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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 October 2012 (11.10.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/138432 A1

(51) International Patent Classification:
G06Q 40/00 (2012.01)

(21) International Application Number:
PCT/US2012/026612

(22) International Filing Date:
24 February 2012 (24.02.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/446,378 24 February 2011 (24.02.2011) US
61/537,985 22 September 2011 (22.09.2011) US

(72) Inventor; and
(71) Applicant *(for all designated States except US)*: **HARDIEK, Scott J.** [US/US]; 50405 Waterstone Court, Plymouth, Michigan 48170-8332 (US).

(74) Agent: **BUNTING, Beverly M.**; Butzel Long IP Docketing Department, 350 South Main Street, Suite 300, Ann Arbor, MI 48104 (US).

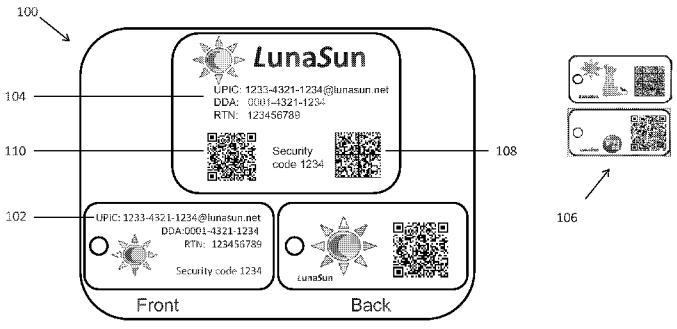
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, 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, 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:
— *with international search report (Art. 21(3))*

(54) Title: SYSTEM AND METHOD FOR FACILITATING VALUE EXCHANGE TRANSACTIONS BETWEEN DISTRIBUTED USERS

Fig. 1



(57) Abstract: A system and method for facilitating a value exchange using a universal identification card includes a payment exchange intermediary system server, a universal identification card having integrated identification information and a financial transaction card linked to the universal identification. The method encodes email account information on the universal identification card. The method links the financial transaction card with the universal identification card, engages the financial transaction card host provider via a communication network and links the identification of the card user with the universal identification card to facilitate the value exchange. The universal identification card is registered by associating the universal identification card with the financial transaction card.

WO 2012/138432 A1

SYSTEM AND METHOD FOR FACILITATING VALUE EXCHANGE TRANSACTIONS BETWEEN DISTRIBUTED USERS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of and priority to U.S. Provisional Application Numbers 61/446,378, filed February 24, 2011, and 61/537,985, filed September 22, 2011, both of which are incorporated herein by reference.

BACKGROUND

[0002] The present disclosure relates generally to a system and method for facilitating the exchange of value among distributed users through a universal token card.

[0003] Payment exchange intermediaries or transfer agents are available that facilitate value exchanges between two users of a system by using alias identifiers so that banking information is kept private. The alias identifiers are associated with underlying banking data which is used to conduct the value exchange transactions. In such a transaction, email addresses and phone numbers are generally used as an alias, and users need to register with the payment exchange intermediary in order to establish an association between the alias and the banking data.

[0004] While this process works, one of the difficulties experienced by individuals engaged in this process relates to the payment exchange intermediaries registration process. This registration process must be completed online (e.g., via a web browser) using a computer device (e.g., a desktop or laptop computer). However, certain individuals may be unable to complete this registration process, such as if they do not have access to the internet, do not own a computer device, or if they are a novice computer user. The foregoing is especially applicable to "unbanked" and "under-banked" market segments.

[0005] These unbanked individuals either do not maintain a formal bank account with a recognized federally insured financial institution or lean heavily toward the use of alternative financial providers such as check cashers or payday lenders. Accordingly, these "unbanked" individuals use alternative strategies for managing their cash flow. For example, an unbanked individual may utilize a check cashing service, such as that sponsored by a local retail outlet. The unbanked individual is usually charged a significant fee for such services. Another detriment is that the unbanked individual has the uncertainly of carrying cash versus maintaining funds in a secure institution.

[0006] In addition to the unbanked or under-banked segments, currently banked users could benefit from an easier method. These and other segments users could benefit from a payment exchange intermediary system that comes “ready for use” as part of an issued debit card account. Additionally, the existing payment exchange intermediary art requires the user to come to them and register with their service.

[0007] Thus, there is a need in the art for a cost effective system and method of providing value exchange transactions among distributed users.

SUMMARY OF THE DISCLOSURE

[0008] Accordingly, a system and method of facilitating a value exchange using a universal payment indicator code token card is provided. The system includes system for facilitating a value exchange using a universal identification card includes a payment exchange intermediary system server; and a universal identification card having integrated identification information, and the integrated identification information includes an email address. The system further includes a financial transaction card configured to be linked to the universal identification card in the payment exchange intermediary system server using the integrated identification information via a communication network.

[0009] The method includes the steps of providing a universal identification card having integrated identification information associated with a card user embedded thereon. The method also includes the step of encoding email account information associated with an email account on the universal identification card, wherein the email account is hosted by a host provider. The method still also includes the steps of providing a financial transaction card and linking the financial transaction card with the universal identification card so that the financial transaction card is usable in the value exchange. The method further includes the steps of configuring the financial transaction card to communicably engage the host provider via a communication network and linking the identification of the card user with the universal identification card to facilitate the value exchange.

[0010] A method for registering a universal identification card for use in a value exchange with a host computer system is also provided. The method includes the steps of receiving by the host computer system, user identification registration information, via a communication network. The method further includes the steps of associating the user identification registration information with the universal identification card and associating the universal identification card with a financial transaction card.

[0011] An advantage of the present disclosure is that a system and method is provided for facilitating a value exchange transaction among distributed users. Another advantage of the present disclosure is that the value exchange transaction may be an electronic banking service that uses a universal bank account card. Another advantage of the present disclosure is that a system and method is provided that is based on an email account associated with the universal bank account. Still another advantage of the present disclosure is that a system and method is provided that provides a user with access to an email account hosted by a universal server and is not reliant on computer ownership by the user. Another advantage of the present disclosure is the user can have very little computer knowledge or even access. Another advantage of the present disclosure is that data transfer linkages are created to facilitate the value exchange transaction. A further advantage of the present

disclosure is that a system and method is provided that preserves the security of the user's identity. Still a further advantage of the present disclosure is that a system and method is provided that allows electronic deposit of funds into the user's account. Yet still a further advantage of the present invention is that a system and method is provided that is flexible so that the user has one card for multiple purposes.

[0012] Other features and advantages of the present disclosure will become readily appreciated as the same becomes better understood after reading the following description when considered in conjunction with the accompanying drawings.

DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 is a plan view of a universal token card.

[0014] FIG. 2 is another plan view of the universal token card of FIG. 1 and associated data.

[0015] FIG. 3 is a plan view of an example of a bundled universal token card and debit card.

[0016] FIG. 4 is a schematic view illustrating a system for conducting value exchange transactions using the universal token card of FIG. 1.

[0017] FIG. 5 is a schematic view illustrating a method of conducting a value exchange transaction in accordance with the system of FIG. 4.

[0018] FIG. 6 is a schematic view illustrating a method of a registration process for use with the method of FIG. 5.

[0019] FIG. 7 is a schematic view illustrating received data for the registration process of FIG. 6.

[0020] FIG. 8 is a schematic view illustrating a method of conducting a secure deposit using an alias bank account number and RTN in accordance with the method of FIG. 5.

[0021] FIG. 9 is a schematic view illustrating incoming and outgoing ACH node transactions.

[0022] FIG. 10 is a schematic view illustrating peer to peer interactions between multiple payment exchange intermediaries.

[0023] FIG.11 is a schematic view illustrating required information to initiate a payment.

[0024] FIG. 12 is a schematic view illustrating a contextual text payment and confirmation of user identity corresponding with a universal payment indicator code.

[0025] FIG. 13 is a schematic view illustrating an example of associating a loyalty program with a universal bank card.

DESCRIPTION

[0026] Referring to FIG. 1, a universal identification token card 100 is illustrated. The universal identification card 100 is essentially a plastic card with an integrated identification means for effectuating a transaction. The universal identification card 100 may be a wallet size which is comparable to a standard credit or debit card, a small key tag size which may be connected to a key ring or the like, or may include another shape or size. It should be appreciated that the examples illustrated herein regarding the size and shape of the universal identification card 100 are non-limiting.

