
Remittance (MGI & WU)
Ext. Processor (CDS & UCP)
Bank (Bancorp/Metal)
GreenDot (MoneyPak Val)
MNO / MVNO (Billing System)
Bill Payment (Direct & Fiserv)
Airtime Topup
Payment GW(Credit/Debit)
Mobile Wallets
Integration Tier 101
Notification Services 102
Service Connectors 103
Business Process Services 104
Paymennt Handler 105
Security Sevices 106
Authorization Services 107
Database 108
Person Mgmt
Company Mgmt
Tx History
Profile Objects
Money Container
Rules Engine 109
Name Matching Engine 110
Processor 121
Clearing House (Web Svc)
Clearing House (Batch)

FIG. 1

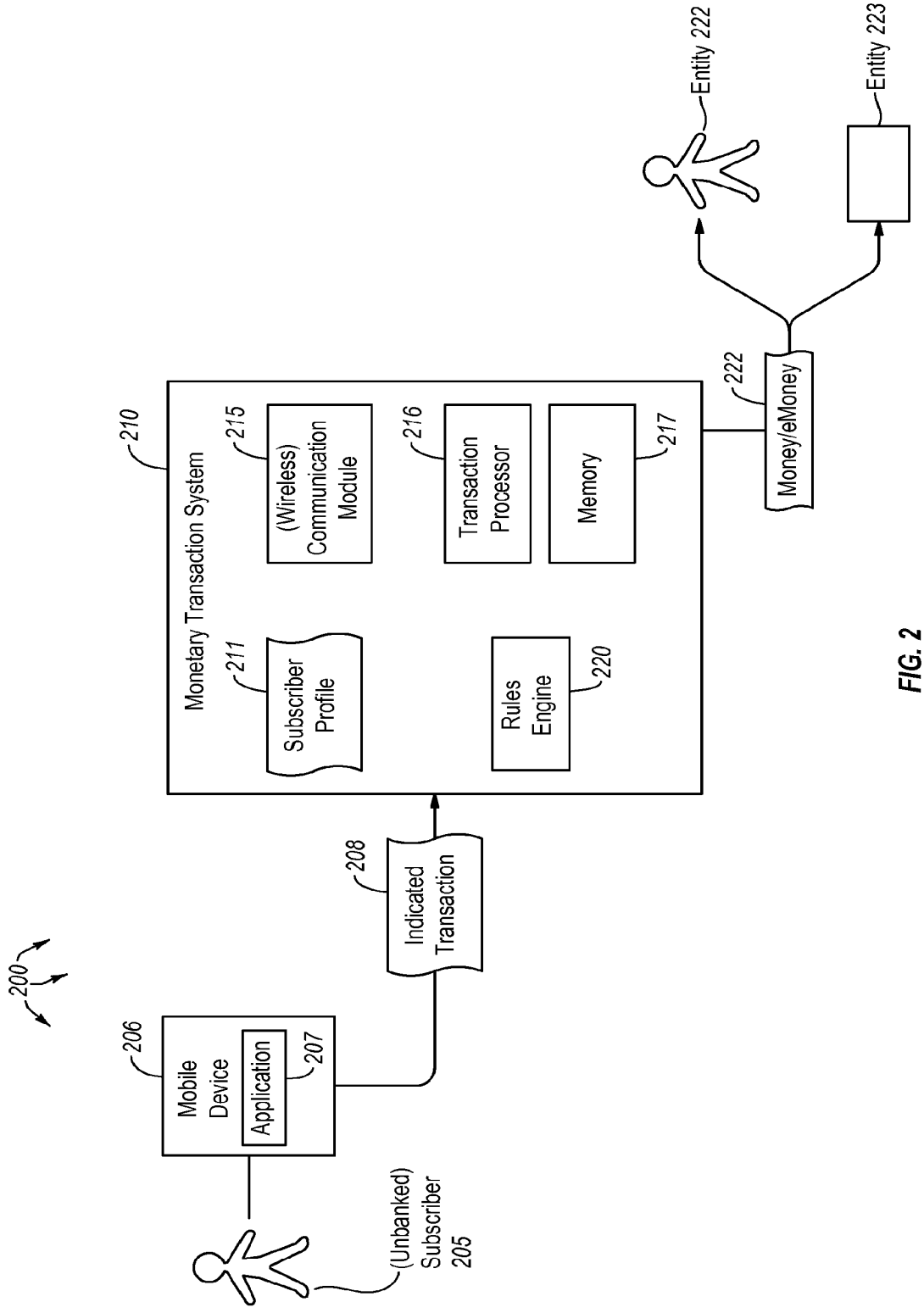
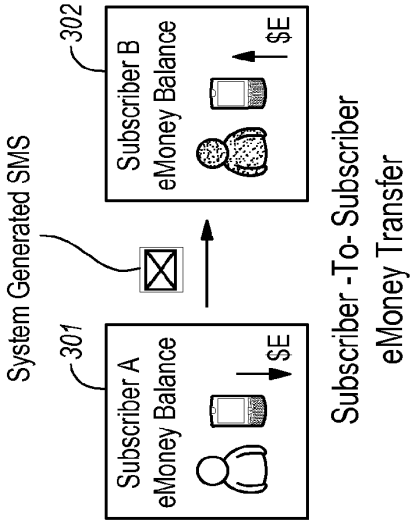
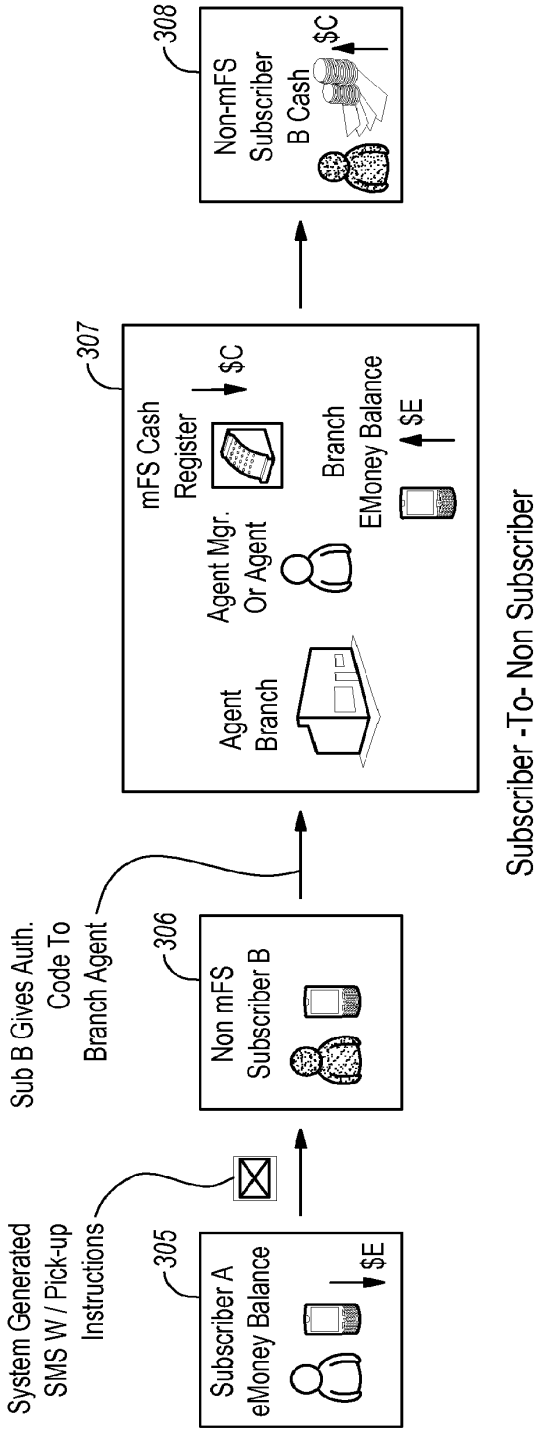

200
206
Mobile Device
Application
207
(Unbanked) Subscriber 205
208
Indicated Transaction
210
Monetary Transaction System
211
Subscriber Profile
215
(Wireless) Communication Module
216
Transaction Processor
217
Memory
220
Rules Engine
222
Money/eMoney
Entity 222
Entity 223

FIG. 2



Subscriber -To- Subscriber
eMoney Transfer

FIG. 3A



Subscriber -To- Non Subscriber
eMoney Transfer

FIG. 3B

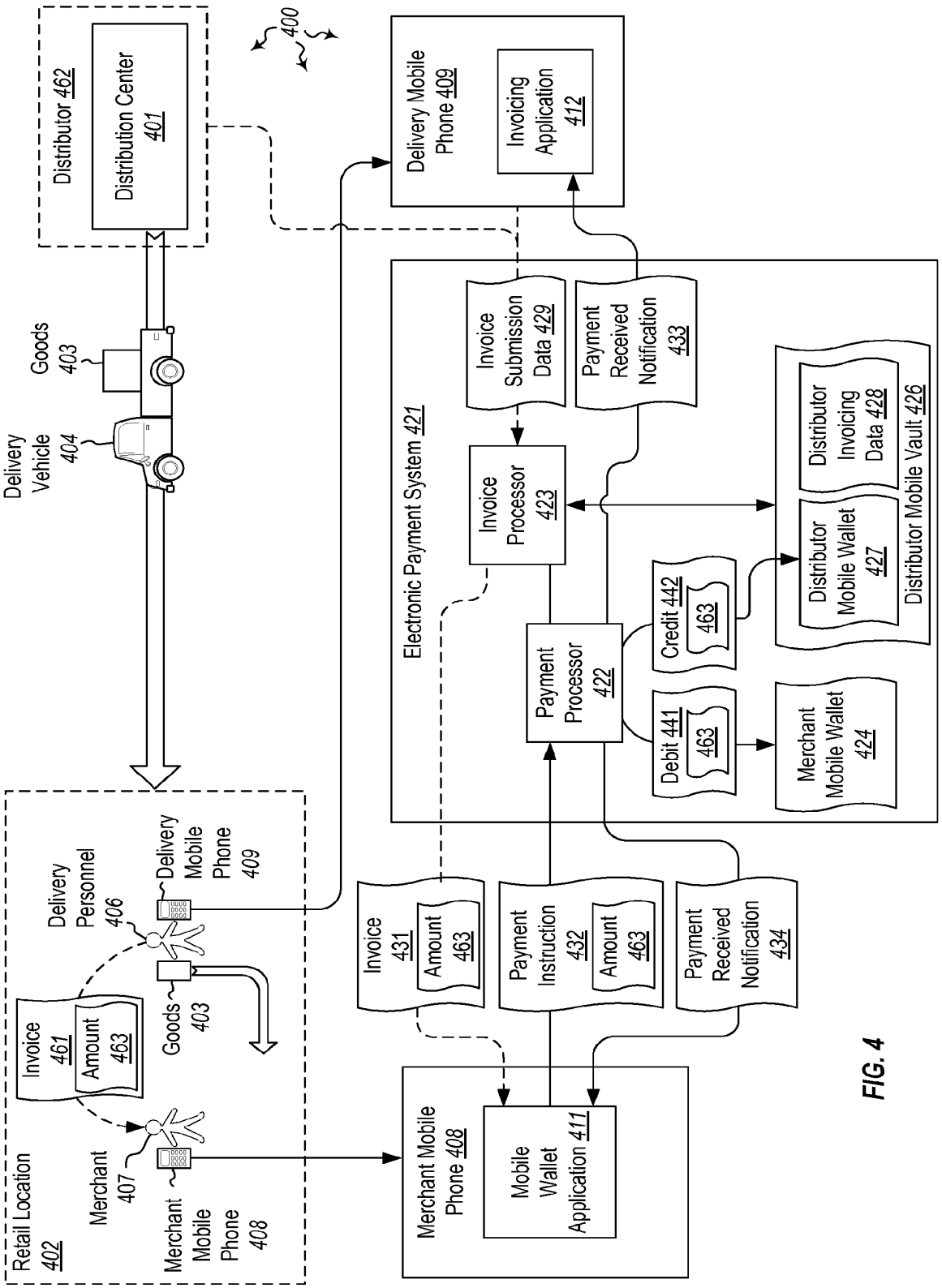

400
Distributor 462
Distribution Center 401
Goods 403
Delivery Vehicle 404
Delivery Mobile Phone 409
Invoicing Application 412
Electronic Payment System 421
Invoice Submission Data 429
Payment Received Notification 433
Invoice Processor 423
Distributor Invoicing Data 428
Distributor Mobile Wallet 427
Distributor Mobile Vault 426
Credit 442
463
Payment Processor 422
Debit 441
463
Merchant Mobile Wallet 424
Retail Location 402
Delivery Personnel 406
Delivery Mobile Phone 409
Invoice 461
Amount 463
Goods 403
Merchant 407
Merchant Mobile Phone 408
Invoice 431
Amount 463
Payment Instruction 432
Amount 463
Payment Received Notification 434
Merchant Mobile Phone 408
Mobile Wallet Application 411

FIG. 4

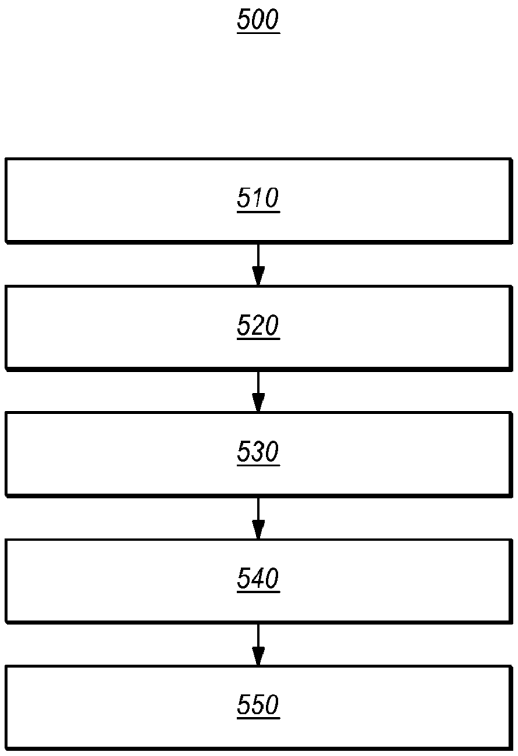


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 12/43321

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 20/00 (2012.01)
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 (2012.01)
USPC: 705/78

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/64; 235/379 (keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST (PGPB, USPT, EPAB, JPAB); Google Scholar; Google Patents; FreePatentsOnline. Search terms used: mobile-wallet mobile-payment electronic-wallet electronic-payment mobile-purse electronic-purse wallet-funds purse-funds wallet-available purse-available wallet-balance purse-balance mobile-vault wallet-sufficient...

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008/0275779 A1 (LAKSHMINARAYANAN) 06 November 2008 (06.11.2008) entire document, especially Abstract; Figs. 6, 8; para [0006], [0023], [0031], [0033], [0041], [0047], [0054], [0056]-[0059], [0062], [0073], [0075], [0077], [0081], [0083], [0092], [0096], [0105], [0131], [0133]	1 - 20
Y	US 2007/0255620 A1 (TUMMINARO et al.) 01 November 2007 (01.11.2007) entire document, especially Abstract; para [0021], [0187], [0202], [0203], [0208], [0255], [0256], [0258], [0367]-[0372], [0590], [0702], [0739], [0882], [1135]	1 - 20
A	US 2010/0030651 A1 (MATOTEK et al.) 04 February 2010 (04.02.2010) 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 August 2012 (09.08.2012)	06 SEP 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

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

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2013 (17.01.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/009446 A1

(51) International Patent Classification:
G06Q 30/00 (2012.01)

(21) International Application Number:
PCT/US2012/043458

(22) International Filing Date:
21 June 2012 (21.06.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/499,927	22 June 2011 (22.06.2011)	US
61/522,099	10 August 2011 (10.08.2011)	US
13/484,199	30 May 2012 (30.05.2012)	US
13/528,720	20 June 2012 (20.06.2012)	US

(71) Applicant *(for all designated States except US)*: **MOZIDO, LLC** [US/US]; 1950 Stemmons Freeway, Suite 6040, Dallas, TX 75207 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LIBERTY, Michael, A.** [US/US]; 5373 Isleworth Country Club Drive, Windermere, FL 34786 (US).

(74) Agents: **STRINGHAM, John, C.** et al.; 60 East South Temple, Suite 1000, Salt Lake City, UT 84111 (US).

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

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

Published:

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

(54) Title: DISRUPTIVELY PRICED OR FREE FINANCIAL SERVICES OR ITEMS IN EXCHANGE FOR PARTICIPATION IN OPT IN ADVERTISING

Platform Functional Architecture

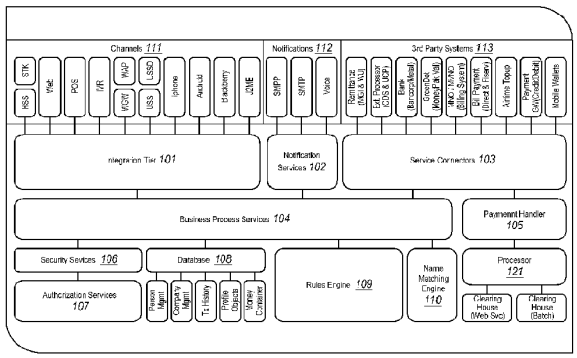


FIG. 1

(57) Abstract: Embodiments are directed to providing disruptively priced or free financial services or goods in exchange for participation in opt-in advertising. A user may opt-in to receive some form of advertising on his or her phone. The advertising may appear in a mobile wallet application used to pay for goods or services. The advertising may be related to products the user has previously purchased using the mobile wallet application. An electronic payment system that provides the mobile wallet application tracks and stores items that the user purchases using the mobile wallet. The electronic payment system then analyzes the user's purchasing habits to identify advertisements and/or promotions that may be of interest to the user. The promotions (such as coupons) may then be sent to the user's mobile wallet application and applied automatically when the user purchases that item using the mobile wallet.