[0027] The universal identification card 100 includes integrated identification which may be used as an alias to initiate or receive payments without revealing

underlying financial data. This alias is associated with banking data and is referred to as a Universal Payment Identifier Code (UPIC) 102. The universal identification card 100 is associated with this UPIC 102.

[0028] In addition to the UPIC 102, the universal identification card 100 may also include other identification data 104 such as a bank account number (DDA), a route transit number (RTN), a security pin number or code, and other identification data.

[0029] Various techniques may be utilized to incorporate the data on the card. For example, the UPIC 102 and identification data 104 may be printed on the card, encoded on the universal identification card 100 in a machine readable data format, such as a 2-dimensional bar code ,electronic or magnetic strip or the like. It should be appreciated that the universal identification card 100 may also include secondary data 106 such as an image of a user; an association, branding, customization, or a logo; or the like. Various examples of secondary data 106 are illustrated in FIG. 1.

[0030] The universal payment identifier code 102 may also have an UPIC email address string format 200, as illustrated in FIG. 2. Various formats may be employed to define the UPIC email address string format 200. In an example, the UPIC email address string format 200 may include a simple, unique and pre-defined alphanumeric account number. In another example, the UPIC email address string format 200 may include characters which are generated through an algorithm or the like. In a further example, the UPIC email address string format 200 may utilize a naming convention similar to a phone numbering system or other alphanumeric characters.

[0031] The universal payment identifier code 102, identification data 104, or secondary data 106 may each, or a combination thereof, be encoded into a bar strip on the universal identification card 100 or embedded thereon utilizing another technology. In an example, the universal identification card 100 may include embedded data related to the universal payment identifier code 102 utilizing a UPIC email address format 200.

[0032] Various encoding techniques may be utilized, such as using a QR code 108, a data matrix code 110, a barcode (not illustrated), a magnetic strip (not illustrated), or the like. It should be appreciated that various technologies may be employed to allow the universal identification card 100 to communicably interface with another device and thereby provide the greatest flexibility in utilizing various point-of-sale equipment.

[0033] The universal identification card 100 may also contain integral security features, such as a pin number, a security certificate, a key, a combination thereof or the like. These additional security features may be utilized to provide the user with a screening function from unwanted communications, such as spam or the like. These security features may be encoded into a bar strip on the universal identification card 100 as previously described. The universal identification card 100 may be pre-linked or associated with a debit card or general purpose reloadable (GPR) debit card in a manner to be described hereafter.

[0034] Referring to FIG. 2, an example of a key tag universal identification card 202 is illustrated. In this example, the same data (e.g., universal payment identifier code 102, identification data 104, etc.) which may be embedded, encoded, or listed on the universal identification card 100 may be included or associated with the key tag universal identification card 202. Accordingly, the key tag universal identification card 202 may also include other identification data 104 such as a bank account number (DDA), a route transit number (RTN), a security pin number or code, and other identification data. Additionally, the UPIC 102, other identification data 104 (e.g., DDA, RTN, or the like), and other data may be encoded into a 2D barcode on the key tag universal identification card 202.

[0035] Regarding the UPIC email address format 200 of the UPIC 102, the portion preceding the "@" symbol may be referred to as the *user id*, 204 or the local-part of the address. In an example, the UPIC 102 may be an account number or bank account (DDA) 206 which is associated with the key tag universal identification card 202 (or the universal identification card 100). The bank account

(DDA) 206 is a holding bank account associated with a payment exchange intermediary or a financial institution.

[0036] By utilizing a bank account number 206, such as the UPIC email address format 200 or a portion thereof, various advantages would be realized as a unique email account number or a separate bank account number may not need to be issued. For example, the user may be issued a unique string related to the UPIC 102 that does not include a portion or an entirety of a bank account number 208 included therein. Additionally, the bank account number 208 may be listed on a portion of the key tag universal identification card 202 or the universal identification card 100.

[0037] Reviewing further the UPIC email address format 200 of the UPIC 102, the portion succeeding the "@" symbol is referred to as a domain name 210 (e.g., "domain_name.com") The domain name 210 may be the hosted domain name of a payment exchange intermediary, or could be that of a financial or other partner 212. The route transit number is that belonging to the payment exchange intermediary system or it could be a financial institution or card network or other partner.

[0038] The UPIC102 may be utilized as an alias to make and receive payments through a payment exchange intermediary without revealing the underlying financial data. The banking RTN and account number (DDA) associated with the universal identification card 100 may be used to receive payments through an automated clearing house without revealing the underlying financial data, in a manner to be described.

[0039] The key tag universal identification card 202 or the universal identification card 100 may include other data such as a security code 214, which in the illustrated example, is shown on the card. The security code 214 may be used to determine if a user is in physical possession of the key tag universal identification card 202 or the universal identification card 100 as a security measure or for other uses. Additionally, the key tag universal identification card 202 or the universal identification card 100 may include a short code texting number 216, also known as "short codes." Short codes (or short numbers) are special telephone numbers which

are usually significantly shorter than a full telephone number. A short code texting number 216 may be utilized to address SMS or MMS messages from a predetermined service provider's mobile phone or a fixed phone. The user may use the short code texting number 216 during a payment initiation process to a payment exchange intermediary.

[0040] Referring to FIG. 3, an example of a combined bundled package 300 is illustrated. The combined bundled package 300 includes a universal identification card 100 and a debit or GPR debit card 302, or ATM card or the like. The universal identification card 100 also includes an alias identification or a universal payment identifier code (UPIC) 102.

[0041] In an example, the UPIC 102 may be issued to the user and not pre-existing. Additionally, the UPIC 102 is provided to the user on the universal identification card 100. The UPIC 102 is pre-associated for the user and provided as a combined bundled system 300 with a debit or GPR debit card 302, or the like The pre-association or bundling of the universal identification card 100 with the debit or GPR debit card 302 may occur at account inception or upon reissue of a current card account, etc. Additionally, the bundled package 300 may be obtained or sold at various locations and through various sales channels 304, including: retailers, direct mail, vending machine, kiosk, financial institution, internet, and the like. Further, a new and/or alternative method of registration may be employed, in a manner to be described hereafter. It should be appreciated that during the set up process, a user's identity may be confirmed by requiring a valid user identification. Advantageously, during the registration process in an example, the identity of the user may be completely verified. Also, in lieu of bundling, the UPIC and other data 305 may be issued on the debit card itself 302. In this scenario the UPIC is now listed and encoded on to the debit card and issued as a stand-alone product.

[0042] Referring to FIG. 4, a system for utilizing a payment exchange intermediary (PEI) or transfer agent system 400 for facilitating a value exchange is illustrated. The payment exchange intermediary 400 may make or receive payments to other users or systems by referencing a user unique alias ID or universal payment

identifier code (UPIC) 102 without revealing the underlying banking information or data. In an example, the universal payment identifier code (UPIC) 102 may include an email address or a phone number which may be utilized as an alias by a payment exchange intermediary instead of the underlying banking information or data. The UPIC 102 may be associated with underlying banking or financial data.

[0043] The payment exchange intermediary system 400 includes a host computer system having a database 402 which is configured to store various information, such as the UPIC 102 and underlying banking or financial data, identification data 104, secondary data 106, or the like. The stored information within the database 402 is utilized to facilitate value exchange transactions.

[0044] The underlying financial data corresponding with the UPIC 102 may include information related to a debit card, general purpose reloadable (GPR) debit card, credit card, bank account along with associated routing number, and the like. The database 402 is connected to a communications network 404 via a payment exchange intermediary system server 406. It should be appreciated that the database 402 may be situated within the system server 406 or may be situated external to the system server 406.

[0045] A user which accesses the payment exchange intermediary system 400 may utilize a communication device 408. Various types of communication devices may be utilized, such as a cell phone, computer, table computer, website or webpage, hosted application program interface (API), and the like. Through the communication device 408, the user may facilitate a value exchange transaction using the payment exchange intermediary system 400. Once a value exchange transaction has been facilitated by the user via the communication device 408, a predetermined data access call is made to the database 402, and the returned data is utilized to further facilitate a transaction with a financial institution via an automated clearing house (ACH) 410, a payment card network 412 gateway, or the like. The payment card network 412 includes various types of payment cards, including: credit, GPR debit, debit, and the like.

[0046] Referring to FIG. 5a, an example of a methodology is provided for use with the payment exchange intermediary system 400 for facilitating a value exchange from a payor 500 to a payee 502. This exemplary methodology may be used for peer to peer transactions, which include person-to-person (P2P), person-to-company (P2C), and company-to-person (C2P) or company to company (C2C) transactions.