WO 2013/009446 A1

DISRUPTIVELY PRICED OR FREE FINANCIAL SERVICES OR ITEMS IN EXCHANGE FOR PARTICIPATION IN OPT IN ADVERTISING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of U.S. Utility Application Ser. No. 13/528,720, filed on June 20, 2012, entitled "Disruptively Priced or Free Financial Services or Items in Exchange for Participation in Opt In Advertising", and claims priority to and the benefits of U.S. Provisional Application Ser. No. 61/499,927, filed on June 22, 2011, entitled "Disruptively Priced or Free Financial Services or Items in Exchange for Participation in Opt In Advertising", which are incorporated herein by reference in their entirety. This application further claims priority to and the benefit of U.S. Patent Application Ser. No. 13/484,199, entitled "Monetary Transaction System", filed on May 30, 2012, which itself claims priority to U.S. Provisional Application Ser. No. 61/522,099, filed on August 10, 2011, entitled "Mobile Wallet Platform", and U.S. Provisional Application Ser. No. 61/493,064, filed on June 3, 2011, entitled "Mobile Wallet Platform". Each of the aforementioned applications is incorporated by reference herein in its entirety.

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 actions 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.

BRIEF SUMMARY

[0003] Embodiments described herein are directed to providing disruptively priced or free financial services or items in exchange for participation in opt-in advertising. A user may opt-in to receive some form of advertising on his or her phone. The advertising may appear in a mobile wallet application used to pay for goods or services. The advertising

may be related to products the user has previously purchased using the mobile wallet application. The user has an account with a mobile payment system that provides the mobile wallet application. The mobile payment system can provide the user with a variety of functionality including purchasing items along with one or more of depositing funds, withdrawing funds, transferring funds, etc. Accordingly, the user can use a digital device (e.g., a computer or mobile phone) to interact with the electronic payment system to pay for goods and/or services.

[0004] In exchange for a financial benefit, the user opts in to receive advertisements, coupons, vouchers, promotions, Buy One Get One ("BOGO") offers or other benefits from the electronic payment system. Upon the user's agreement to participate in opt-in advertising, the electronic payment system may be permitted to store (e.g., by capturing purchase orders), track, and analyze items that the user purchases through their account with the electronic payment system. The electronic payment system stores and maintains a list of a user's purchased items in a data warehouse. The electronic payment system then analyzes the user's purchasing habits to identify advertisements and/or promotions that may be of interest to the user. The promotions (such as coupons) may then be sent to the user's mobile wallet application and applied automatically when the user purchases that item using the mobile wallet.

[0005] 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.

[0006] 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.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] 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:

[0008] Figure 1 illustrates a monetary transaction system architecture in which embodiments described herein may operate.

[0009] Figure 2 illustrates an alternate example embodiment of a monetary transaction system.

[0010] Figures 3A and 3B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber eMoney transfers via a mobile wallet, respectively.

[0011] Figure 4 illustrates an example data flow for making a retail purchase using a mobile wallet.

[0012] Figure 5 illustrates a monetary transaction system architecture in which free or reduced price items may be provided in exchange for opt-in advertising.

[0013] Figure 6 illustrates an example data flow for providing free or reduced price items in exchange for participation in opt-in advertising.

[0014] Figure 7 illustrates an example screen shot of a mobile wallet application with opt-in advertisements.

DETAILED DESCRIPTION

[0015] Embodiments described herein are directed to providing disruptively priced or free financial services or items in exchange for participation in opt-in advertising. A user may opt-in to receive some form of advertising on his or her phone. The advertising may appear in a mobile wallet application used to pay for goods or services. The advertising may be related to products the user has previously purchased using the mobile wallet application. The user has an account with a mobile payment system that provides the mobile wallet application. The mobile payment system can provide the user with a variety of functionality including purchasing items along with one or more of depositing funds, withdrawing funds, transferring funds, etc. Accordingly, the user can use a digital device (e.g., a computer or mobile phone) to interact with the electronic payment system to pay for goods and/or services.

[0016] In exchange for a financial benefit, the user opts in to receive advertisements, coupons, vouchers, promotions, Buy One Get One ("BOGO") offers or other benefits from the electronic payment system. Upon the user's agreement to participate in opt-in advertising, the electronic payment system may be permitted to store (e.g., by capturing purchase orders), track, and analyze items that the user purchases through their account with the electronic payment system. The electronic payment system stores and maintains a list of a user's purchased items in a data warehouse. The electronic payment system then analyzes the user's purchasing habits to identify advertisements and/or promotions that may be of interest to the user. The promotions (such as coupons) may then be sent to the user's mobile wallet application and applied automatically when the user purchases that item using the mobile wallet.

[0017] Embodiments 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.

[0018] Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change 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.

[0019] 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.

[0020] 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.

[0021] 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.

[0022] 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.

[0023] 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 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.

[0024] 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.

[0025] 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.

[0026] 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.

[0027] Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a 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.

[0028] Various terminology will be used herein to describe the monetary transaction system (also referred to as a "mobile wallet platform", "mobile wallet program", "mobile wallet transaction system", "mobile financial services (mFS) platform" or "electronic payment system"). The term "agent" is used to refer to an individual with 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.

[0029] 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 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.

[0030] 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.

[0031] 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. 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.

[0032] 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 mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

[0033] 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.

[0034] 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.

[0035] 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.

[0036] 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 distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

[0037] 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.

[0038] 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".

[0039] 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. 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.

[0040] 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. 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.

[0041] 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.

[0042] 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".

[0043] 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.

[0044] 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.

[0045] 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 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.

[0046] 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.

[0047] 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 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.

[0048] 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.

[0049] 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.

[0050] 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 the external processor. A Clearing House subsystem of transaction processor 121 can be used to exchange the financial information with a bank.

[0051] 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.

[0052] 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.

[0053] Figure 2 depicts a monetary transaction system 200 similar to that described in Figure 1. The monetary transaction system 200 may provide a more 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 know your customer (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.

[0054] 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.

[0055] 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 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).

[0056] 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.

[0057] 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.

[0058] 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.

[0059] 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 an electronic payment system or a third party), adding a bank/credit union account to a mobile wallet, adding a debit/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, making in store purchases from a mobile wallet, or transferring money or eMoney from one business account to another business account (i.e. from one business's mobile vault to another business's mobile vault, as will be shown in Figure 4).

[0060] Figure 3A depicts a subscriber-to-subscriber eMoney transfer. In a merchant and distributor scenario, either or both of the merchant and the distributor (including any delivery personnel) may be subscribers. To perform such a transfer, subscriber A (301) 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 (302). 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.

[0061] Figure 3B illustrates a subscriber-to-non-subscriber eMoney transfer. Accordingly, as mentioned above, either or both of the merchant and the distributor may be non-subscribers. In graphic 305, 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 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 (306). 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.

[0062] 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 (307) and the user leaves with the cash in hand (308). 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.

[0063] Figure 4 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 (401) and credits the agent branch's eMoney account (402). 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 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.

[0064] 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 channel 111. 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.

[0065] 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 and receives a subsequent agent branch communication over a channel indicating that the purchase code has been presented to an agent (branch). The monetary transaction system 210 validates the status of the specified payment method, determines if the specified payment method can accommodate a purchase for the specified amount, performs a limit check and/or a velocity check on the selected payment method, debits the specified payment method by the specified amount of funds, returns a notification to the agent branch authorizing the purchase and sends a receipt to the unbanked subscriber over a communication channel. The monetary transaction system 210 may thus be used in this manner to make a retail purchase using a mobile wallet.

[0066] Figure 5 depicts a physical environment and corresponding computer system architecture 500 for providing disruptively priced or free financial services or items in exchange for participation in opt-in advertising. The environment 500, like the scenarios described in Figures 3A, 3B and 4, involves the use of a mobile wallet application 511. The mobile wallet application 511 can be used to provide disruptively priced or free financial services or items in exchange for participation in opt-in advertising. The mobile wallet application may be run on any type of digital device including a mobile phone, tablet, laptop or other digital device. Embodiments include providing digital data (e.g., coupons or vouchers) for obtaining disruptively priced or free items (e.g., consumer goods or groceries) to such digital devices.

[0067] In some embodiments, a user has an account with a mobile payment system. The mobile payment system (e.g. 210 of Figure 2 or 521 of Figure 5) can provide the user 507 with a variety of functionality including purchasing items (see Figure 4), depositing funds, withdrawing funds, transferring funds (see Figures 3A and 3B), etc. Accordingly, the user can use a digital device to interact with the electronic payment system 521 to pay for goods and/or services.

[0068] In exchange for some type of financial benefit, the user opts in to receive advertisements. The financial benefits may include coupons, vouchers, promotions, Buy One Get One ("BOGO") offers or any other type of benefit (such as a reduced cost or free

financial service or good) from the electronic payment system. The benefit may be targeted to the user based on the user's age, location or other demographic information, or based on the user's past purchases. At least in some embodiments, when the user agrees to participate in opt-in advertising, the electronic payment system 521 is permitted to store (e.g., by capturing purchase orders), track, and analyze items that the user purchases through their account with the electronic payment system. The electronic payment system stores and maintains lists of the users' purchased items in a data warehouse. The electronic payment system may also store information about the user (anonymous or otherwise) including age, income level, an indication of whether kids are in the family, or other information that may be useful in targeting ads or benefits to the user.

[0069] The electronic payment system analyzes 534 the users purchasing habits to identify advertisements and/or promotions that may be of interest to the user. The advertisements and/or promotions can be for items the user has purchased 503. The advertisements and/or promotions can also be for items related to items the user has purchase. For example, if user has purchased a particular brand of razor, advertisements for the brand's shaving cream can be identified. Advertisements for related items can also be used for cross-promotion.

[0070] From time to time, at specified intervals, or based on location (e.g., having a coupon for a merchant this is with a specified proximity) the electronic payment system sends identified advertisements and/or promotions to the user's digital device. When specified advertising thresholds are satisfied (e.g., a specified number and/or type of advertisements and/or promotions are presented), the electronic payment system confers a financial benefit on the user's account. For example, the electronic payment system can provide the user's account with a low cost (e.g., reduced fee) or free financial service, such as, for example, one reduced cost bill pay or one free bill pay. Alternately, the electronic payment system can provide the user's account with a coupon or voucher for an item (e.g., an item a user has pre-selected or an item the user has purchased in the past).

[0071] In some embodiments, a client application for the electronic payment system runs on the user's digital device (e.g. mobile wallet application 511). The user interacts with the electronic payment system through the client application. From a screen of the client application, the user can agree to accept opt in advertising. Accordingly,

embodiments of the invention essentially permit a user to self-monetize themselves through their digital device.

[0072] As further depicted in Figure 5, computer architecture 500 includes digital device 508, retail location 502, and electronic payment system 521. Digital device 508 further includes mobile wallet application 511. Retail location 502 further includes its own mobile wallet application 512. Electronic payment system 521 includes marketing module 533, data warehouse 532, advertisements 538, payment processor 522, user mobile wallet 524 (user 507's mobile wallet), and merchant mobile wallet 526 (retail location 502's mobile wallet).

[0073] Generally, each company in packaged goods companies 571 (or retailers that sell the packaged goods or other goods or services) can send advertisement data to electronic payment system 521. Advertisements 538 represent the collection of advertisement data sent from packaged goods companies 571. Each company in packaged goods companies 571 can also submit benefit rules to electronic payment system 521. Benefit rules 578 represent the collection of benefit rules sent from packaged goods companies 571. Benefit rules 578 define when a benefit, such as, for example, a free financial service, a coupon, a promotion, etc, is to be granted to a user of electronic payment system 521. For example, in response to completing a questionnaire linked to a product advertisement, a user can be given a coupon for the product or for a related product.

[0074] In general, user 507 can use mobile wallet application 511 to pay for goods purchased at retail location 502 (as shown in Figure 4). For example, user 507 can use mobile wallet application 511 to purchase goods 503. To pay for goods 503, mobile wallet application 511 can send payment instruction 543 in amount 563 to electronic payment system 521. Payment processor 522 can receive payment instruction 543. In response, payment processor 522 can debit 541 user mobile wallet 524 by amount 563. Payment processor 522 can also credit 542 merchant mobile wallet 526 by amount 563.

[0075] User 507 can use mobile wallet application 511 to participate in opt-in advertising. For example, user 507 can use mobile wallet application 511 to send opt-in 544 to electronic payment system 521. Advertising module 533 can receive opt-in 544 and record that mobile wallet application 511 has opted in for advertising. As such, when user 507 makes a purchase using mobile wallet application 511, a list of purchased items

is sent to electronic payment system 521. For example, upon purchasing goods 503, item list 531 is sent to electronic payment system 521 and stored in data warehouse 532.

[0076] Propensity analysis module 534 can analyze user 507's purchases, including item list 531. From the analysis, propensity analysis module 534 can identify items or categories of items user 507 may be interested in. The items can be items user 507 has purchased in the past (e.g., an item in goods 503) or items related to items user 507 has purchases in the past. Propensity analysis module 534 can indicate identified items or categories of items to advertisement identification module 536. These identified items or categories are items that the user is likely interested in and, as such, may have a propensity toward buying these items. The propensity analysis module may use past purchases, personal preferences, lifestyle or demographic information or other data in the propensity analysis.

[0077] Advertisement identification module 536 can then select advertisements from advertisements 538 that correspond to the identified items or categories of items. For example, advertisement identification module 536 can select advertisement 546 for presentation at mobile wallet application 511. Advertisement 546 can be an advertisement for a product made by a company in packaged goods companies 571. Additionally or alternatively, the advertisement 546 may be created by the merchant and may advertise products or services sold by that merchant.

[0078] Advertising module 533 can send selected advertisements to mobile wallet application 511. For example, advertising module 533 can send advertisement 546 (e.g., related to an item in goods 503) to mobile wallet application 511. In general, advertisements can include interactive content. For example, advertisement 546 includes content 573. Content 573 can be a video, a link to a company website (e.g., for a company in packaged goods companies 571), a call to action (such as a questionnaire), or some other content user 507 can interact with through digital device 508. User 507 can interact with content 573, for example, responding to questions in content 573. Advertisement response 574 can indicate how user 507 has interacted with content 573. In one embodiment, a call to action may be to post an update on Facebook® or some other website such as a retail establishment ranking website. If the user makes such a post or performs some other call to action, the user may be rewarded with a benefit. That benefit may be related to the product about which the user posted on the various websites.

[0079] Based on advertisement response 574, benefit determination module 576 can determine if a benefit is to be conferred upon user 507. Benefit determination module 576 can refer to benefit rules 578 when making a determination whether or not to confer a benefit. Thus, when user 507 interacts with advertisement 546 in a specified way (e.g., completes a survey, watches a video, etc.), benefit rules 578 can indicate that a company benefit (e.g., benefit 577) is to be conferred upon user 507. For example, benefit determination module 576 can confer benefit 577 on user 507. When user 507 receives an advertisement for a razor, for instance, and answers a questionnaire on how often they shave, a razor manufacture can give user 507 a coupon for reduced cost or free razor blades.

[0080] When a benefit is to be conferred on a user, the benefit can be stored in the user's brand locker. For example, benefit determination module 576 can store benefit 577 in brand locker 572 (part of user mobile wallet 524). Benefit 577 can be a coupon, a reduced cost or free financial service, a voucher, a promotion, a free bill pay, etc.

[0081] Benefit determination module 576 can also track aggregate statistics, such as, for example, specified number and/or type of advertisements received, for advertisements presented at mobile wallet application 511. Benefits can also be conferred upon users based on the aggregate statistics. For example, benefit determination module 576 can confer a benefit upon user 507 in response to twenty advertisements being presented at mobile wallet application 511. Thus, conferred benefits can be company-specified benefits or can be electronic payment system-specified benefits. Electronic payment system 521 can notify a user when a benefit is conferred. For example, electronic payment system 521 can send benefit notification 547 to mobile wallet application 511 to indicate benefit 577 being stored in brand locker 572.

[0082] When user 507 makes subsequent purchases through user mobile wallet 524, electronic payment system 521 can automatically check brand locker 572 for benefits related to any purchases items. If benefits for an item are identified, user 507 can be notified through mobile wallet application 511. In some cases, if benefits are identified, those benefits can be applied automatically when the user purchases that item or service. Thus, if the benefit is a coupon or a buy one get one free offer, that benefit may be applied automatically when the user uses his or her mobile wallet application 511 to purchase that item. Accordingly, embodiments of the invention permit user 507 to self monetize digital device 508 through agreeing to participate in opt-in advertising.

[0083] Although not depicted, various other modules from the architecture of Figures 1 or 2 can also be included electronic payment system 521. The modules expressly depicted in Figure 5 can interoperate with these other modules as appropriate to facilitate desired functionality.

[0084] In one embodiment, as shown in Figure 6, a method 600 for providing reduced cost or free services or goods in exchange for participation in opt-in advertising is described. This method is further described in conjunction with the electronic payment system 521 of Figure 5, as well as the example screenshot of a mobile wallet application 711 illustrated in Figure 7.

[0085] Method 600 includes receiving an indication that user 507 is opting in to receive opt-in advertising from electronic payment system 521 in exchange for a reduced cost or free financial service (step 610). The user has a mobile wallet account 524 with the electronic payment system 521. Next, method 600 includes receiving a list of one or more items 531 that the user has purchased using the mobile wallet account 524 (step 620) and analyzing 534 the list of items to identify items or item categories in which the user may be interested (and which the user may have a propensity toward buying) (step 630). Method 600 further includes selecting one or more advertisements 546 based on the identified items or item categories (step 640) and sending the selected advertisements to mobile wallet application 511 (which is tied to the user's mobile wallet account 524) for use by the user (step 650). Method 600 then includes determining that the user's interactions 574 with the selected advertisements 543 warrant conferring a benefit 577 to the user 507 (step 660), where the benefit is selected from among a reduced cost or free financial service, a coupon, a voucher, and a buy one get one free offer, and then conferring the selected benefit 577 upon the user by sending the benefit to the user's mobile wallet application 511 (step 670).