[0047] The methodology begins at step 504 with a payor 500 utilizing a communication device 408 (e.g., a cell phone, computer tablet, and the like) to instruct the payment exchange intermediary system server 406 on the value of the user specified or intended exchange and identifies the payee 502 by a UPIC 102, email address, phone number, alternative identifier, or the like or a combination of the foregoing. The payor 500 may additionally include other remittance data such as a billing account number, notes related to the transaction, or the like. It should be appreciated that the user may directly interface with the payment exchange intermediary system server 406 or the user could access the server system 406 utilizing an application programming interface (API) or other type of interface situated on a financial partner or third-party website.

[0048] The methodology advances to step 506 with the payment exchange intermediary system server 406 facilitating the transaction by withdrawing funds from the payor's account utilizing the underlying financial instruments from a financial institution 508. The underlying financial instruments from the financial institution 508 may be provided via a bank, credit union, credit card company, and the like.

[0049] The methodology advances to step 510 with the payment exchange intermediary system server 406 transferring the withdrawn funds from the payor's underlying financial instruments from the financial institution 508 and depositing them into the payee's underlying financial institution and account 512. The deposited funds may include deductions therefrom related to fees.

[0050] The payor's underlying account 508 or the payee's underlying account 510 may have a holding bank account or demand deposit account (DDA) 514/516 which is associated therewith. These bank account or DDA accounts 514/516 may hold funds on hand or may be used to channel funds through to the user underlying financial instruments 508/512.

[0051] It should be appreciated that the payment exchange intermediary system 400 may complete the transaction using a payment card network, an automated clearing house (ACH) system, or the like.

[0052] Referring to FIG. 5b, another embodiment of a methodology for facilitating a value exchange between a payor and a payee is illustrated for a card not present type transaction. These transactions are generally utilized in a context where the payee 502 is a merchant. Additionally, for a card not present type transaction, the payee 502 (e.g., merchant) and the payor 500 may not be co-located at the same physical location. It should be appreciated that the following methodology may be applicable to other types of transactions beyond a card not present transaction.

[0053] The methodology begins at step 520 with a payor 500 utilizing a communication device 408 such as a cell phone, computer, tablet computer, or the like, instructing the payment exchange intermediary system server 406 regarding the value of the exchange but identifying themselves by their UPIC 102. The payor 500 in this step is interacting with the payment exchange intermediary system server 406 using an application programming interface (API) which may be located on a third party website 518, or the like. The foregoing step may be applicable to a transaction which originates on a merchant website during checkout to pay for merchandise. In such an example, the payee 502 (e.g., the merchant) may be connected to the payment exchange intermediary system server 406 through a webpage or the like using an API 518 of the payment exchange intermediary system 400.

[0054] The methodology advances to step 520 with the user via the hosted API 518 instructing the payment exchange intermediary system server 406 on the value of the user specified value or intended exchange and identifies the themselves, the

payor 500, by their UPIC 102. In an example, the communication between the payment exchange intermediary system server 406 and other devices of the payment exchange intermediary system 400 may be secured by secure sockets layer (SSL) or another type of encryption.

[0055] The methodology advances to step 522 with the payment exchange intermediary system server 406 initiating the transaction by withdrawing funds from the payor's account utilizing the underlying financial instruments from a financial institution 508. The underlying financial instruments from the financial institution 508 may be provided via a bank, credit union, credit card company, and the like.

[0056] The methodology advances to step 524 with the payment exchange intermediary system server 203 transferring the withdrawn funds from the payor's underlying financial instruments from the financial institution 508 and depositing them into the payee's underlying financial institution and account 512. The deposited funds may include deductions therefrom related to fees.

[0057] The payor's underlying account 508 or the payee's underlying account 510 may have a holding bank account or demand deposit account (DDA) 514/516 which is associated therewith. These bank account or DDA accounts 514/516 may hold funds on hand or may be used to channel funds through to the user underlying financial instruments 508/512.

[0058] It should be appreciated that the payment exchange intermediary system 400 may complete the transaction using a payment card network, an automated clearing house (ACH) system, or the like.

[0059] It should further by appreciated that there are various types of accounts which may be applicable to the payment exchange intermediary system 400, including: 1) a consumer account that makes and receives payments; 2) a merchant that generally receives immediate payment for goods and services; and 3) a recurring biller that generally receives payment upon the presentation of a billing statement, and other types are contemplated.

[0060] In an instance where a user does not have a communication device 408 to effectuate a transaction as a payor 500, they may still be the recipient of a transaction as a payee 502. The foregoing is an advantageous benefit to the at risk unbanked segment of the population which are more likely to experience intermittent or complete loss of cellular or data network access.

[0061] Referring to FIG. 6, a method related to a registration process is illustrated for use in a value exchange between a payor and a payee. The methodology begins at step 600 with providing to the user a combined bundled package 300 including a universal identification card 100 having a universal payment identifier code (UPIC) 102 and a debit or GPR debit card 302. This bundled package 300 may be offered for sale in many different locations and through various channels of commerce (physical or electronic). For example, the bundled package 300 may be sold via a merchant, direct mail, over the phone, kiosk, internet, and the like.

[0062] The methodology advances to step 602, and includes registering an account. The registration 602 may occur via various registration means utilizing a website, individual voice response system, call center, SMS text, mobile application, customer service representative, direct mail, and the like.

[0063] The methodology advances to step 604, and includes the step of providing user-provided data. The user may be required to provide personal data associated with the opening of a bank account. This user provided personal data may include items such as a name, address, social security number, driver's license number, and the like. The user can provide a phone number or pre-existing email address to be used as an additional or alternative UPIC in the system. Additionally, it should be appreciated that a cell phone number may be utilized as part of the system to facilitate the transaction. In such an instance, the cell phone number would likely be required to be authenticated.

[0064] The methodology advances to step 606, and includes the step of authenticating or verifying the user-provided data of step 604. In an example, the payment exchange intermediary system 400 may determine if the provided cellular telephone number is correct and corresponds with a given user. It should be

appreciated that other identifying user data may require verification including a social security number, driver's license number, and the like. The foregoing is not limiting as several other methods may be utilized to perform an authentication or verification of the user-provided data of step 604.

[0065] The methodology may advance further to step 607 with converting a financial institution's current debit account holder customers or users 607. This additional step is an important registration avenue as various entities including banks, credit unions, pre-paid agents, and the like already possess within their databases much of the information necessary to open an associated payment exchange intermediary account. However, such institutions lack some of the items necessary to complete the account as the UPIC alias and the payment exchange intermediary service. Working with the financial institutions the payment exchange intermediary will likely provide the needed items to complete and issue an account. This additional step may be accomplished during card issue or reissue, or the like. In such an instance, it should be appreciated that the user may not need to provide any additional data.

[0066] Referring to FIG. 7, a method related to providing data from various entities received during a registration process for use in a value exchange between a payor and payee is illustrated. It should be noted that to open an account, a user may be registering with may need to register with a financial institution and the payment exchange intermediary system 400 simultaneously. To complete an account, the following entities may be required to provide data to the payment exchange intermediary system 400.

[0067] The methodology begins at step 700 with the user providing user provided data. The user provided data may include a name, address, phone number, social security number, driver's license number, and the like.

[0068] The methodology advances to step 701 and includes the step of the financial institution providing various banking data such as a DDA, RTN, or the like.

[0069] The methodology advances to step 702 and the financial institution/card network provides data relating to the physical debit or GPR debit card.

[0070] The methodology advances to step 703 and includes the step of the payment exchange intermediary providing information relating to the transaction, such as a UPIC identification, a holding bank account number, route transit number, and other data. In an example, the financial institution may supply the holding account information.

[0071] The methodology advances to step 704 and includes the step of the financial institution or the payment exchange intermediary providing the physical universal token card. If the payment exchange intermediary provides the physical universal token card, the financial institution and the payment exchange intermediary servers and databases would need to interact and synchronize.

[0072] The methodology advances to step 704, and includes the step of a user adding additional pre-existing accounts, such as new credit cards, or other debit or GRP cards, to the account during the registration process or at a later time.