[0086] After the benefit has been conferred upon the user, the user may use the benefit when purchasing a corresponding product or service. Accordingly, as shown in Figure 7, for example, if Ad 1 or Ad 2 (701) shows a name brand diaper and the user interacts with the ad in some way, the company that produces the diaper may send a coupon or other benefit to the user's mobile wallet 511. Then, when the user is at a retail location (e.g. 502), the user may purchase that name brand diaper using their mobile wallet (e.g. using the "Purchases" button 706). The coupon or other benefit sent by the diaper producer will be automatically applied at checkout, such that the user obtains the

diapers for a discounted price. Many different coupons or other benefits may be stored in the user's brand locker 572, and each of these may be applied automatically when the electronic payment system 521 determines that the user is purchasing that product or service.

[0087] Still further, as mentioned above, the user may use their mobile wallet application 711 to perform other tasks such as adding airtime to their phone (702), paying a bill (703), sending money to another party (704), transferring money (705) or withdrawing money (707) at an agent branch, for example. Many other functions may be provided by the mobile wallet application. As such, buttons 702-707 are merely examples of possible buttons. Moreover, the look and feel of mobile wallet application 711 may be as illustrated in Figure 7, or may be substantially different, or may be modified by the user. Accordingly, the layout shown in Figure 7 is just one example of a possible button and advertisement layout. Many such layouts are possible, and may be different for each phone or digital device.

[0088] Thus, using the electronic payment system 521, a user may opt in to receive opt-in advertising. Then, after receiving that advertising (and possibly after interacting with it), the user may be conferred a benefit. This benefit may be used to receive reduced cost or free financial services or goods. The benefit may be applied automatically as the user is purchasing that good or service.

[0089] 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, 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.

[0090] 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. 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.

[0091] 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 electronic payment system can perform AML and CFT checks on all electronic financial transactions to ensure that 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 electronic payment system within the allowable limits.

[0092] 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.

CLAIMS

What is claimed:

1. A computer system comprising the following:

one or more processors;

system memory;

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 providing a reduced cost or free financial service in exchange for participation in opt-in advertising, the method comprising the following:

receiving an indication that a user is opting in to receive opt-in advertising from an electronic payment system in exchange for a reduced cost or free financial service or good, the user having a mobile wallet account with the electronic payment system;

receiving a list of one or more items that the user has purchased using the mobile wallet account;

analyzing the list of items to identify items or item categories in which the user may be interested;

selecting one or more advertisements based on the identified items or item categories;

sending the selected advertisements to a mobile wallet application for the user that is tied to the user's mobile wallet account;

determining that the user's interactions with the selected advertisements warrant conferring a benefit to the user, the benefit being selected from among a reduced cost or free financial service or good, a coupon, a voucher, and a buy one get one free offer; and

conferring the selected benefit upon the user by sending the benefit to the user's mobile wallet application.

2. The computer system of claim 1, further comprising:

recording an indication that the benefit was conferred to the user such that the benefit can be used for subsequently purchased items; and

indicating that the benefit is available to the user by sending a message to the mobile wallet application for the user.

3. The computer system of claim 2, wherein recording an indication that the benefit was conferred to the user comprises storing the benefit in a brand locker associated with the user's mobile wallet account.

4. The computer system of claim 2, wherein recording an indication that the benefit was conferred to the user comprises recording a benefit defined by a producer of a product in an advertisement sent to the mobile wallet application.

5. The computer system of claim 1, wherein recording an indication that the benefit was conferred to the user comprises recording a benefit defined the electronic payment system.

6. The computer system of claim 1 wherein determining when the user's interactions with the selected advertisements warrants conferring a benefit to the user comprises determining that a benefit is to be conferred on the user based on the user participating in a call to action contained in the content of the advertisement.

7. The computer system of claim 1, wherein the electronic payment system is wirelessly connected to a plurality of mobile telephones their corresponding mobile wallet users.

8. The computer system of claim 1, wherein the mobile wallet application is running on a digital device.

9. The computer system of claim 3, wherein the digital device is a mobile telephone.

10. The computer system of claim 1, wherein the received list of one or more items is analyzed along with one or more other items previously purchased by the user to determine items or item categories in which the user may be interested.

11. The computer system of claim 1, further comprising receiving an indication that the user has redeemed the conferred benefit.

12. The computer system of claim 11, wherein the conferred benefit comprises a coupon for a specified item and wherein the coupon is applied automatically as the user pays for the specified item using the mobile wallet application.

13. A computer system comprising the following:

one or more processors;

system memory;

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 redeeming a benefit received for participation in opt-in advertising, the method comprising the following:

receiving a first indication from a user's mobile wallet that a user is attempting to pay for a good or service using a mobile wallet application;

validating the user's mobile wallet account to ensure that the user's mobile wallet account has sufficient funds to pay for the specified good or service;

receiving a second indication from the user's mobile wallet application that a specified benefit is to be applied for the purchase of the good or service;

determining that the specified benefit applies to the indicated good or service; and

applying the specified benefit to the indicated good or service, such that the user purchases the indicated good or service at a price reduced by the amount of the benefit.

14. The computer system of claim 13, wherein the specified benefit is applied automatically as the user purchases the indicated good using the mobile wallet application.

15. The computer system of claim 13, further comprising sending a notification to the user indicating that the specified benefit was applied to the purchase of the indicated good.

16. The computer system of claim 13, further comprising sending a notification to the producer of the good indicating the benefit was applied to the purchase of producer's good.

17. The computer system of claim 16, wherein the producer of the good provides an additional benefit to the user for purchasing the producer's goods.

18. The computer system of claim 17, wherein the additional benefit is stored in a brand locker in the user's mobile wallet application.

19. A computer system comprising the following:

one or more processors;

system memory;

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 redeeming a coupon received for participation in opt-in advertising, the method comprising the following:

receiving a first indication from a user's mobile wallet that a user is attempting to pay for a good or service using a mobile wallet application;

validating the user's mobile wallet account to ensure that the user's mobile wallet account has sufficient funds to pay for the specified good or service;

receiving a second indication from the user's mobile wallet application that the coupon is to be applied for the purchase of the good or service;

determining that the coupon applies to the indicated good or service; and

applying the coupon to the indicated good or service, such that the user purchases the indicated good or service at a price reduced by the amount of the coupon.

20. The computer system of claim 19, wherein coupons stored in the user's brand locker are automatically applied when purchasing the coupon's corresponding product or service.

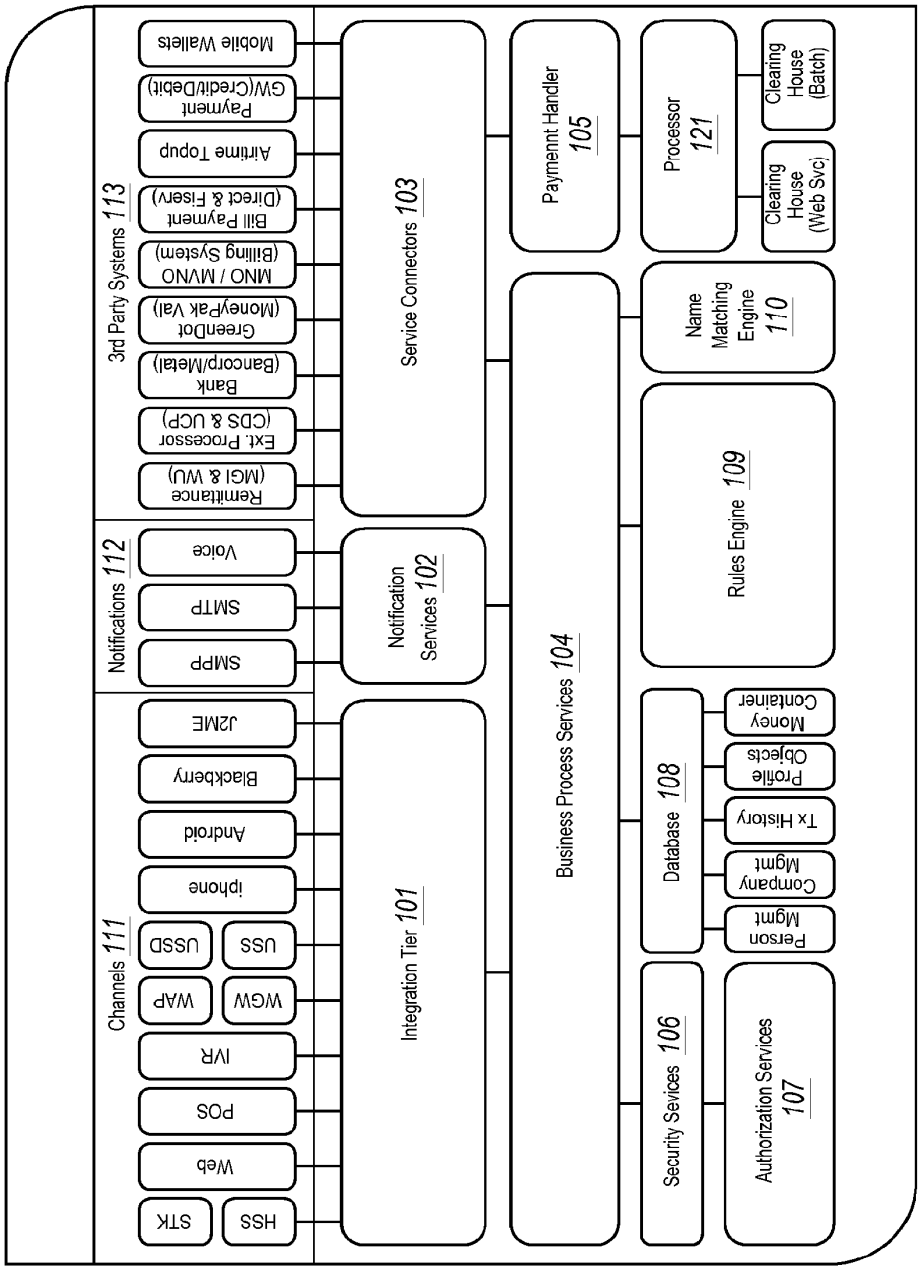

Platform Functional Architecture
Channels 111
HSS
STK
Web
POS
IVR
WGW
WAP
USS
USSD
iphone
Android
Blackberry
J2ME
Notifications 112
SMPP
SMTP
Voice
3rd Party Systems 113
Remittance (MGI & WU)
Ext. Processor (CDS & UCP)
Bank (Bancorp/Metal)
GreenDot (MoneyPak Val)
MNO / MVNO (Billing System)
Bill Payment (Direct & Fiserv)
Airtime Topup
Payment GW(Credit/Debit)
Mobile Wallets
Integration Tier 101
Notification Services 102
Service Connectors 103
Business Process Services 104
Paymennt Handler 105
Security Sevices 106
Authorization Services 107
Database 108
Person Mgmt
Company Mgmt
Tx History
Profile Objects
Money Container
Rules Engine 109
Name Matching Engine 110
Processor 121
Clearing House (Web Svc)
Clearing House (Batch)

FIG. 1

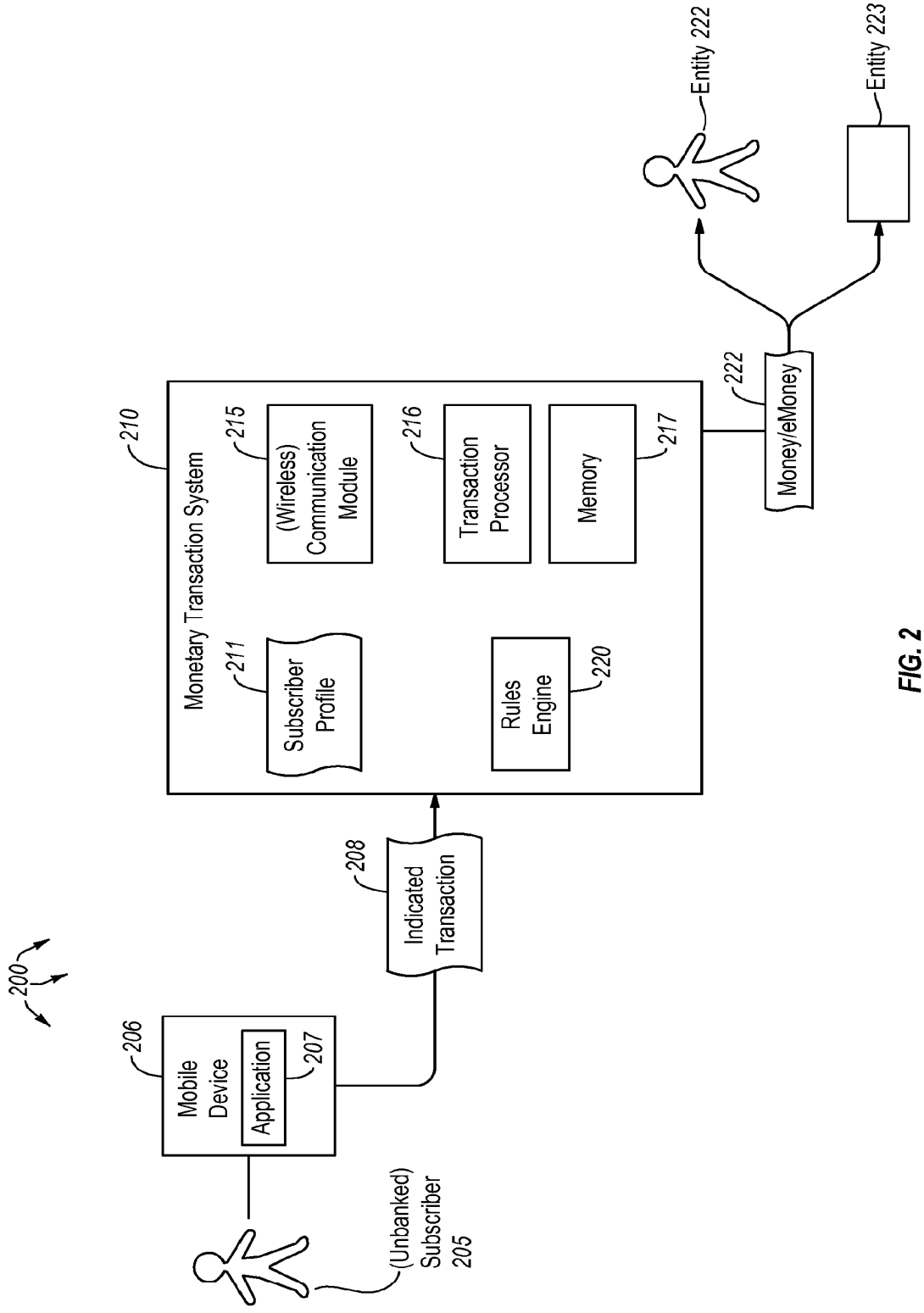
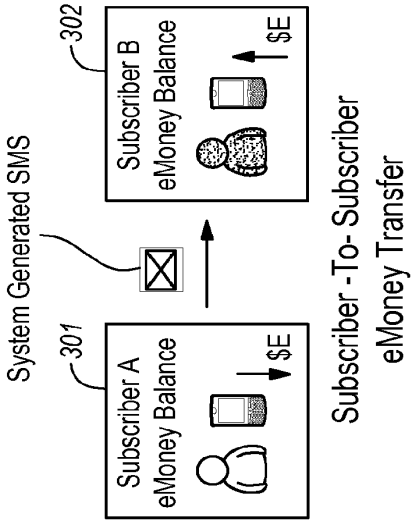
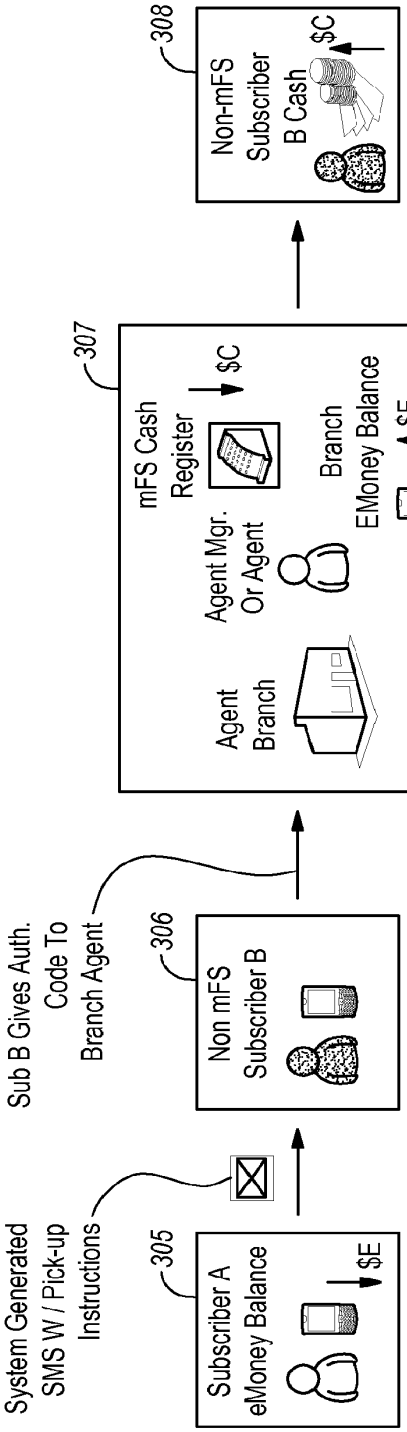

200
206
Mobile Device
Application
207
(Unbanked) Subscriber 205
208
Indicated Transaction
210
Monetary Transaction System
211
Subscriber Profile
215
(Wireless) Communication Module
216
Transaction Processor
217
Memory
220
Rules Engine
222
Money/eMoney
Entity 222
Entity 223

FIG. 2



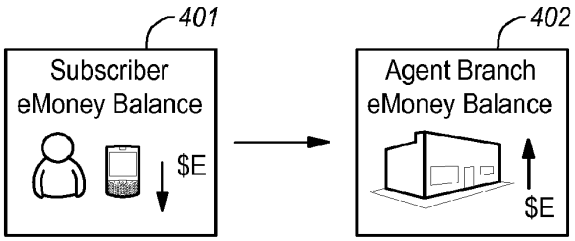
Subscriber -To- Subscriber
eMoney Transfer

FIG. 3A



Subscriber -To- Non Subscriber
eMoney Transfer

FIG. 3B



Subscriber Makes Retail Purchase

FIG. 4

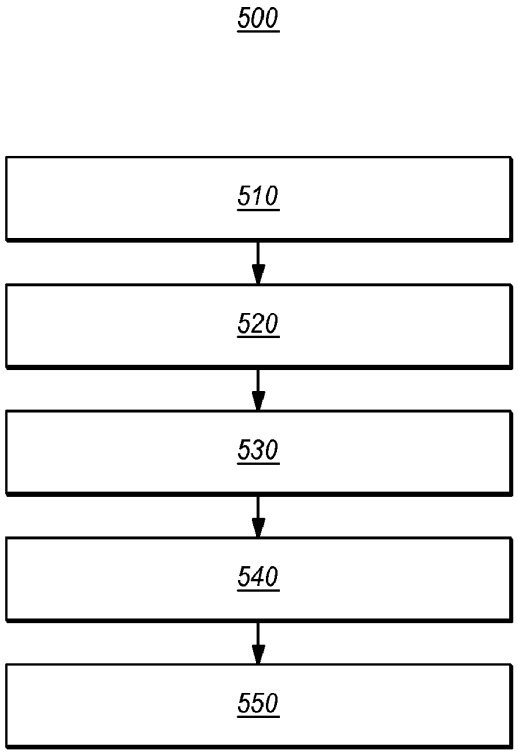


FIG. 5

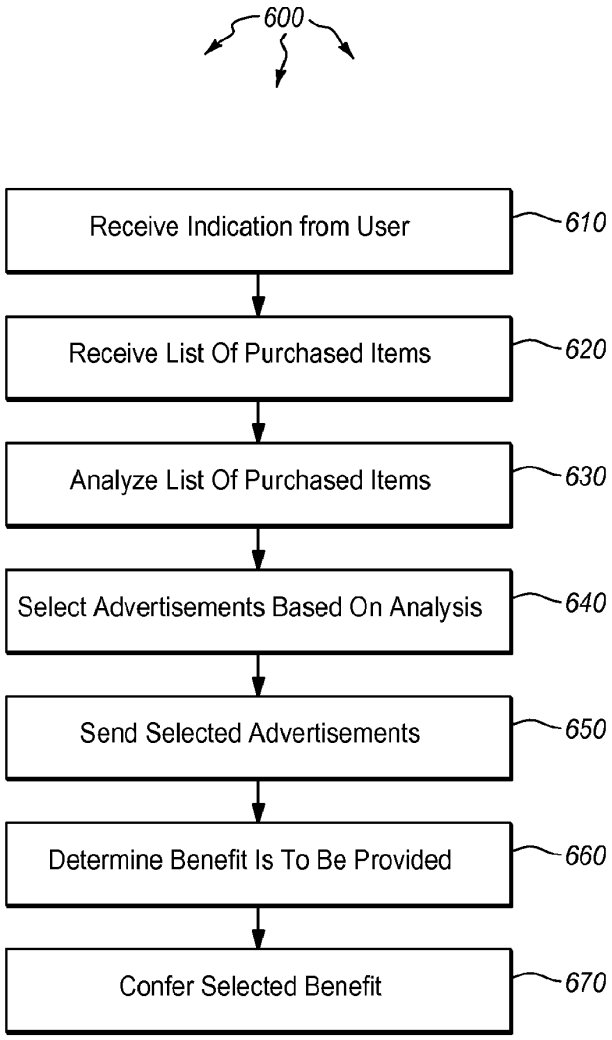

600
Receive Indication from User
610
Receive List Of Purchased Items
620
Analyze List Of Purchased Items
630
Select Advertisements Based On Analysis
640
Send Selected Advertisements
650
Determine Benefit Is To Be Provided
660
Confer Selected Benefit
670

FIG. 6

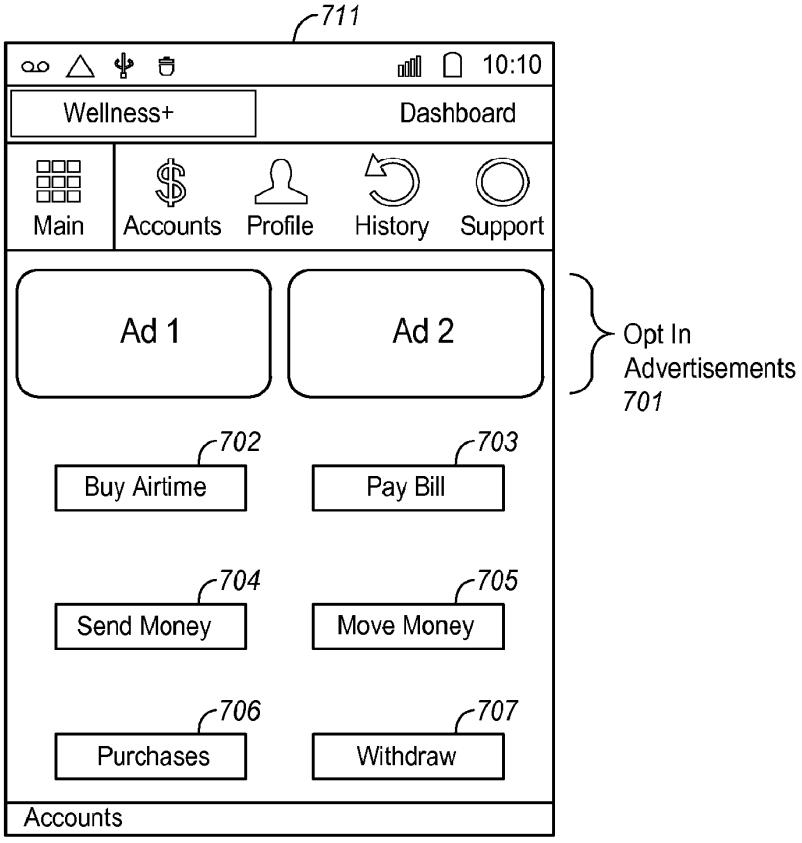

711
10:10
Wellness+
Dashboard
Main
Accounts
Profile
History
Support
Ad 1
Ad 2
Opt In
Advertisements
701
702
Buy Airtime
703
Pay Bill
704
Send Money
705
Move Money
706
Purchases
707
Withdraw
Accounts

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 12/43458

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 30/00 (2012.01)
USPC - 705/14.13
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)
USPC: 705/14.13; IPC(8): G06Q 30/00 (2012.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/1.1, 14.1, 14.13, 30, 35, 40; 700/1, 90; IPC(8): G06Q 30/00 (2012.01)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DialogWeb: Google Scholar; Google Web; Google Patents; PubWest; Thomson Innovation
Search Terms: ADVERTISE, COMPUTER, PROCESSOR, MEMORY, STORE, SAVE, MEDIA, MEDIA, PROGRAM, SOFTWARE, CODE, REDUCED, COST, PRICE, FREE, DISCOUNT, SERVICE, PRODUCT, GOODS, EXCHANGE, TRADE, INTERCHANGE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010/0250356 A1 (Gillenson et al.) 30 September 2010 (30.09.2010), entire document, especially para [0040], [0066], [0068], [0084], [0115]-[0117], [0120], [0123], [0130]-[0131], [0136]-[0137], [0139]-[0140], [0144], [0157], [0160], [0162], [0167]	1-20
Y	US 7,548,915 B2 (Ramer et al.) 16 June 2009 (16.06.2009), entire document, especially col. 3, ln 10-28; col. 9, ln 64 to col. 10, ln 28; col. 27, ln 12-46	1-20
A	US 7,689,506 B2 (Fei et al.) 30 March 2010 (30.03.2010), entire document	1-20
A	US 7,694,876 B2 (Barnes et al.) 13 April 2010 (13.04.2010), entire document	1-20
A	US 2011/0047016 A1 (Cook) 24 February 2011 (24.02.2011), 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
27 July 2012 (27.07.2012)	17 AUG 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

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

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 February 2013 (21.02.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/025273 A1

(51) International Patent Classification:
G06Q 20/00 (2012.01)

(21) International Application Number:
PCT/US2012/040131

(22) International Filing Date:
31 May 2012 (31.05.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/493,064	3 June 2011 (03.06.2011)	US
61/522,099	10 August 2011 (10.08.2011)	US
13/484,199	30 May 2012 (30.05.2012)	US

(71) Applicant *(for all designated States except US)*: **MOZIDO, LLC** [US/US]; 1950 Stemmons Freeway, Suite 6040, Dallas, TX 75207 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LIBERTY, Michael, A.** [US/US]; 5373 Isleworth Country Club Drive, Windermere, FL 34786 (US).

(74) Agents: **STRINGHAM, John, C.** et al.; Workman Nydegger, 60 East South Temple, Suite 1000, Salt Lake City, UT 84111 (US).

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

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

Published:

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

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

(54) **Title**: MONETARY TRANSACTION SYSTEM

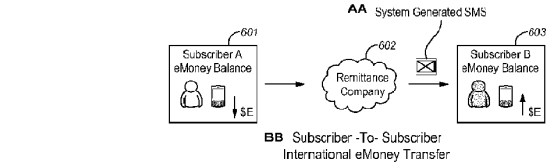


FIG. 6A

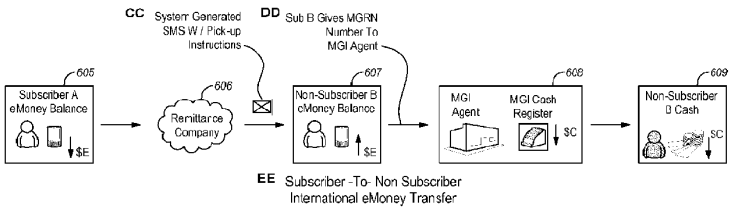


FIG. 6B

(57) **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.

WO 2013/025273 A1

MONETARY TRANSACTION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to and the benefit of U.S. Utility Application Ser. No. 13/484,199, filed on May 30, 2012, entitled "Monetary Transaction System", and also 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". All of the aforementioned provisional applications are incorporated by reference in their entirety herein.

BACKGROUND

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.

BRIEF SUMMARY

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.

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.

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, 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.

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.

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.

BRIEF DESCRIPTION OF THE DRAWINGS

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:

Figure 1 illustrates a monetary transaction system architecture in which embodiments described herein may operate.

Figure 2 illustrates an alternate example embodiment of a monetary transaction system.

Figure 3 illustrates an example data flow for performing a subscriber deposit via a mobile wallet.

Figure 4 illustrates an example data flow for performing a subscriber withdrawal via a mobile wallet.

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.

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.

Figure 7 illustrates an example data flow for performing a subscriber airtime purchase via a mobile wallet.

Figure 8 illustrates an example data flow for performing a subscriber-initiated bill pay via a mobile wallet.

Figure 9 illustrates an example data flow for performing a subscriber-initiated retail purchase via a mobile wallet.

Figures 10A and 10B illustrate example data flows for requesting and repaying micro-loans via a mobile wallet, respectively.

Figure 11A illustrates an example data flow of a subscriber receiving a direct deposit via a mobile wallet.

Figure 11B illustrates an example data flow of a subscriber receiving a governmental welfare payment via a mobile wallet.

Figure 12A illustrates an example data flow of an agent administrator distributing eMoney via a mobile wallet.

Figure 12B illustrates an example data flow of an agent company making a deposit using a mobile wallet.

Figure 13 illustrates an example data flow of an agent company making a withdrawal using a mobile wallet.

Figure 14 illustrates an example data flow of a subscriber making a deposit at an agent branch using a mobile wallet.

Figure 15 illustrates an example data flow of a subscriber making a deposit with a non-agent using a mobile wallet.

Figure 16 illustrates an example data flow of a subscriber making a withdrawal with an agent using a mobile wallet.

Figure 17A illustrates an example data flow of a subscriber making a withdrawal from an ATM using a mobile wallet.

Figure 17B illustrates an example data flow of a subscriber-to-subscriber money transfer using a mobile wallet.

Figure 17C illustrates an example data flow of a subscriber-to-non-subscriber money transfer using a mobile wallet.

Figure 18A illustrates an example data flow of a subscriber-to-subscriber international money transfer using a mobile wallet.

Figure 18B illustrates an example data flow of a subscriber-to-non-subscriber international money transfer using a mobile wallet.

Figure 19A illustrates an example data flow of a subscriber-to-subscriber international money transfer using a mobile wallet.

Figure 19B illustrates an example data flow of a non-subscriber-to-subscriber international money transfer using a mobile wallet.

DETAILED DESCRIPTION

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.

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.

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, 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.

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.

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.

Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change 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.

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.

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.

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.

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.

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 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.

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.

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.

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.

Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a 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.

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.

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 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.

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.

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 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.

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.

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 mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

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.

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.

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".

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.

In some embodiments, in countries with more developed economics, 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.

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 distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

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.

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".

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.

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 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.

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.

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.

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 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.

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.

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.

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 system, the company accepts payment from mFS mobile wallet accounts, either in the form of eMoney or through periodic settlements.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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".

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.

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.

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.

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 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).

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.

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.

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 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.

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.

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 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.

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.

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.

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 the external processor. A Clearing House subsystem of transaction processor 121 can be used to exchange the financial information with a bank.

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.

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.

Figure 2 depicts a monetary transaction system 200 similar to that described in Figure 1. The monetary transaction system 200 may provide a more 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.

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.

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 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).

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.

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.

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.

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.

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 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.

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.

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).

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 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.

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.

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 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.

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).

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 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.

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.

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 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.

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.

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.

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.

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).

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 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.

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.

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 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).

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.

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 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.

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 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.

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.

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.

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 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.

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.

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.

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 eMoney balance, log the transaction, and sends transaction details to the mFS platform bank.

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.

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 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.

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.

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.

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.

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.

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.

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 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.

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 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.

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).

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.

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). 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).

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.

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 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).

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.

Figure 17C illustrates subscriber-to-non-subscriber money transfers. In this embodiment, subscriber A (an mFS subscriber) wishes to send money to another 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).

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.

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 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).

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.

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 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).

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).

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 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.

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.

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 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.

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.

In another embodiment, the monetary transaction system 210 is implemented to add a bank or credit union account to a mobile wallet. The 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.

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 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.

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.

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®. 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.

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 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.

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.

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.

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;

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;

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;

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;

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;

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

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.

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;

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.

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;

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;

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.

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

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.

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 and other mobile wallet transaction system components via the wireless service provider's network.

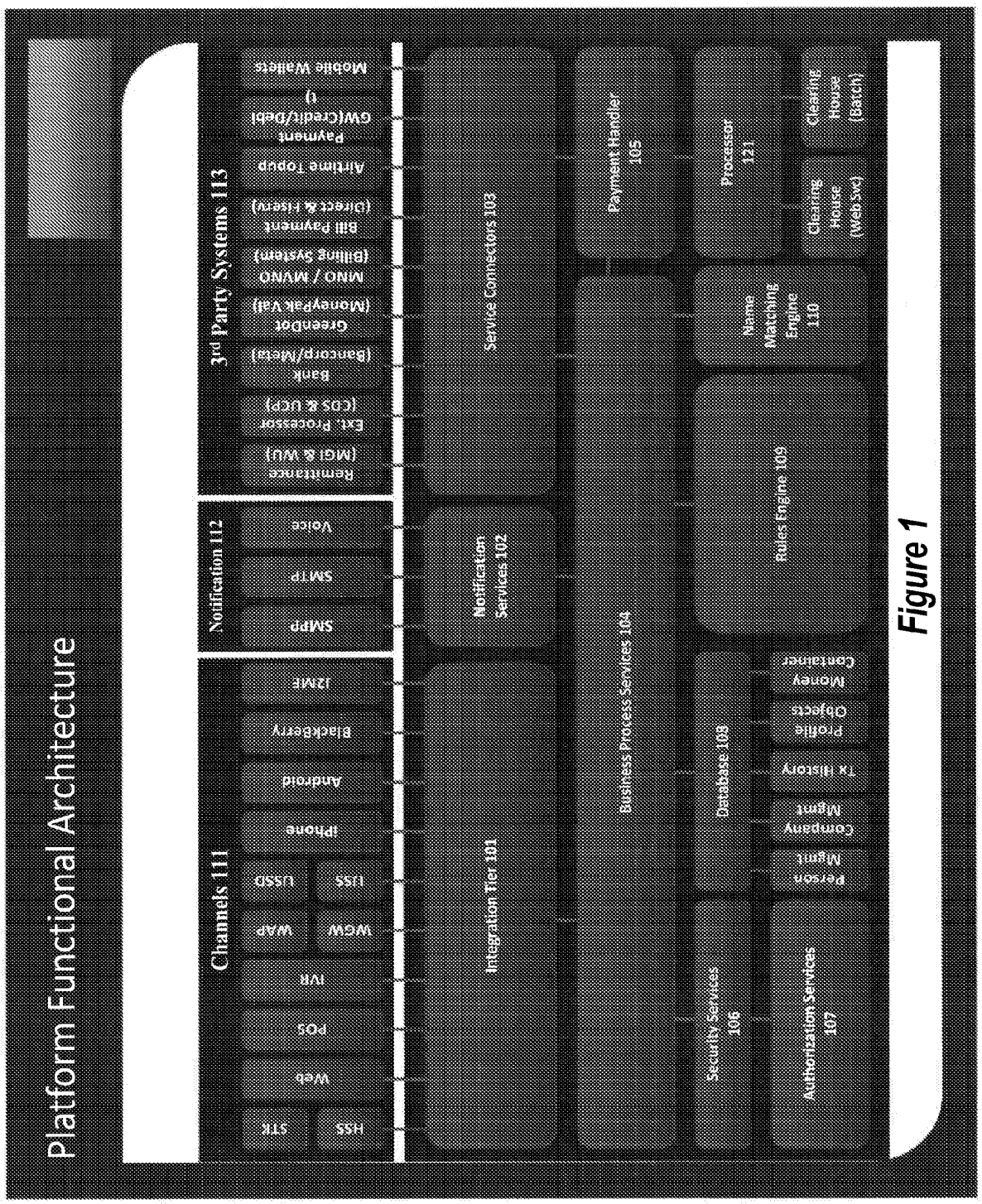

Platform Functional Architecture
Channels 111
HSS
STK
Web
POS
IVR
WGW
WAP
USSD
USS
iPhone
Android
BlackBerry
J2ME
Notification 112
SMPP
SMTP
Voice
3rd Party Systems 113
Remittance (MGI & WU)
Ext. Processor (CDS & UCP)
Bank (Bancorp/Meta)
GreenDot (MoneyPak Vail)
MNO / MVNO (Billing System)
Bill Payment (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
Name Matching Engine 110
Processor 121
Clearing House (Web Svc)
Clearing House (Batch)
Authentication Services 107
Person Mgmt
Company Mgmt
Tx History
Profile Objects
Money Container
Figure 1