[0073] It should be appreciated that if the payment exchange intermediary is able to partner with a financial institution, the financial institution could convert existing users as discussed previously with reference to FIG. 6. In such an instance, the financial institution could provide all the necessary users' data needed for the payment exchange intermediary for issuance of a new account. Conversely, if the payment exchange intermediary system is unable to partner with financial institutions such as issuer banks, the banking financial data required would need to be supplied by the user entirely. If not packaged with an issuing financial partner, the token card and system may be offered as a stand-alone product. In such an instance, the user would have to provide a pre-existing debit, GPR debit, or credit card information to the system, and the user provided data would need to be verified.

[0074] Referring to FIG. 8, a method is illustrated for depositing an incoming deposit using the ACH clearing house for the value exchange between a payor and payee.

[0075] The methodology begins at step 801 with the step of making an incoming deposit to an alias holding bank account 802 controlled by a payment exchange intermediary, the issuer bank, or the card network via the ACH clearing house. The alias bank account information may be listed on a universal token card. The data includes a route transit number and a bank account number (DDA).

[0076] It should be appreciated that the true or underlying issuing banking account data (RTN and user's bank account number) is not located on the token card as this data is kept private. However, this true or underlying issuing banking account data is known by the payment exchange intermediary, the issuing financial institution, and possibly the issuing card network. This underlying data is maintained in a database 803, and this information may or may not be provided to the user.

[0077] The payment exchange intermediary receives the incoming deposit 801 to a holding account. Whenever the system detects an incoming ACH deposit it begins the next step of the methodology.

[0078] The methodology advances to step 804 and includes the step of the system redirecting the incoming deposit to the underlying or masked account of the issuing bank. The payment exchange intermediary takes the alias account data and references the true underlying issuing bank institution's RTN and the user bank account number (DDA) from its database 803.

[0079] The methodology advances to step 806 and includes the step of the payment exchange intermediary using the data of the former step for initiating another ACH transfer to the users issuing bank (RTN) 805 and into the user account (DDA) 806. The payment exchange intermediary redirected the original deposit from the holding account to the user underlying account. The payment exchange intermediary acted as an ACH transfer agent. The deposit is made without revealing the underlying banking information to the party making the original deposit.

[0080] Referring to FIG. 9, an ACH node is defined as the address of a financial institution. The address is represented by a unique number known as the Route

Transits Number (RTN). In this example, the ACH incoming transfers can come from any other ACH node 900. These nodes can be other banks or they can be other institutions such as payroll servicers, other transfer agents, etc. Once a transaction comes into the users account held at the Payment Exchange Intermediary 901 it is re-directed or forwarded to the underlying issuing bank or institution 902, as previously discussed. The underlying user's financial institution RTN is a second node 902. The second node financial information is controlled and the access to making outgoing transactions is limited. Only the Issuing financial institution/card network 903 and the Payment Exchange Intermediary 904 know the users underlying banking node and account. Therefore, only these institutions can facilitate an outgoing transaction from this node. This provides for not only secure direct deposits but limits the risk of unauthorized outgoing transfers because the account can only be accessed by these institutions. Alternatively, in another example, the transfer may be implemented only by a financial institution for an added security benefit and not tied to a payment exchange intermediary. In this case only the financial institution would know the underlying banking information.

[0081] Referring to FIG. 10, an additional advantage of the system is illustrated, demonstrating that similarly structured payment exchange intermediaries can make ACH payment transfers using the data available on the universal UPIC token card. Similarly, System A 1001 can facilitate transfers to users of the System A 1003 and System B 1004. As shown in FIG. 10, System B 1002 can facilitate transfers to Users of the System A 1003 and System B 1004. These peer to peer transactions can be P2P, P2C, C2P and C2C transfers conducted through an ACH gateway.

[0082] Today, payment transactions can be facilitated using a simple messaging system text system. The current art requires the user to place all the information within one text. The information includes who to pay and how much. in such an instance, the text becomes very much coded in nature. Also, such an instance may require a substantial amount of information to place in just one text. An improvement is to break up the text to more closely follow a conversation or dialog. Referring to Fig. 11, typical information associated with a paper check is illustrated. The

information includes data such as who to pay 1101, how much to pay 1102, amount of the payment 1103, and when to pay 1004 is universal in nature and is common to a paper check or to an electronic peer-to-peer transaction.

[0083] Figure 12, illustrates an example of a conversational payment texting used for a value exchange between a payor and payee. Conversational payment texting is the process of making a payment through text using several text exchanges between the user and the payment exchange intermediary. The texts form a conversation between the user and the payment exchange intermediary. The conversation is an exchange of information on the requested transaction. The conversation answers predetermined questions to effectuate the transaction, such as who 1201, how much 1202, what (memo) 1203 and when (not shown). The end result is a flow of texts back and forth that more closely follow a dialog or conversation. Also, one of the most important parts is the conformation of the exact person's identity 1205. Especially with a user id of email address and phone number it is easy to mistype a character. Mistyping a single charter could mean the payment to an unintended recipient. This is why it is important to confirm the actually payee real name or entity to the payor as conformation before processing or completing the transaction. This conformation of the Payee's real identity is also applicable other types of payment entry such as a smart phone app, webpage, API and etc.

[0084] Referring to Figure 13, a method of using the token card at a POS merchant to effectuate a value exchange between a payor and payee is illustrated. The merchant can also choose to use the UPIC unique and ubiquitous standard identification for loyalty programs or virtual receipts. In this example, the universal token card is being used in the manner of a loyalty card. The method includes the steps of the user presenting the token card 1300 to a merchant, and the merchant scans or reads the information contained on the card 1301. The universal token UPIC identification is used as an alternative identification for a merchant's loyalty program. A registered account of the consumer's account is cross-referenced within the merchant's database servers 1302. After scanning the token card the merchant

proceeds with the transaction 1303. The transaction can be any transaction for goods or services 1304. The merchant updates the loyalty account as appropriate.

[0085] Once the transaction is complete, the merchant gives the consumer a hard copy of the receipt 1305, and the merchant may send a copy to their 1306 for storage in their database 1302 and may also send an electronic copy to an email address of the user declared email address 1308. The merchant server 1307 does not have to interact with the payment exchange intermediary. The user's server may pick up the message and place into a folder associated with the user's inbox 608. The message may be a receipt, or warranty or other product information.

[0086] The present disclosure has been described in an illustrative manner. It is to be understood that the terminology which has been used is intended to be in the nature of words of description rather than of limitation. Many modifications and variations of the present example are possible in light of the above teachings. Therefore, within the scope of the appended claims, the present disclosure may be practiced other than as specifically described.

WHAT IS CLAIMED IS:

1. A method of facilitating a value exchange using a universal identification card, said method comprising the steps of:

providing a universal identification card having integrated identification information of a card user embedded thereon;

encoding email account information associated with an email account on the universal identification card, wherein the email account is hosted by a host provider;

providing a financial transaction card;

linking the financial transaction card with the universal identification card so that the financial transaction card is usable in the value exchange, wherein the financial transaction card is configured to communicably engage the host provider via a communication network; and

linking the identification of the card user with the universal identification card to facilitate the value exchange.

2. The method of claim 1, wherein the financial transaction occurs at a point of sale.

3. The method of claim 1, wherein the host provider is a payment exchange intermediary system server connected to an electronic network associated with a financial transaction.

4. The method of claim 1, wherein the integrated identification information includes a predetermined access code.

5. The method of claim 1, wherein the integrated identification information is selected from the group consisting of a user name, a user social security number, a user driver license number, and a user thumb print.

6. The method of claim 1, further comprising the step of encoding a security feature on the universal identification card.

7. The method of claim 1, wherein the financial transaction card is a reloadable debit.

8. A method for registering a universal identification card for use in a value exchange with a host computer system, said method comprising the steps of:

receiving by the host computer system, user identification registration information, via a communication network;

associating the user identification registration information with the universal identification card; and

associating the universal identification card with a financial transaction card.

9. The method of claim 8, wherein the universal identification card includes a universal payment identifier to link the financial transaction card with an automated clearing house network system.

10. The method of claim 9, wherein the universal payment identifier is an email address.

11. The method of claim 10, wherein the email address is pre-linked to the automated clearing house network system.

12. The method of claim 10, wherein the email address is predetermined.

13. The method of claim 9, wherein the universal payment identifier is a phone

number.

14. The method of claim 8, wherein the universal identification card includes a plurality of universal payment identifiers to link the financial transaction card with the automated clearing house network system.