FIG. 1

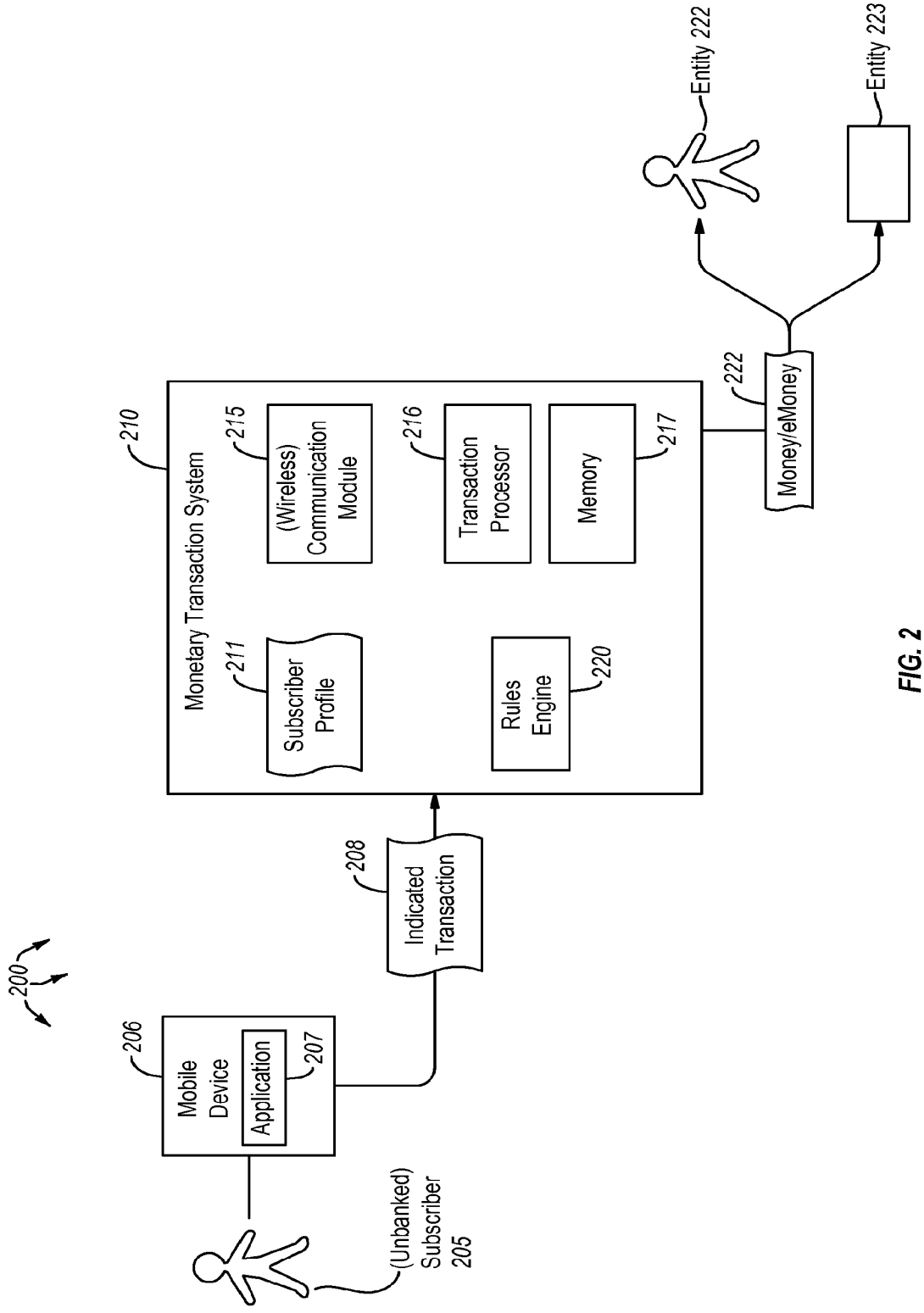
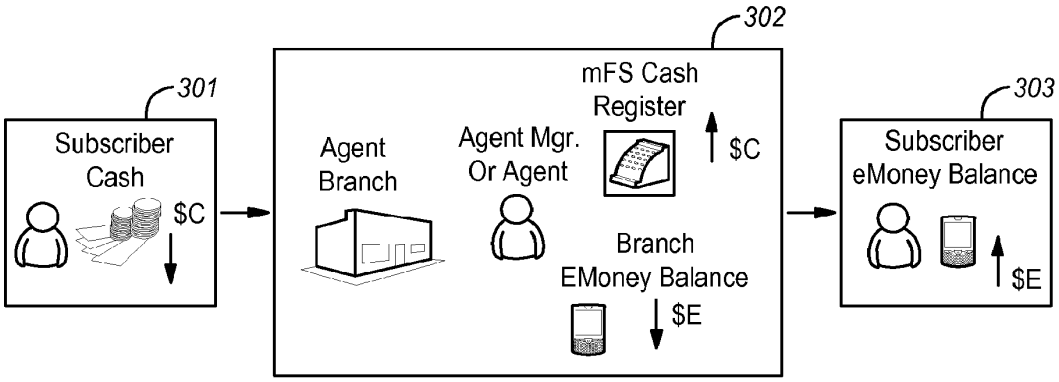

200
206
Mobile Device
Application
207
(Unbanked) Subscriber 205
208
Indicated Transaction
210
Monetary Transaction System
211
Subscriber Profile
215
(Wireless) Communication Module
216
Transaction Processor
217
Memory
220
Rules Engine
222
Money/eMoney
Entity 222
Entity 223

FIG. 2


301
Subscriber Cash
$C
302
Agent Branch
Agent Mgr. Or Agent
mFS Cash Register
$C
Branch EMoney Balance
$E
303
Subscriber eMoney Balance
$E

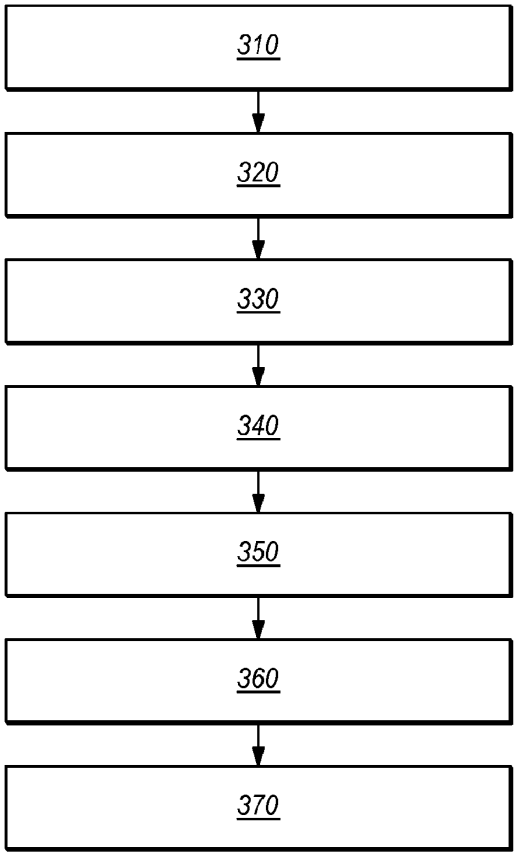
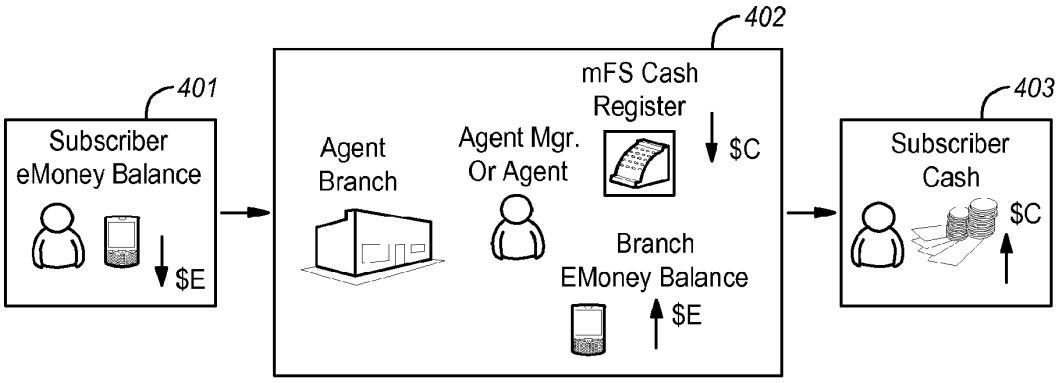

Subscriber Deposit
310
320
330
340
350
360
370

FIG. 3



Subscriber Withdrawal

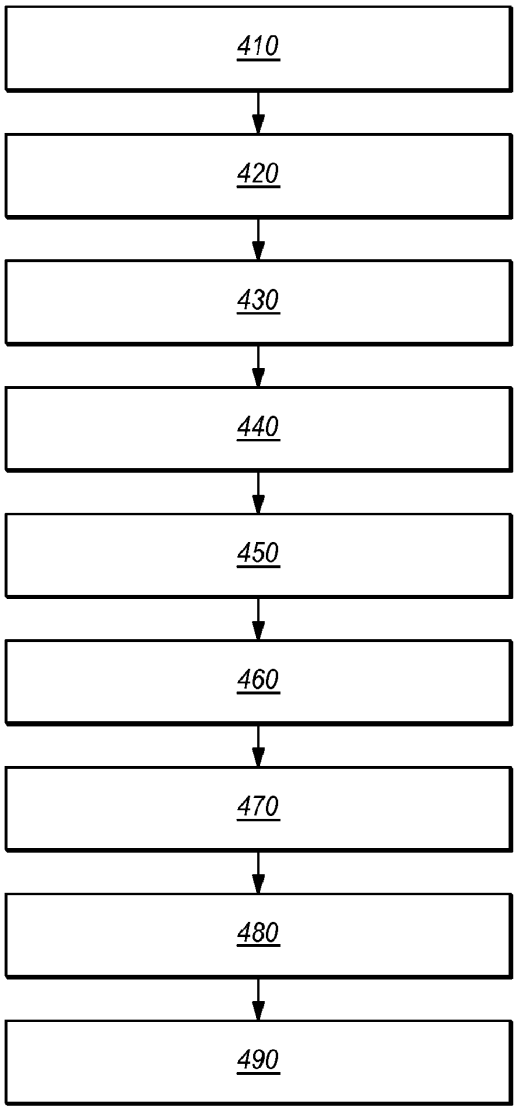
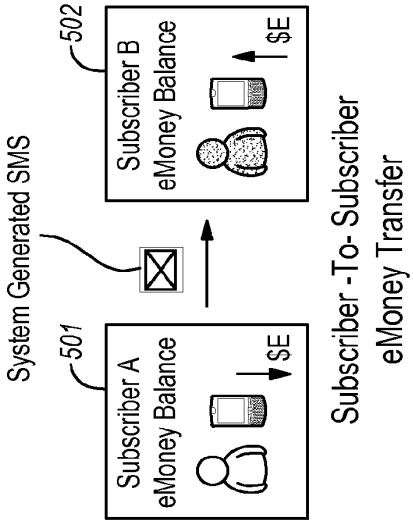
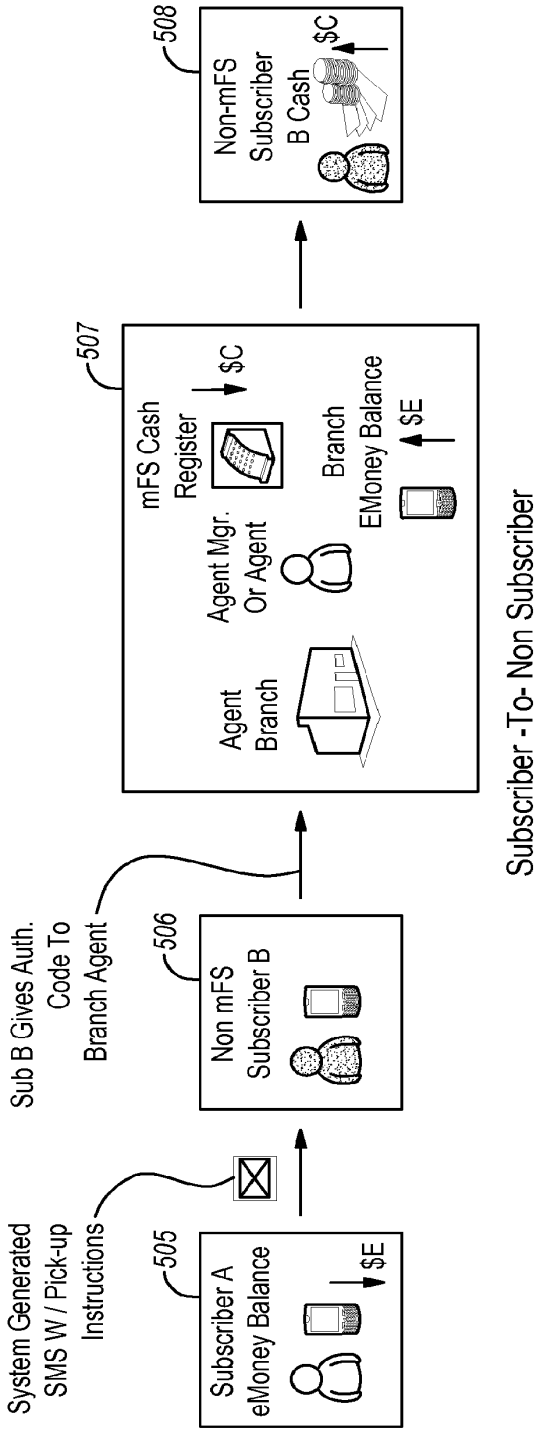


FIG. 4



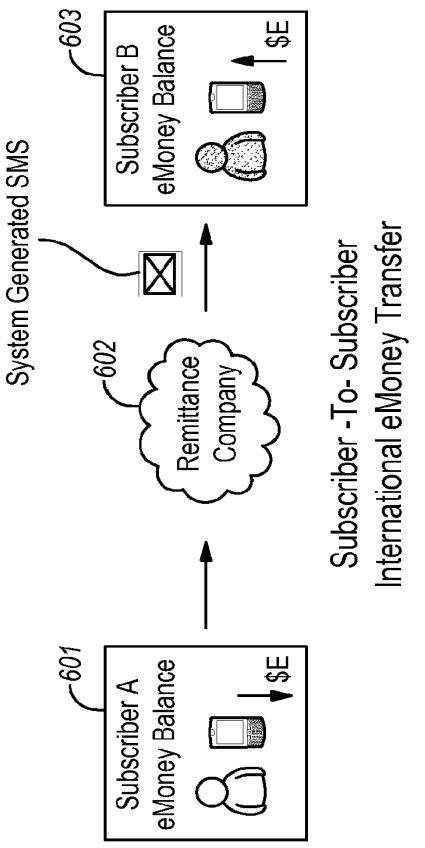
Subscriber -To- Subscriber
eMoney Transfer

FIG. 5A



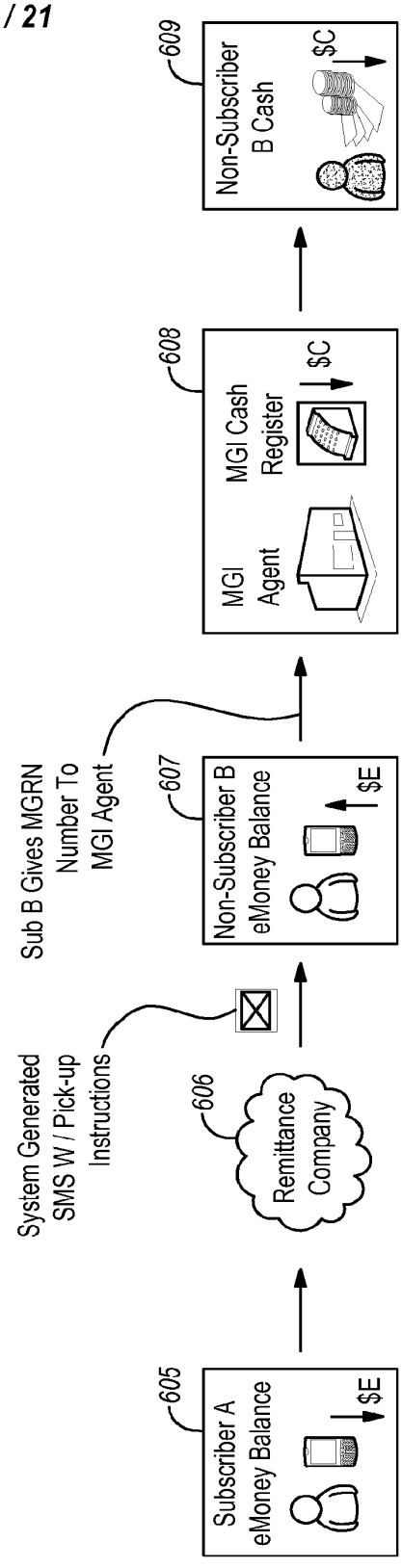
Subscriber -To- Non Subscriber
eMoney Transfer

FIG. 5B



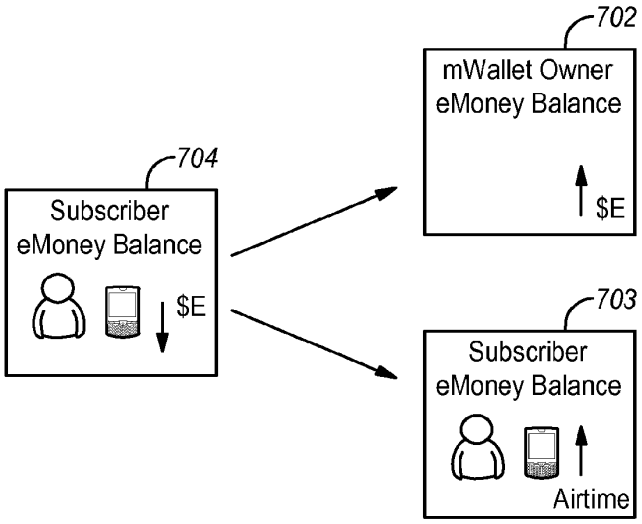
Subscriber -To- Subscriber
International eMoney Transfer

FIG. 6A



Subscriber -To- Non Subscriber
International eMoney Transfer

FIG. 6B



Subscriber Buys Airtime

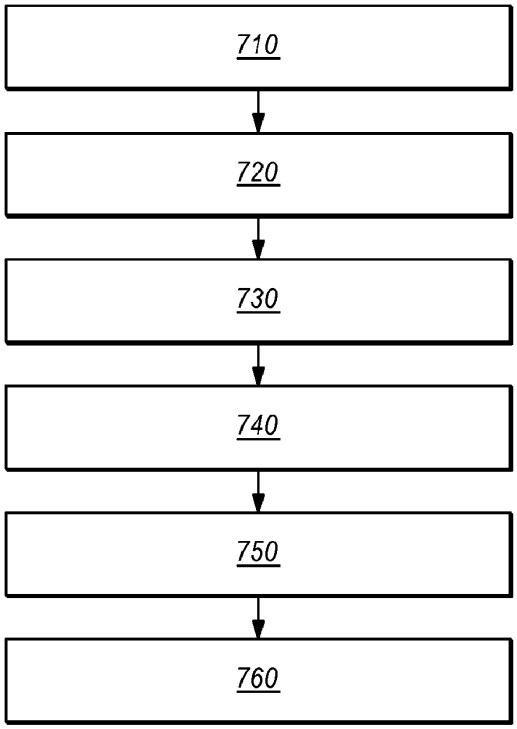
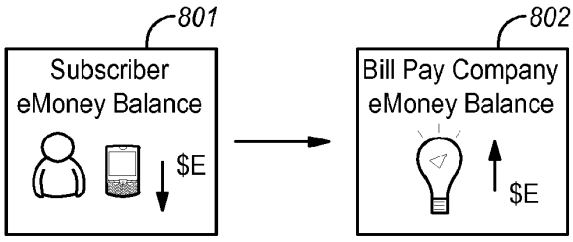


FIG. 7



Subscriber Pays Bill

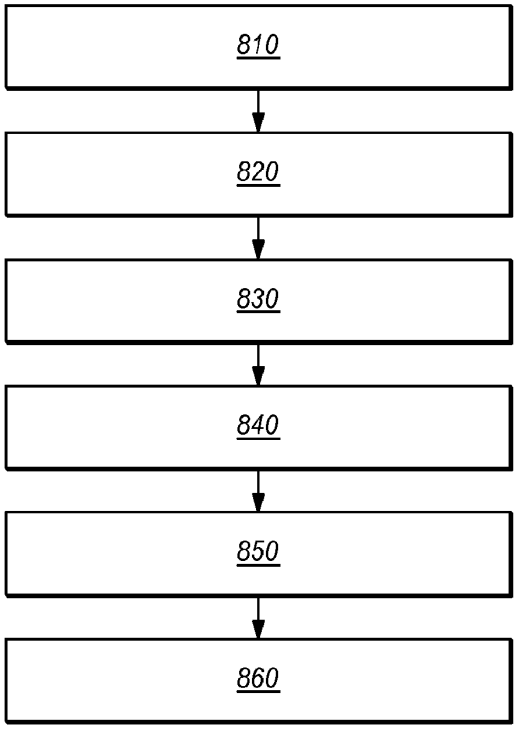
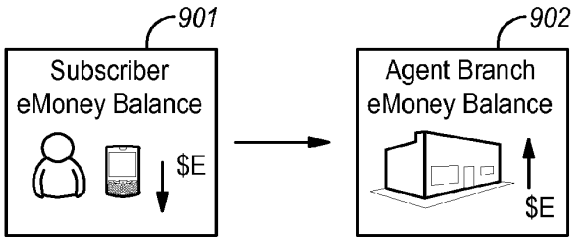


FIG. 8



Subscriber Makes Retail Purchase

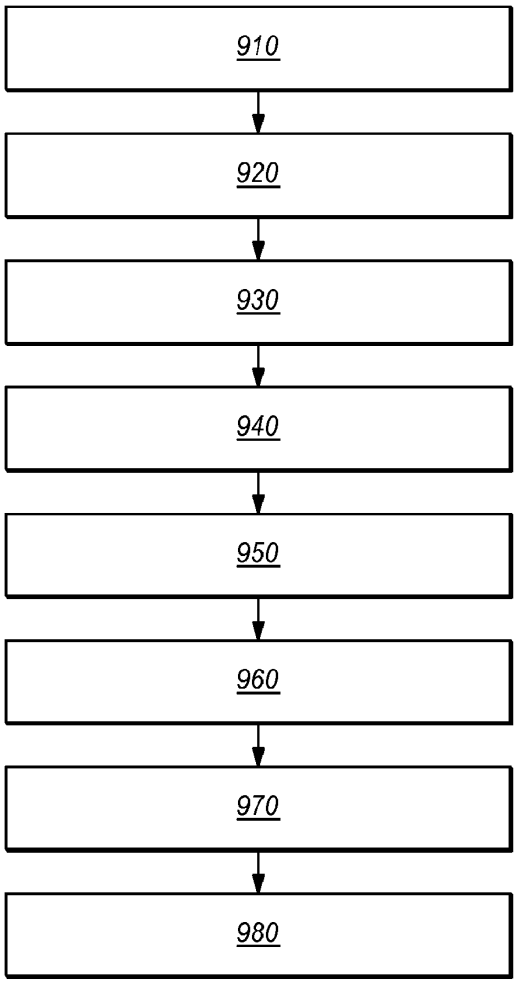
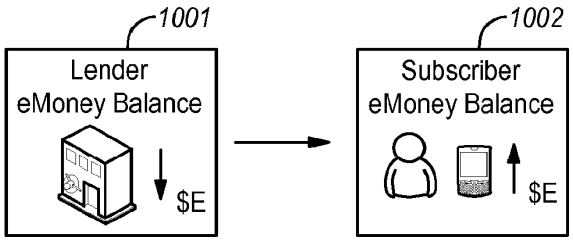
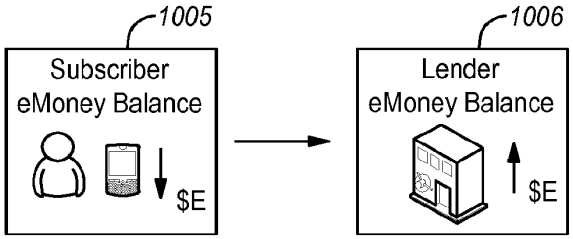


FIG. 9



Subscriber Requests Micro-Loan

FIG. 10A



Subscriber Repays Micro-Loan

FIG. 10B

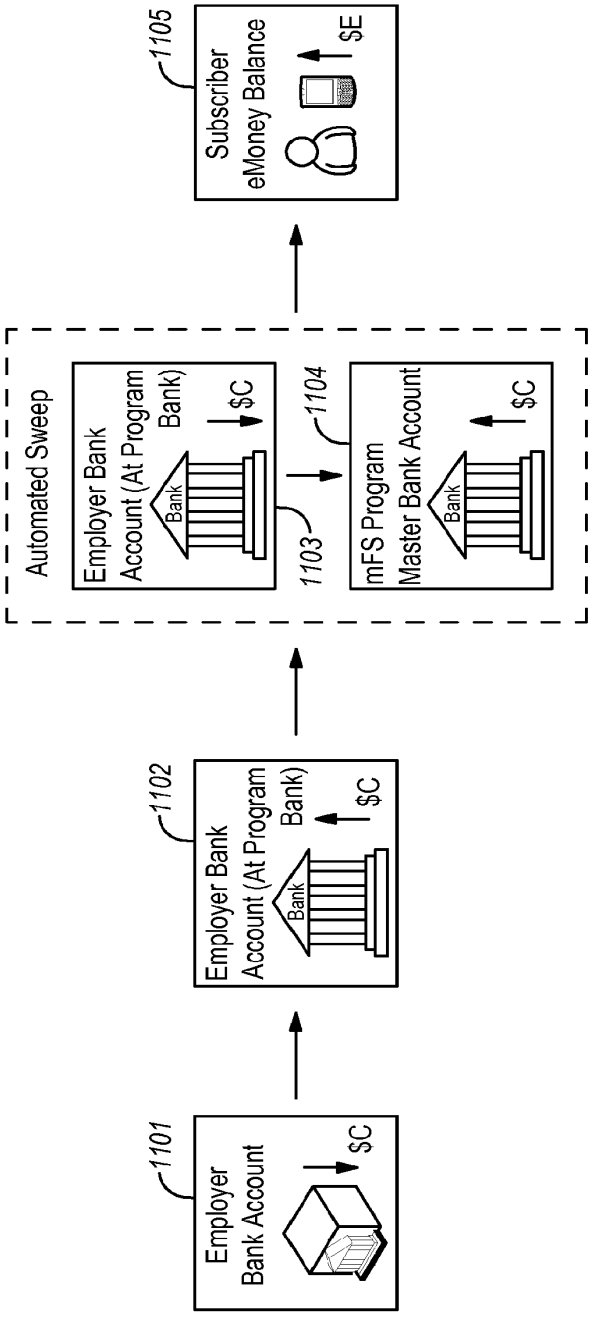
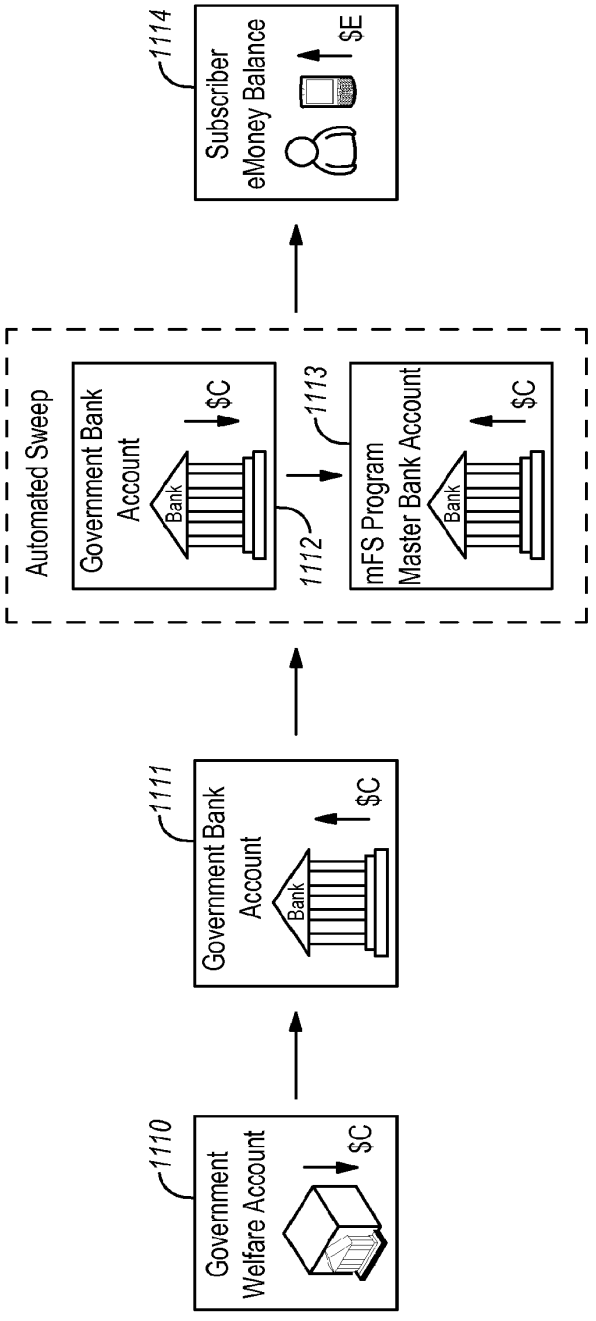

1101
Employer Bank Account
$C
1102
Employer Bank Account (At Program Bank)
Bank
$C
Automated Sweep
Employer Bank Account (At Program Bank)
Bank
$C
1103
1104
mFS Program Master Bank Account
Bank
$C
1105
Subscriber eMoney Balance
$E
Subscriber Receives Direct Deposit

FIG. 11A



Subscriber Receives Government Welfare Payment

FIG. 11B

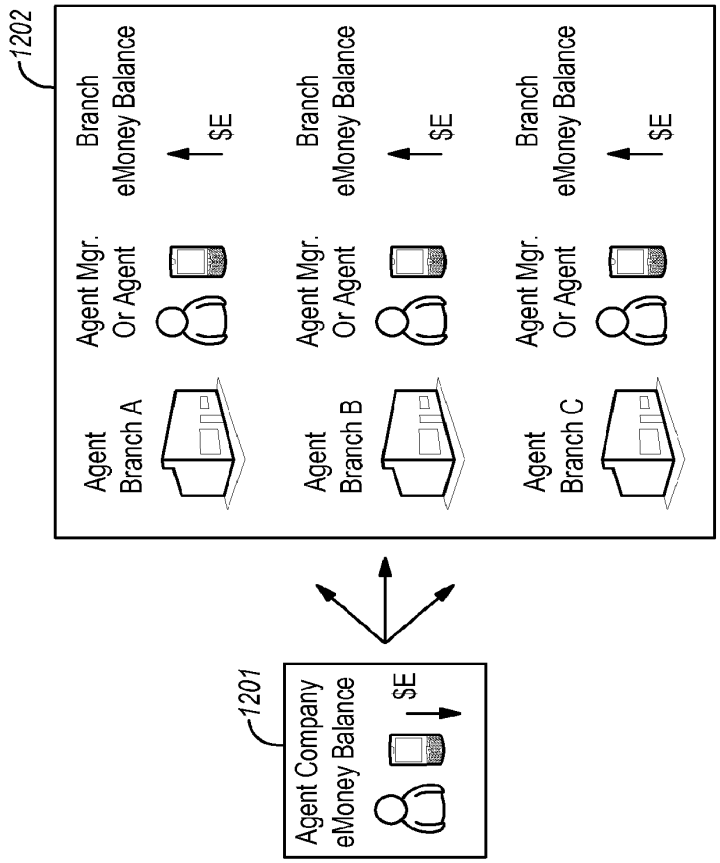

1202
Agent Branch A
Agent Mgr. Or Agent
Branch eMoney Balance
$E
Agent Branch B
Agent Mgr. Or Agent
Branch eMoney Balance
$E
Agent Branch C
Agent Mgr. Or Agent
Branch eMoney Balance
$E
1201
Agent Company eMoney Balance
$E
Agent Administrator Distributes eMoney

FIG. 12A

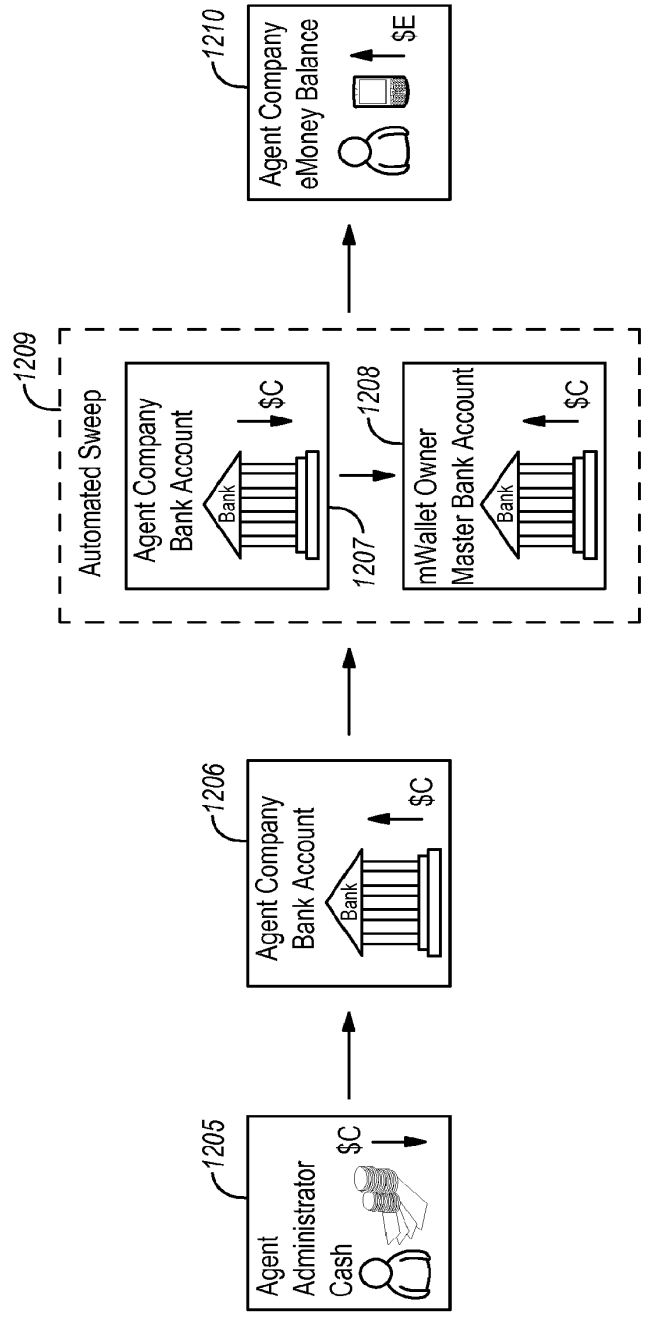

1205
Agent Administrator Cash
$C
1206
Agent Company Bank Account
Bank
$C
1209
Automated Sweep
Agent Company Bank Account
Bank
$C
1207
1208
mWallet Owner Master Bank Account
Bank
$C
1210
Agent Company eMoney Balance
$E
Agent Company Deposit