15. The method of claim 9, further comprising the step of associating the universal identification card with the financial transaction card by comparing first security information of the universal identification card with second security information of the financial transaction card.

16. The method of claim 9, further comprising the step of associating the universal identification card with the financial transaction card by comparing first identification information of the universal identification card with second identification information of the financial transaction card.

17. The method of claim 9, further comprising the step of receiving funds for application to the financial transaction card using the universal payment identifier.

18. The method of claim 10, further comprising the step of receiving an invoice via the email address.

19. The method of claim 18, further comprising the step of paying the invoice via a payment application of a mobile device.

20. A system for facilitating a value exchange using a universal identification card, comprising:

a payment exchange intermediary system server;

a universal identification card having integrated identification information, wherein the integrated identification information includes an email address; and

a financial transaction card configured to be linked to the universal identification card in the payment exchange intermediary system server using the integrated identification information via a communication network to facilitate the value exchange.

Fig. 1

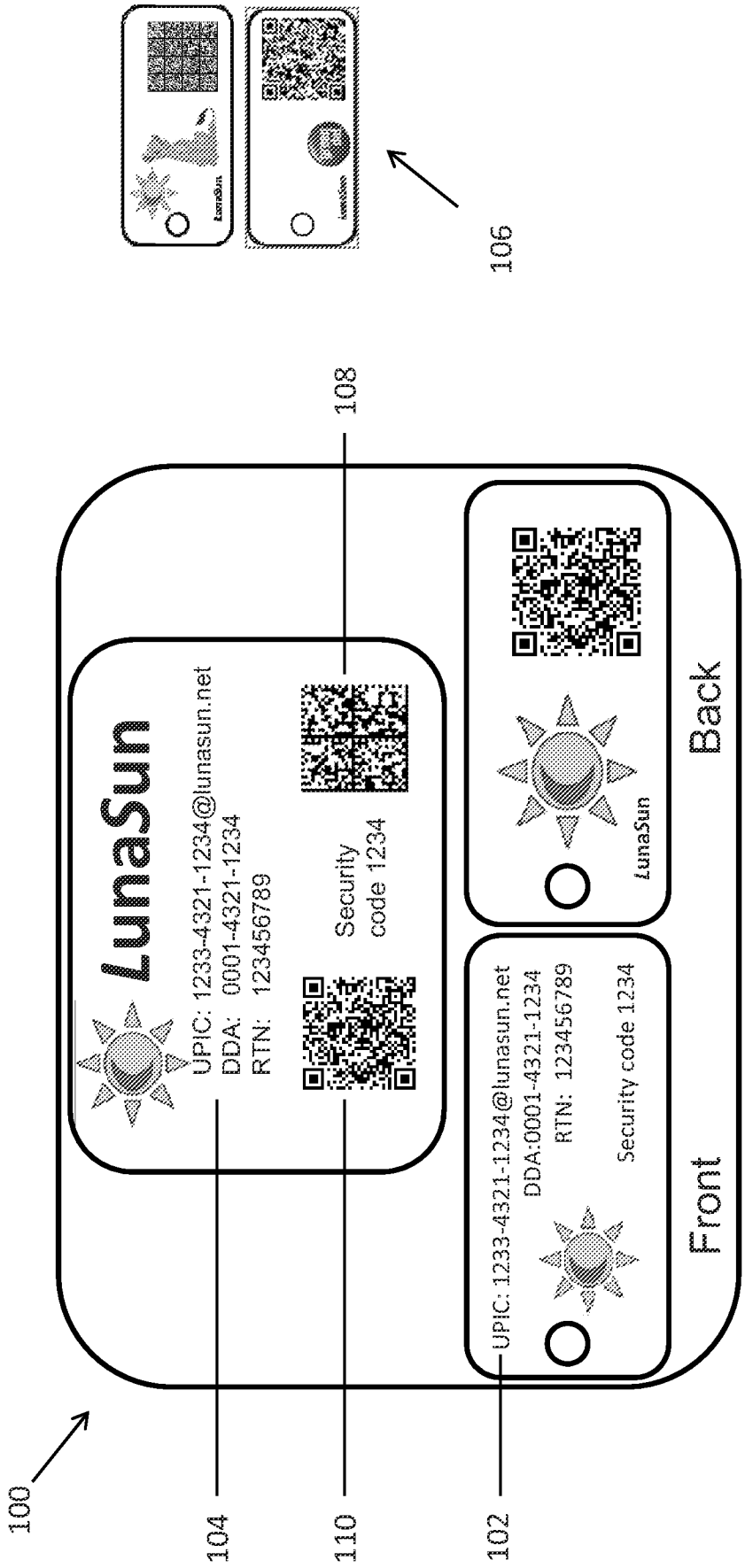

100
104
110
102
108
106
LunaSun
UPIC: 1233-4321-1234@lunasun.net
DDA: 0001-4321-1234
RTN: 123456789
Security code 1234
Front
Back
LunaSun

Fig. 2

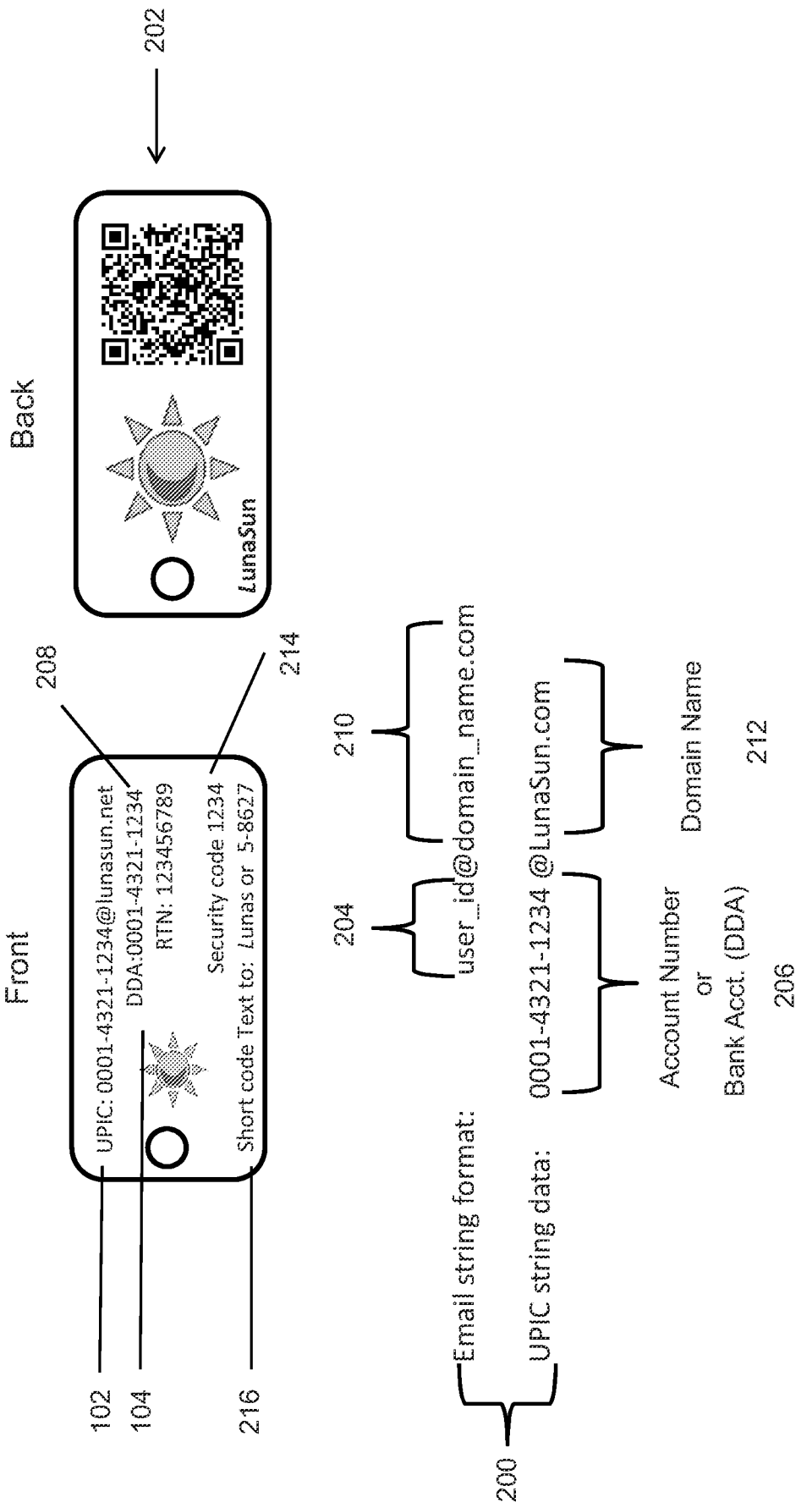

Front
Back
202
208
214
UPIC: 0001-4321-1234@lunasun.net
DDA:0001-4321-1234
RTN: 123456789
Security code 1234
Short code Text to: Lunas or 5-8627
LunaSun
102
104
216
200
Email string format:
UPIC string data:
204
210
user_id@domain_name.com
0001-4321-1234 @LunaSun.com
Account Number
or
Bank Acct. (DDA)
206
Domain Name
212