FIG. 12B

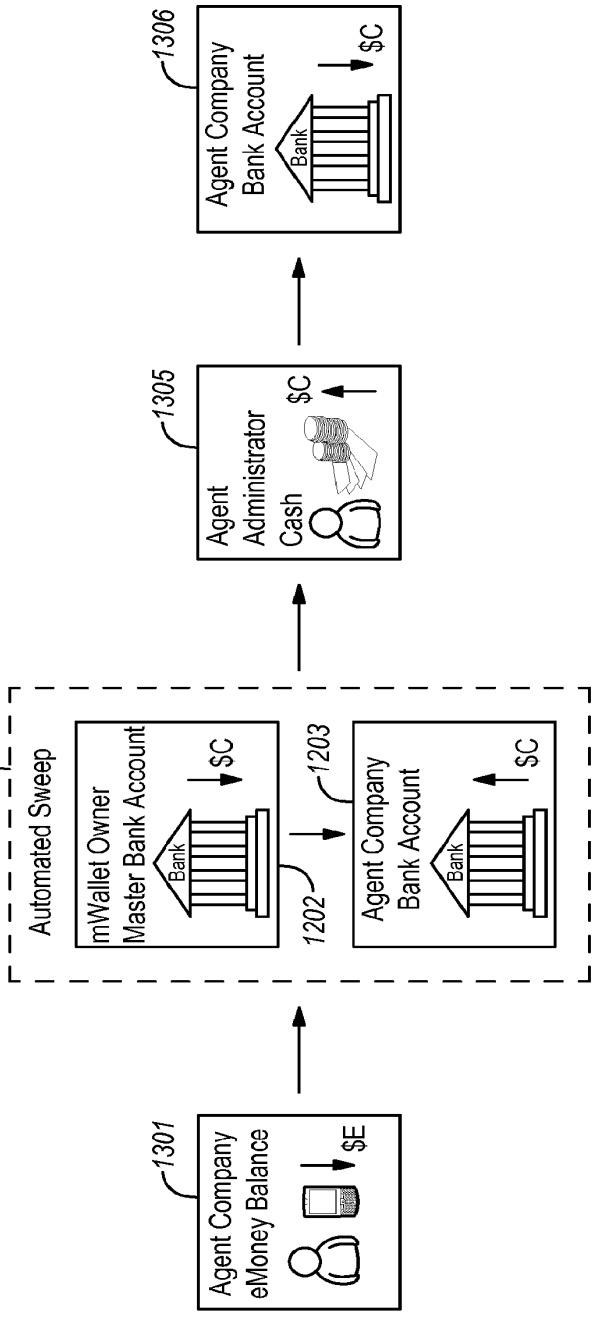
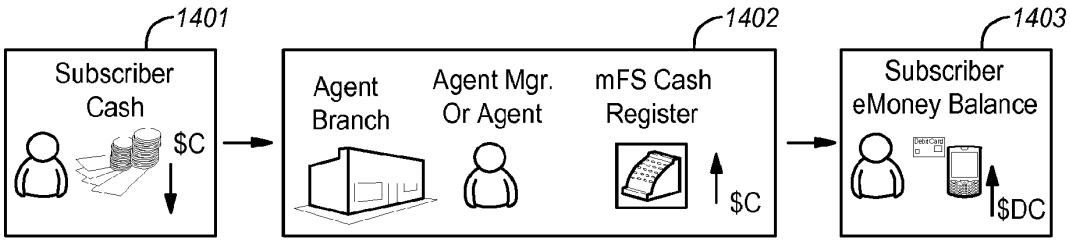

1306
Agent Company
Bank Account
Bank
$C
1305
Agent
Administrator
Cash
$C
1304
Automated Sweep
mWallet Owner
Master Bank Account
Bank
$C
1202
1203
Agent Company
Bank Account
Bank
$C
1301
Agent Company
eMoney Balance
$E
Agent Company Withdrawal

FIG. 13



Subscriber Deposit At Agent Branch

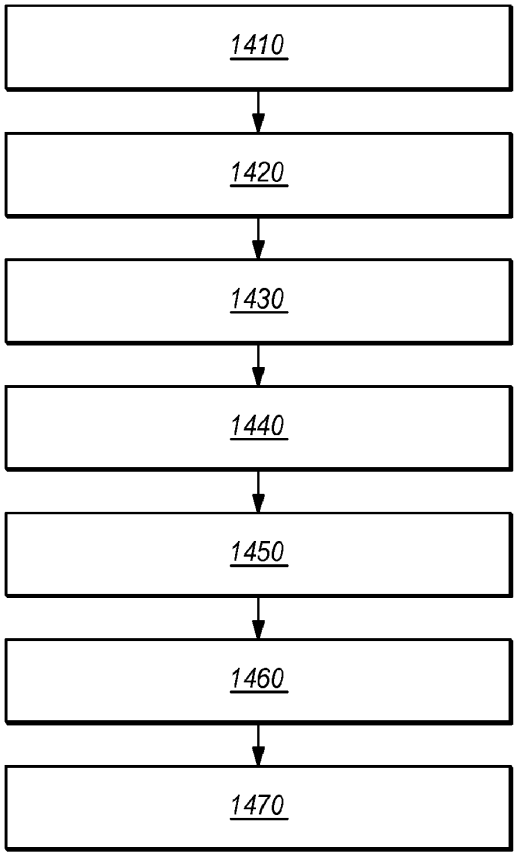
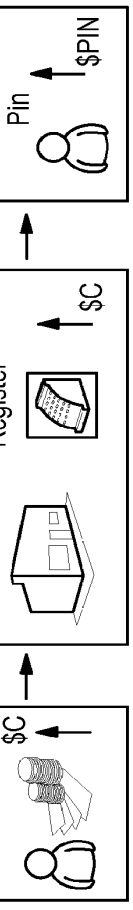
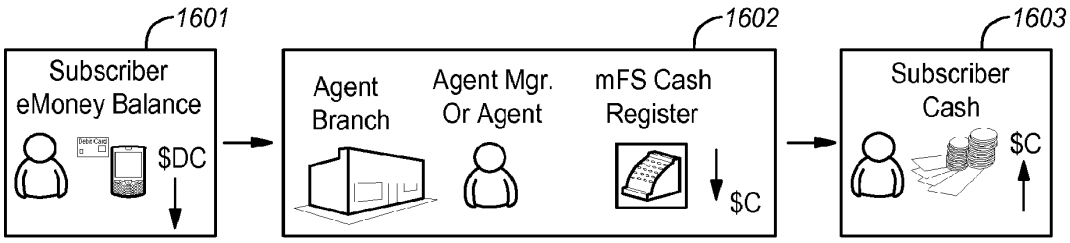


FIG. 14



Subscriber Deposit (Non-Agent)

FIG. 15



Subscriber Withdrawal (Agent)

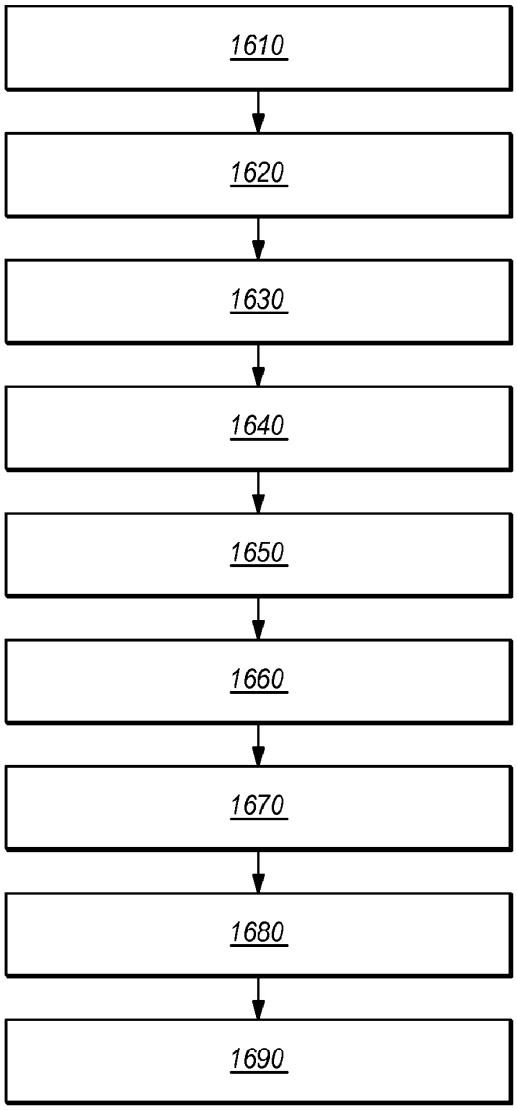
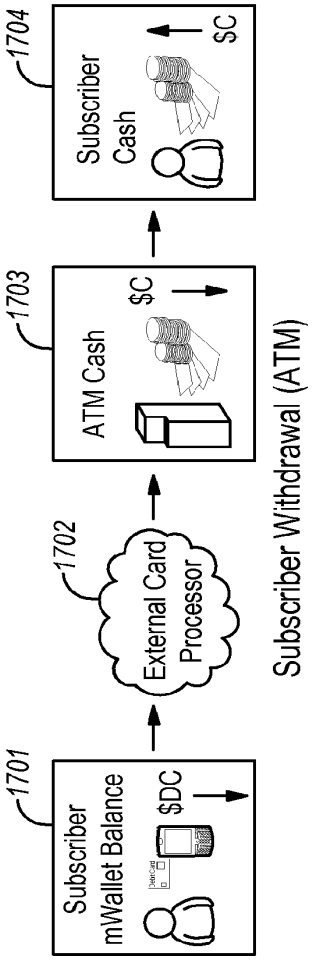
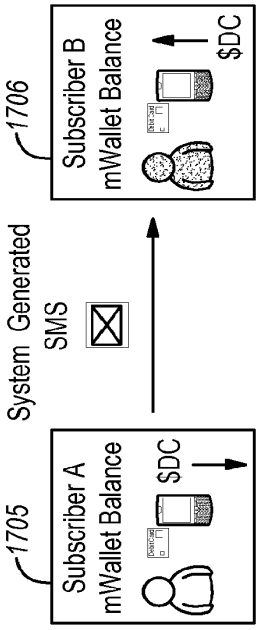


FIG. 16



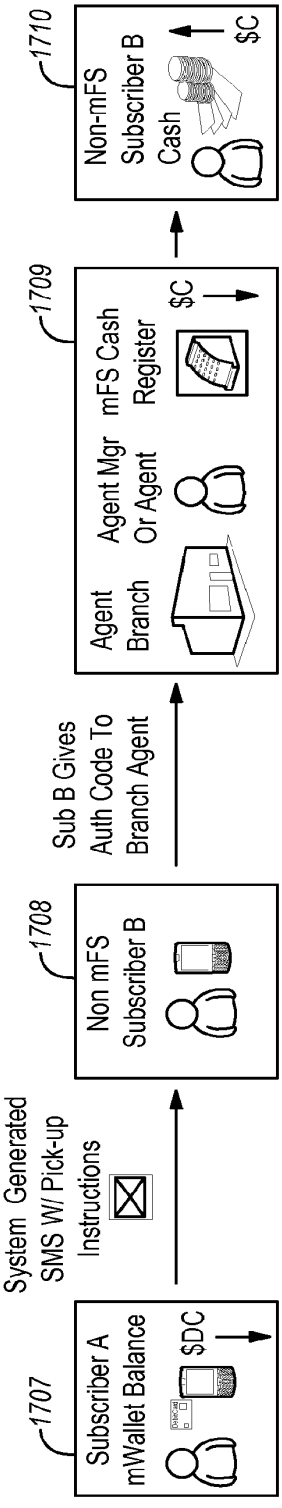
Subscriber Withdrawal (ATM)

FIG. 17A



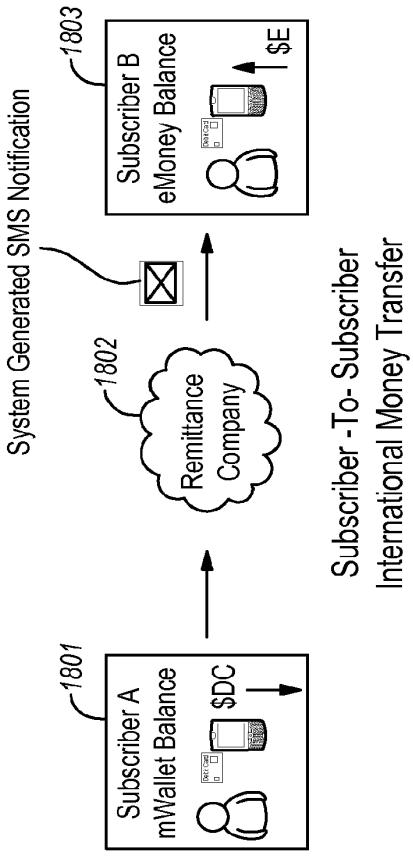
Subscriber To Subscriber Money Transfer

FIG. 17B



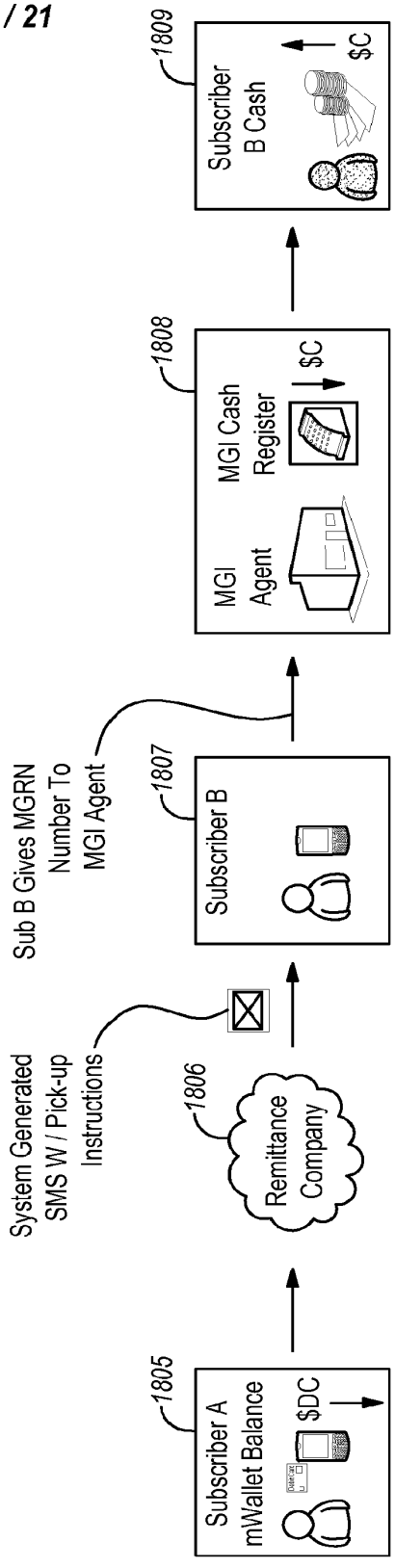
Subscriber To Non-Subscriber Money Transfer

FIG. 17C



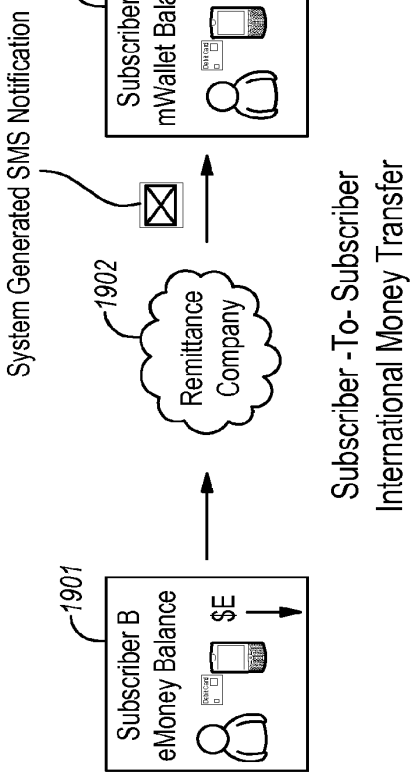
Subscriber -To- Subscriber
International Money Transfer

FIG. 18A



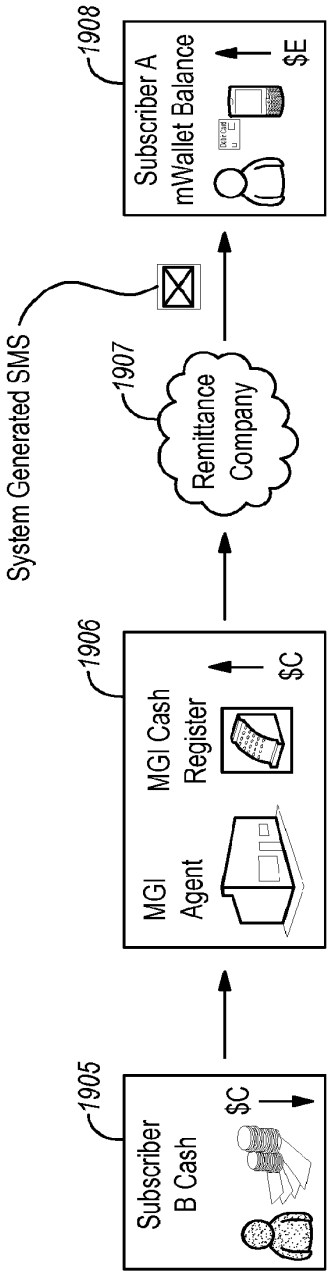
Subscriber -To- Non Subscriber
International Money Transfer

FIG. 18B



Subscriber -To- Subscriber
International Money Transfer

FIG. 19A



Non-Subscriber -To- Subscriber
International Money Transfer

FIG. 19B

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 [0028], [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], [1168]	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)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 May 2013 (30.05.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/078176 A1

(51) International Patent Classification:
G06Q 20/00 (2012.01)

(21) International Application Number:
PCT/US2012/066013

(22) International Filing Date:
20 November 2012 (20.11.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/562,301 21 November 2011 (21.11.2011) US
13/680,824 19 November 2012 (19.11.2012) US

(71) Applicant: **MOZIDO, LLC** [US/US]; 1950 Stemmons Freeway, Suite 6040, Dallas, TX 75207 (US).

(72) Inventor: **LIBERTY, Michael, A.**; 5373 Isleworth Country Club Drive, Windermere, FL 34786 (US).

(74) Agents: **STRINGHAM, John, C.** et al.; 60 East South Temple, Suite 1000, Salt Lake City, UT 84111 (US).

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

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

Published:

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

(54) **Title**: USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS

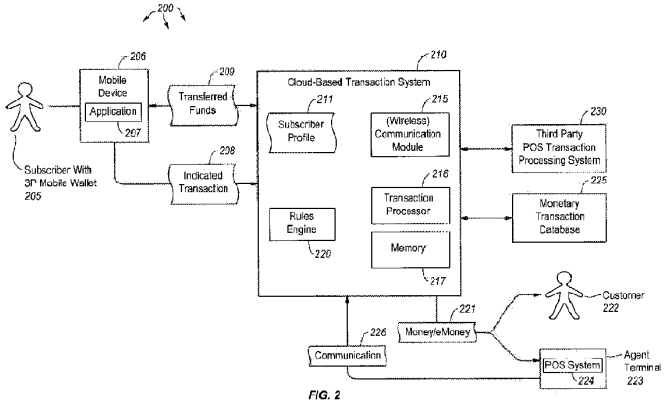


FIG. 2

(57) **Abstract**: Embodiments are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one scenario, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

WO 2013/078176 A1

USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of U.S. Application Ser. No. 13/680,895, entitled "Using a Mobile Wallet Infrastructure to Support Multiple Mobile Wallet Providers", filed on November 19, 2012, and U.S. Provisional Application Ser. No. 61/562,301, entitled "Using a Mobile Wallet Infrastructure to Support Multiple Mobile Wallet Providers", filed on November 21, 2011, which are herein incorporated by reference in their entirety.

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.

BRIEF SUMMARY

[0003] Embodiments described herein extend to methods, systems, and computer program products for a cloud-based transaction platform. Embodiments include an infrastructure that can be used with third party mobile wallets provided by third party mobile wallet providers. Users with native or third party mobile wallets can use the cloud-based transaction platform to enroll a customer for a third party mobile wallet, add a stored value account (either hosted by the cloud-based transaction platform or a third party), add a bank/credit union account to a third party mobile wallet, add a debit/credit card account to a third party mobile wallet, deposit funds in a third party mobile wallet, withdraw funds from a third party mobile wallet, pay bills from a third party mobile wallet, top up a prepaid mobile account through a third party mobile wallet, transfer funds through a third party mobile wallet, and make in store purchases from a third party mobile wallet.

[0004] Embodiments described herein are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one embodiment, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

[0005] In another embodiment, a cloud-based transaction platform performs a transaction using a third party point of sale (POS) system. The cloud-based transaction platform receives communication from a specified POS system implemented at an agent terminal over a communication channel connected to the cloud-based transaction platform. The POS communication indicates that a customer has initiated a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the POS communication to a corresponding third party POS transaction processing system that has been established to process POS transactions from the specified POS system, receives communication from the third party POS transaction processing system confirming processing of the transaction, and sends communication to the specified POS system implemented at the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

[0006] In yet another embodiment, a cloud-based transaction platform is provided which allows users to make purchases from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform receives communication from a customer over a communication channel connected to the cloud-based transaction platform. The customer communication indicates that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet. The cloud-based transaction platform returns a secure, perishable purchase code to the customer over at

least one the communication channels connected to the cloud-based transaction platform and receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent terminal communication indicates that the purchase code has been presented to an agent. The cloud-based transaction platform then debits the customer's third party mobile wallet by the specified amount of funds to complete the purchase.

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

[0008] 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.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] 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:

[0010] Figure 1 illustrates a monetary transaction system architecture in which embodiments described herein may operate.

[0011] Figure 2 illustrates an example embodiment of a cloud-based transaction platform.

[0012] Figures 3A and 3B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber eMoney transfers via a mobile wallet, respectively.

[0013] Figure 4 illustrates an example data flow for making a retail purchase using a mobile wallet.

[0014] Figure 5 illustrates an example embodiment of a monetary transaction system architecture.

[0015] Figure 6 illustrates an alternate example embodiment of a cloud-based transaction platform.

[0016] Figure 7 illustrates an example embodiment data flow for performing a transaction using a third party mobile wallet.

[0017] Figure 8 illustrates an example embodiment data flow for performing a transaction using a third party point of sale (POS) system.

[0018] Figure 9 illustrates an example embodiment data flow for making a purchase from a third party mobile wallet provided by a third party mobile wallet provider.

DETAILED DESCRIPTION

[0019] Embodiments described herein extend to methods, systems, and computer program products for a cloud-based transaction platform. Embodiments include an infrastructure that can be used with third party mobile wallets provided by third party mobile wallet providers. Users with native or third party mobile wallets can use the cloud-based transaction platform to enroll a customer for a third party mobile wallet, add a stored value account (either hosted by the cloud-based transaction platform or a third party), add a bank/credit union account to a third party mobile wallet, add a debit/credit card account to a third party mobile wallet, deposit funds in a third party mobile wallet, withdraw funds from a third party mobile wallet, pay bills from a third party mobile wallet, top up a prepaid mobile account through a third party mobile wallet, transfer funds through a third party mobile wallet, and make in store purchases from a third party mobile wallet.

[0020] Embodiments described herein are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one embodiment, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends

communication to the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

[0021] In another embodiment, a cloud-based transaction platform performs a transaction using a third party point of sale (POS) system. The cloud-based transaction platform receives communication from a specified POS system implemented at an agent terminal over a communication channel connected to the cloud-based transaction platform. The POS communication indicates that a customer has initiated a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the POS communication to a corresponding third party POS transaction processing system that has been established to process POS transactions from the specified POS system, receives communication from the third party POS transaction processing system confirming processing of the transaction, and sends communication to the specified POS system implemented at the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

[0022] In yet another embodiment, a cloud-based transaction platform is provided which allows users to make purchases from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform receives communication from a customer over a communication channel connected to the cloud-based transaction platform. The customer communication indicates that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet. The cloud-based transaction platform returns a secure, perishable purchase code to the customer over at least one the communication channels connected to the cloud-based transaction platform and receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent terminal communication indicates that the purchase code has been presented to an agent. The cloud-based transaction platform then debits the customer's third party mobile wallet by the specified amount of funds to complete the purchase. Such purchases may be for items that are provided by the cloud-based transaction platform, either directly or via a third-party provider. These items may include music, movies, games and other downloadable content, physical items that can be shipped to the user and other items such as health care services.

[0023] Embodiments 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.

[0024] Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change 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.

[0025] 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.

[0026] 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.

[0027] 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.

[0028] 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.

[0029] 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 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.

[0030] 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.

[0031] 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.

[0032] 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.

[0033] Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a 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.

[0034] Various terminology will be used herein to describe the cloud-based transaction platform (also referred to as a "monetary transaction system", "mobile wallet platform", "mobile wallet program", "mobile wallet transaction system", "mobile financial services (mFS) platform" or "electronic payment system"). The term "agent" is used to refer to an individual with 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.

[0035] The cloud-based transaction platform includes an infrastructure that allows native mobile wallet application and third party mobile wallet applications to interact both with the transaction system and with each other. This allows the user of a native or a third party mobile wallet to make purchases, transfer money or perform any of the other transactions described herein. The cloud-based transaction platform may include a mobile wallet application and a web interface or some other type of functionality that allows the user to interact with the cloud-based transaction platform using their mobile device. The native and third party mobile wallet applications may include a subscriber identity module (SIM) application, an Unstructured Supplementary Service Data (USSD) application, a smartphone application, a web application, a mobile web 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.

[0036] As used herein, a mobile wallet application is a mobile wallet application installed on a SIM card or elsewhere on a mobile device. The mobile wallet application may either be native (i.e. provided by the provider of the cloud-based transaction platform) or third party (i.e. provided by a provider other than the provider of the cloud-based transaction platform).

[0037] 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. 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. Indeed, the cloud-based transaction platform allows different POS systems to interact with each other and conduct transactions between themselves.

[0038] 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. 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.

[0039] 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 mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

[0040] 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.

[0041] 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.

[0042] 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.

[0043] 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 distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

[0044] 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.

[0045] 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".

[0046] 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. 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.

[0047] 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. 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.

[0048] 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.

[0049] 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".

[0050] 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.

[0051] 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.

[0052] 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 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.

[0053] Figure 1 illustrates an example system architecture for a cloud-based transaction 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.

[0054] 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 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.

[0055] 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.

[0056] 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.

[0057] Name matching engine 110 is configured to match different objects according to specified configuration rules. Matching engine 110 can be used 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 the external processor. A Clearing House subsystem of transaction processor 121 can be used to exchange the financial information with a bank.

[0058] 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.

[0059] 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 third party mobile wallet, adding a debit or credit card account to a third party mobile wallet, depositing funds in a third party mobile wallet, withdrawing funds from a third party mobile wallet, paying bills from a third party mobile wallet, topping up a prepaid mobile account through a third party mobile wallet, transferring funds through a third party mobile wallet (nationally or internationally), making in-store purchases using a third party mobile wallet, selecting health care providers and paying for health care services, paying for music, games, movies or other downloadable provided by a third party provider and made available over the cloud-based transaction system, and various other tasks as described herein below.

[0060] Figure 2 depicts a monetary transaction architecture 200 similar to that described in Figure 1. The monetary transaction architecture 200 may provide a more 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 cloud-based transaction system 210. The profile includes the subscriber's know your customer (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 native or third party mobile wallet application 207.

[0061] The subscriber can indicate, using the mobile wallet 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 220 and/or a transaction database 225.

[0062] 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 221 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 entity such as a user or agent (e.g. customer 222) to or from an establishment such as an agent terminal (i.e. a retail store or agent company) 223.

[0063] In some cases, the cloud-based transaction system 210 provides a web interface that allows subscribers of third party mobile wallet applications to perform the same functions provided for native subscribers. For instance, mobile wallet application 207 may provide a web interface that allows a user to enroll for a native or third party mobile wallet. The web interface (or the mobile wallet application itself) receives a subscriber-initiated transaction over one of a plurality of communication channels (111 from Figure 1) connected to the cloud-based 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 communication 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.

[0064] Once the subscriber has an account, the cloud-based transaction system generates (or allows the third party provider to generate) 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 third party or native mobile wallet functionality described herein.

[0065] 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.

[0066] 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 third party mobile wallet, adding a stored value account (either hosted by an electronic payment system or a third party), adding a bank/credit union account to a third party mobile wallet, adding a debit/credit card account to a third party mobile wallet, depositing funds in a third party mobile wallet, withdrawing funds from a third party mobile wallet, paying bills from a third party mobile wallet, topping up a prepaid mobile account through a third party mobile wallet, transferring funds through a third party mobile wallet, making in store purchases from a third party mobile wallet, or transferring money or eMoney from one business account to another business account (i.e. from one business's mobile vault to another business's mobile vault, as will be shown in Figure 4).

[0067] Figure 3A depicts a subscriber-to-subscriber eMoney transfer. In a merchant and distributor scenario, either or both of the merchant and the distributor (including any delivery personnel) may be subscribers. To perform such a transfer, subscriber A (301) 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 (302). 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 cloud-based platform subscribers, one or both of which may be unbanked. The cloud-based 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.

[0068] Figure 3B illustrates a subscriber-to-non-subscriber eMoney transfer. Accordingly, as mentioned above, either or both of the merchant and the distributor may be non-subscribers. In graphic 305, subscriber A wishes to send eMoney to another individual that is not a subscriber to the cloud-based transaction 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 cloud-based transaction system 210 cannot credit them with eMoney. Instead, the cloud-based 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 (306). The cloud-based 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.

[0069] 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 cloud-based transaction 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 (307) and the user leaves with the cash in hand (308). The cloud-based transaction platform processes the transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction details to a platform-specified bank.

[0070] Figure 4 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 cloud-based transaction platform and are able to accept native and third party 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 (401) and credits the agent branch's eMoney account (402). 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 processes the purchase request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends transaction details to a cloud-based transaction platform-specified bank.

[0071] In one embodiment, the cloud-based 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 channel 111. 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 native or third party mobile wallet.

[0072] 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 and receives a subsequent agent branch communication over a channel indicating that the purchase code has been presented to an agent (branch). The monetary transaction system 210 validates the status of the specified payment method, determines if the specified payment method can accommodate a purchase for the specified amount, performs a limit check and/or a velocity check on the selected payment method, debits the specified payment method by the specified amount of funds, returns a notification to the agent branch authorizing the purchase and sends a receipt to the unbanked subscriber over a communication channel. The cloud-based transaction system 210 may thus be used in this manner to make a retail purchase using a native or third party mobile wallet.

[0073] Figure 5 depicts a physical environment and corresponding computer system architecture 500 for allowing a user to participate in various services using a native or third party mobile wallet (e.g. 511). Some of these services include allowing the user 507 to access disruptively priced or free financial services or items in exchange for participation in opt-in advertising. The environment 500, like the scenarios described in Figures 3A, 3B and 4, involves the use of a native or third party mobile wallet application 511. The mobile wallet application 511 can be used to provide disruptively priced or free financial services or items in exchange for participation in opt-in advertising. The mobile wallet application may be run on any type of digital device including a mobile phone, tablet, laptop or other digital device. Embodiments include providing digital data (e.g., coupons or vouchers) for obtaining disruptively priced or free items (e.g., consumer goods or groceries) to such digital devices.

[0074] In some embodiments, a user has an account with a mobile payment system. The cloud-based transaction system (e.g. 210 of Figure 2 or electronic payment system 521 of Figure 5) can provide the user 507 with a variety of functionality including purchasing items (see Figure 4), depositing funds, withdrawing funds, transferring funds (see Figures 3A and 3B), and others all from a third party wallet. Accordingly, the user can use a digital device to interact with the electronic payment system 521 to pay for goods and/or services.

[0075] In exchange for some type of financial benefit, the user opts in to receive advertisements. The financial benefits may include coupons, vouchers, promotions, Buy One Get One ("BOGO") offers or any other type of benefit (such as a reduced cost or free financial service or good) from the electronic payment system. The benefit may be targeted to the user based on the user's age, location or other demographic information, or based on the user's past purchases. At least in some embodiments, when the user agrees to participate in opt-in advertising, the electronic payment system 521 is permitted to store (e.g., by capturing purchase orders), track, and analyze items that the user purchases through their account with the electronic payment system. The electronic payment system stores and maintains lists of the users' purchased items in a data warehouse. The electronic payment system may also store information about the user (anonymous or otherwise) including age, income level, an indication of whether kids are in the family, or other information that may be useful in targeting ads or benefits to the user.

[0076] The electronic payment system analyzes 534 the users purchasing habits to identify advertisements and/or promotions that may be of interest to the user. The advertisements and/or promotions can be for items the user has purchased 503. The advertisements and/or promotions can also be for items related to items the user has purchase. For example, if user has purchased a particular brand of razor, advertisements for the brand's shaving cream can be identified. Advertisements for related items can also be used for cross-promotion.

[0077] From time to time, at specified intervals, or based on location (e.g., having a coupon for a merchant this is with a specified proximity) the electronic payment system sends identified advertisements and/or promotions to the user's digital device. When specified advertising thresholds are satisfied (e.g., a specified number and/or type of advertisements and/or promotions are presented), the electronic payment system confers a financial benefit on the user's account. For example, the electronic payment system can provide the user's account with a low cost (e.g., reduced fee) or free financial service, such as, for example, one reduced cost bill pay or one free bill pay. Alternately, the electronic payment system can provide the user's account with a coupon or voucher for an item (e.g., an item a user has pre-selected or an item the user has purchased in the past).

[0078] In some embodiments, a client application for the electronic payment system runs on the user's digital device (e.g. mobile wallet application 511). The user interacts with the electronic payment system through the client application. From a screen of the

client application, the user can agree to accept opt in advertising. Accordingly, embodiments of the invention essentially permit a user to self-monetize themselves through their digital device.

[0079] As further depicted in Figure 5, computer architecture 500 includes digital device 508, retail location 502, and electronic payment system 521. Digital device 508 further includes mobile wallet application 511. Retail location 502 further includes its own mobile wallet application 512. Electronic payment system 521 includes marketing module 533, data warehouse 532, advertisements 538, payment processor 522, user mobile wallet 524 (user 507's mobile wallet), and merchant mobile wallet 526 (retail location 502's mobile wallet).

[0080] Generally, each company in packaged goods companies 571 (or retailers that sell the packaged goods or other goods or services) can send advertisement data to electronic payment system 521. Advertisements 538 represent the collection of advertisement data sent from packaged goods companies 571. Each company in packaged goods companies 571 can also submit benefit rules to electronic payment system 521. Benefit rules 578 represent the collection of benefit rules sent from packaged goods companies 571. Benefit rules 578 define when a benefit, such as, for example, a free financial service, a coupon, a promotion, etc, is to be granted to a user of electronic payment system 521. For example, in response to completing a questionnaire linked to a product advertisement, a user can be given a coupon for the product or for a related product.

[0081] In general, user 507 can use native or third party mobile wallet application 511 to pay for goods purchased at retail location 502 (as shown in Figure 4). For example, user 507 can use mobile wallet application 511 to purchase goods 503. To pay for goods 503, mobile wallet application 511 can send payment instruction 543 in amount 563 to electronic payment system 521. Payment processor 522 can receive payment instruction 543. In response, payment processor 522 can debit 541 user mobile wallet 524 by amount 563. Payment processor 522 can also credit 542 merchant mobile wallet 526 by amount 563.

[0082] User 507 can use mobile wallet application 511 to participate in opt-in advertising. For example, user 507 can use mobile wallet application 511 to send opt-in 544 to electronic payment system 521. Advertising module 533 can receive opt-in 544 and record that mobile wallet application 511 has opted in for advertising. As such, when user 507 makes a purchase using mobile wallet application 511, a list of purchased items