Fig. 3

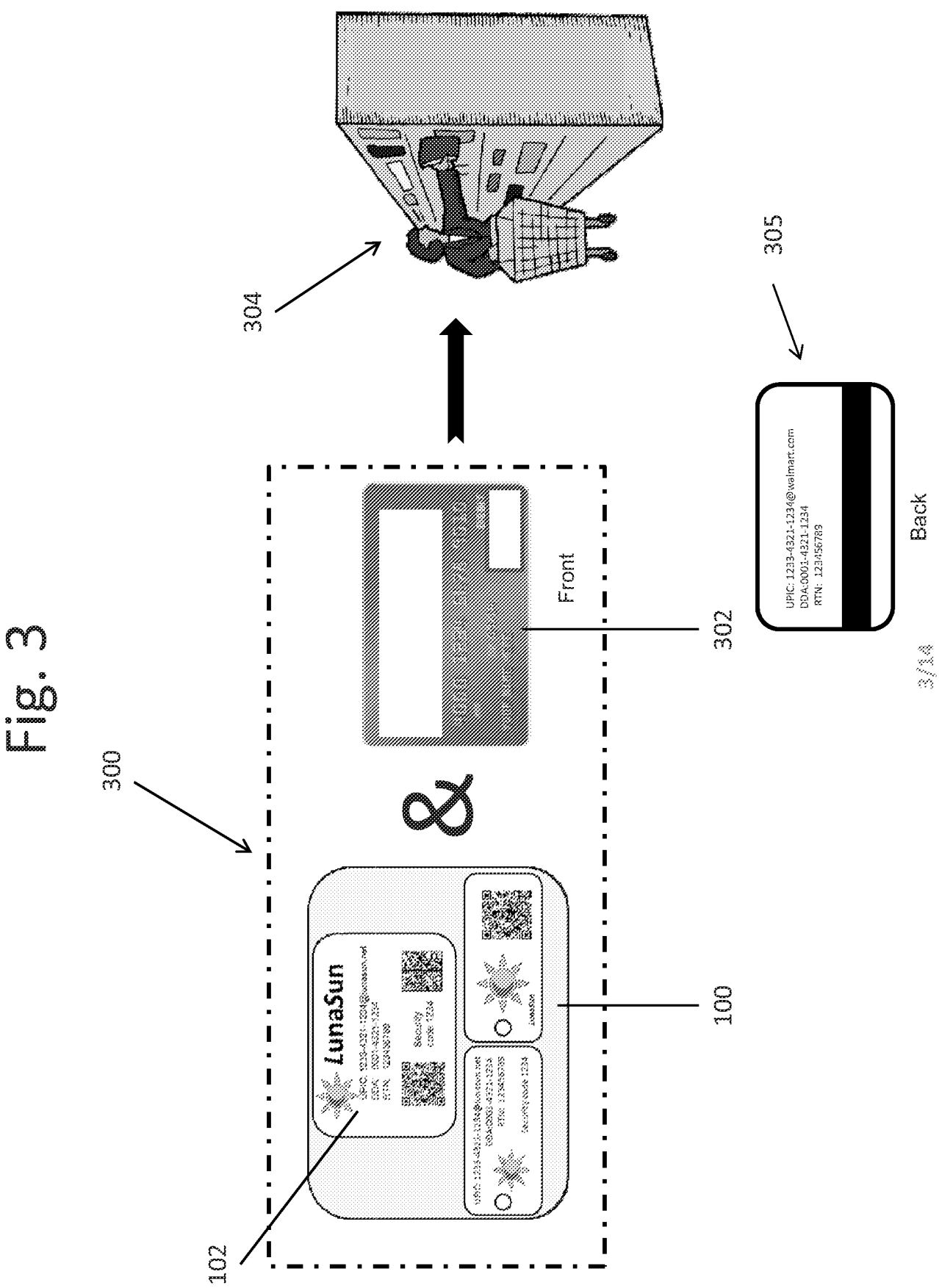

300
102
100
302
Front
Back
304
305
LunaSun
UPIC: 1233-4321-1234@walmart.com
DDA:0001-4321-1234
RTN: 123456789

Fig. 4

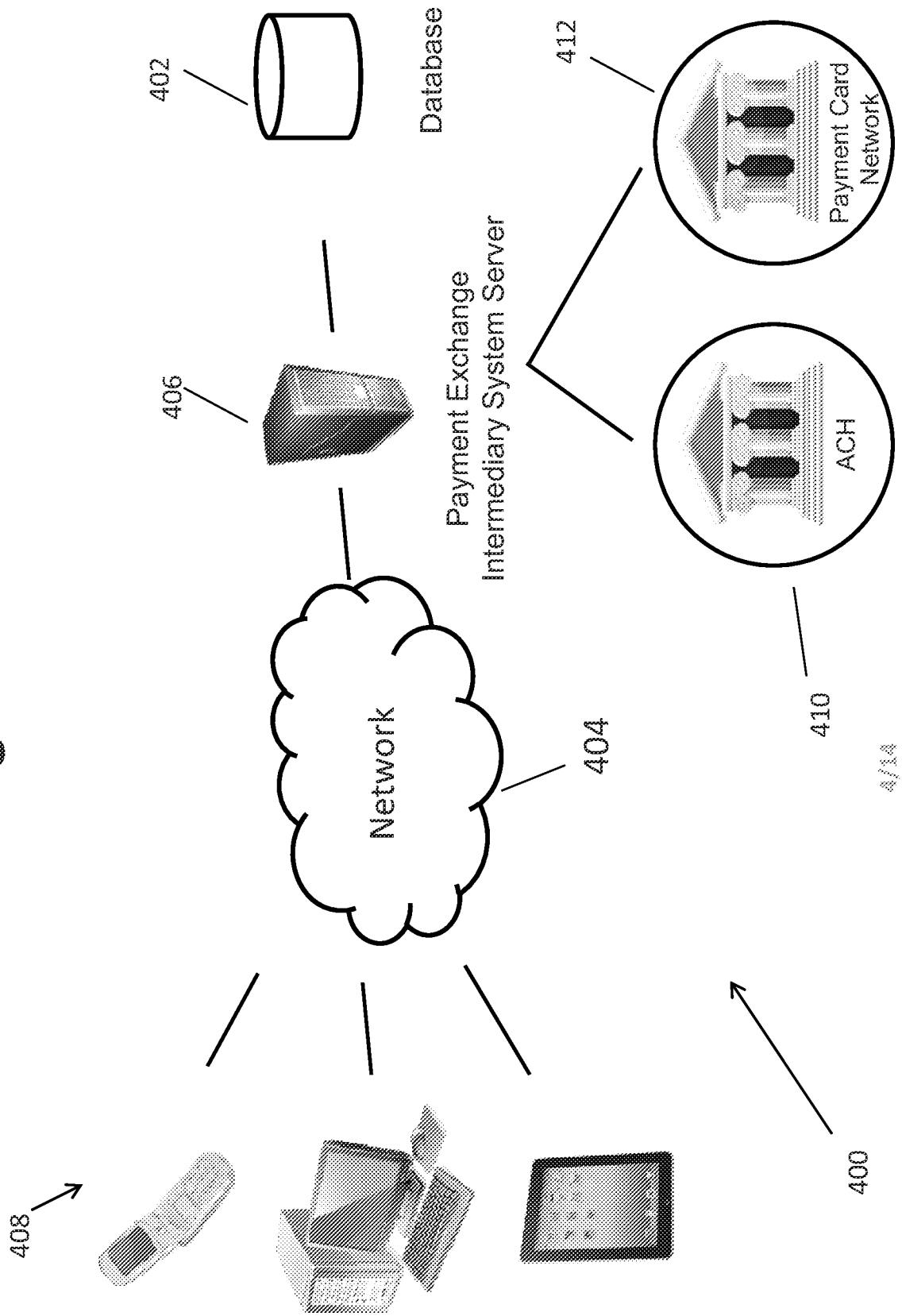

402
Database
412
Payment Card Network
406
Payment Exchange Intermediary System Server
ACH
Network
404
410
408
400

Fig. 5a

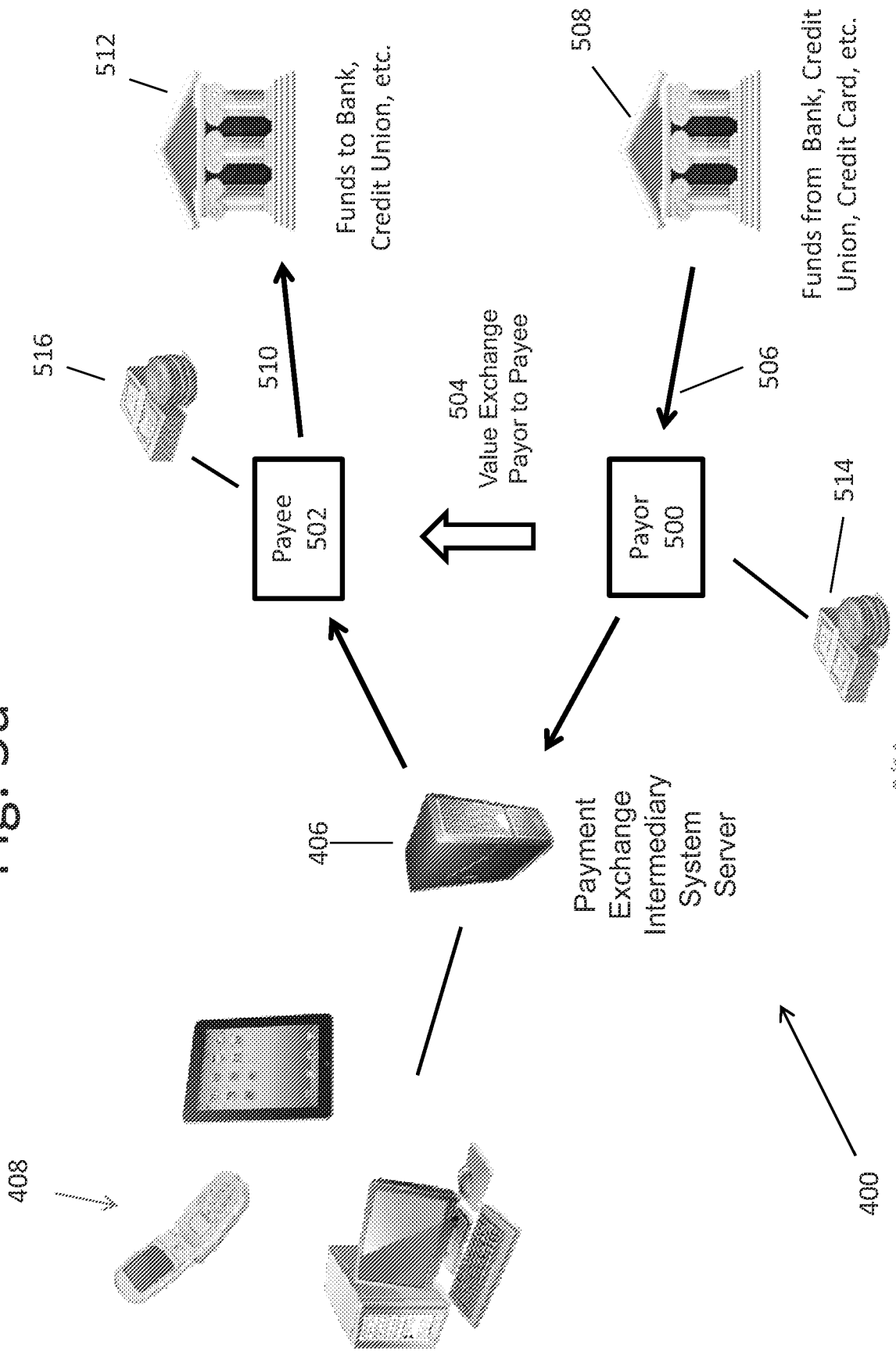

512
Funds to Bank, Credit Union, etc.
508
Funds from Bank, Credit Union, Credit Card, etc.
516
510
504
Value Exchange
Payor to Payee
506
Payee
502
Payor
500
514
406
Payment Exchange Intermediary System Server
408
400

Fig. 5b

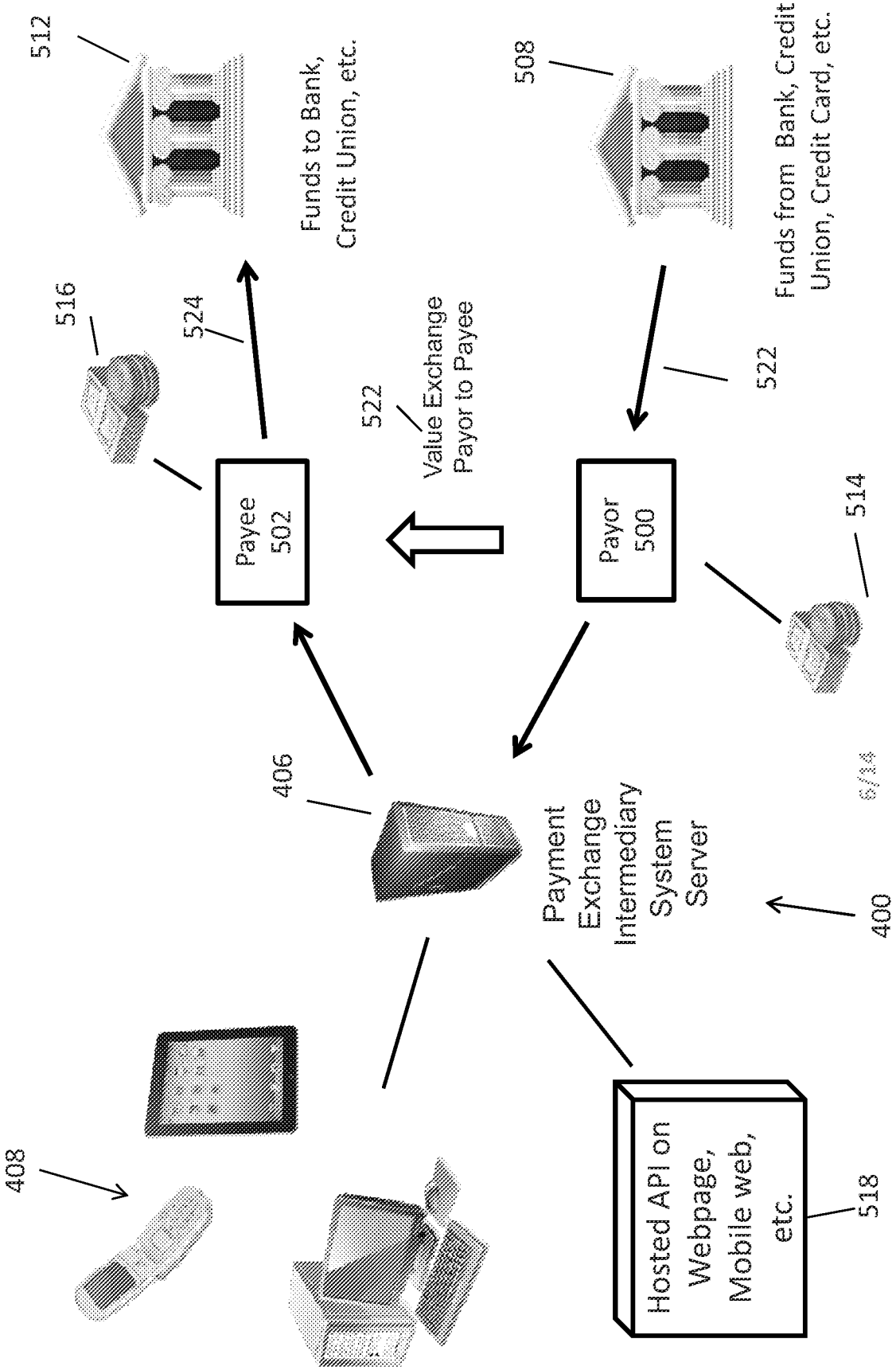
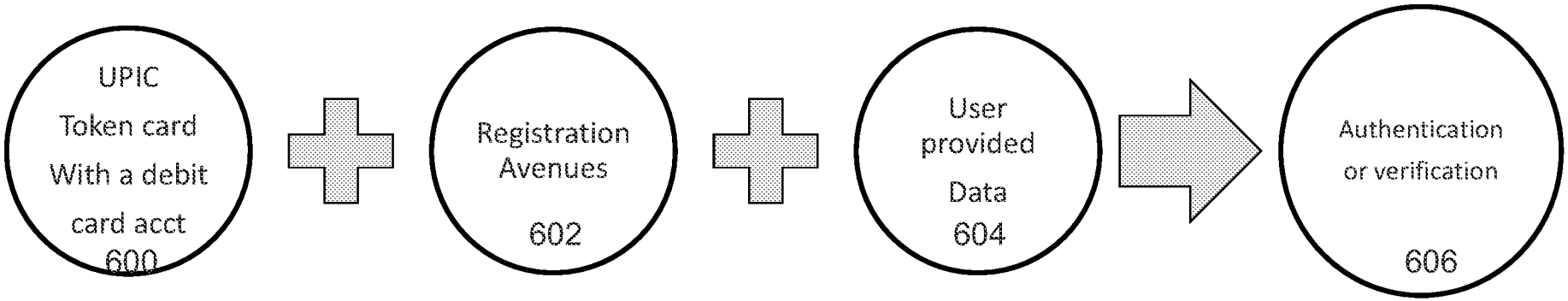
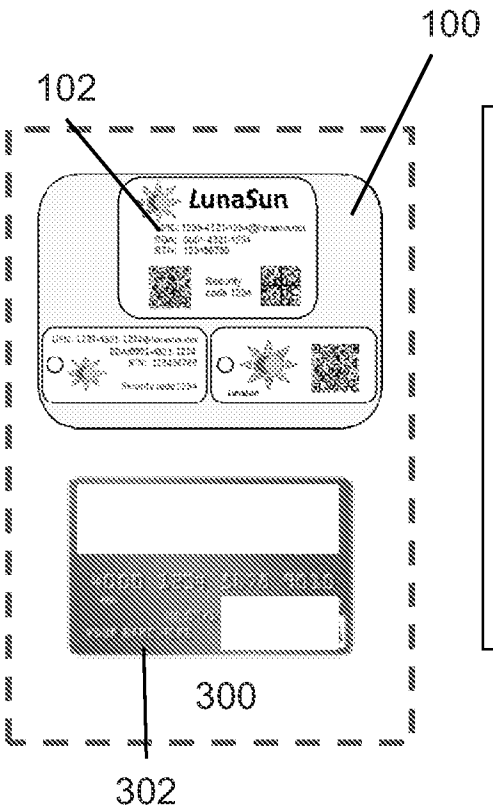

512
Funds to Bank, Credit Union, etc.
508
Funds from Bank, Credit Union, Credit Card, etc.
516
524
522
Value Exchange Payor to Payee
522
Payee 502
Payor 500
514
406
Payment Exchange Intermediary System Server
400
408
Hosted API on Webpage, Mobile web, etc.
518

Fig. 6

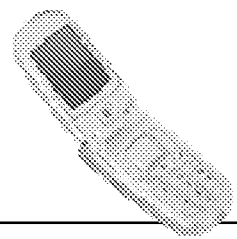




- Website
- IVR System
- Call Center
- SMS Text
- Customer Service Rep.
- Direct Mail.
- Current user database

607

- Name
- Address
- Social Security
- Driver's License
- Cell Phone number
- Alt. email
- etc



- Verify user supplied data

WO 2012/138432
PCT/US2012/026612

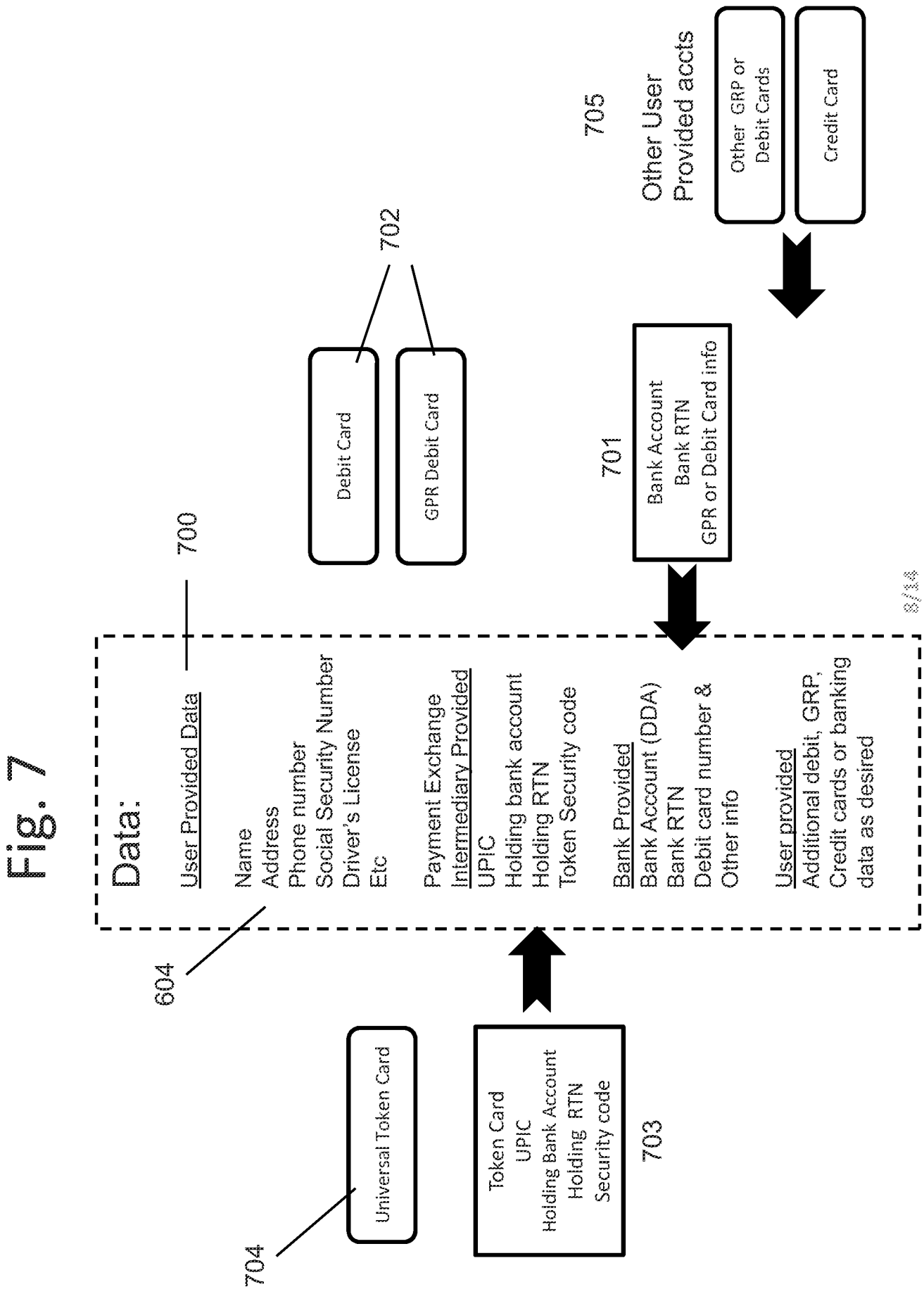


Fig. 7
Data:
User Provided Data
Name
Address
Phone number
Social Security Number
Driver's License
Etc
Payment Exchange Intermediary Provided
UPIC
Holding bank account
Holding RTN
Token Security code
Bank Provided
Bank Account (DDA)
Bank RTN
Debit card number &
Other info
User provided
Additional debit, GRP,
Credit cards or banking
data as desired
700
604
Debit Card
GPR Debit Card
702
Bank Account
Bank RTN
GPR or Debit Card info
701
Other User
Provided accts
Other GRP or
Debit Cards
Credit Card
705
Token Card
UPIC
Holding Bank Account
Holding RTN
Security code
703
Universal Token Card
704
8/14

Fig. 8

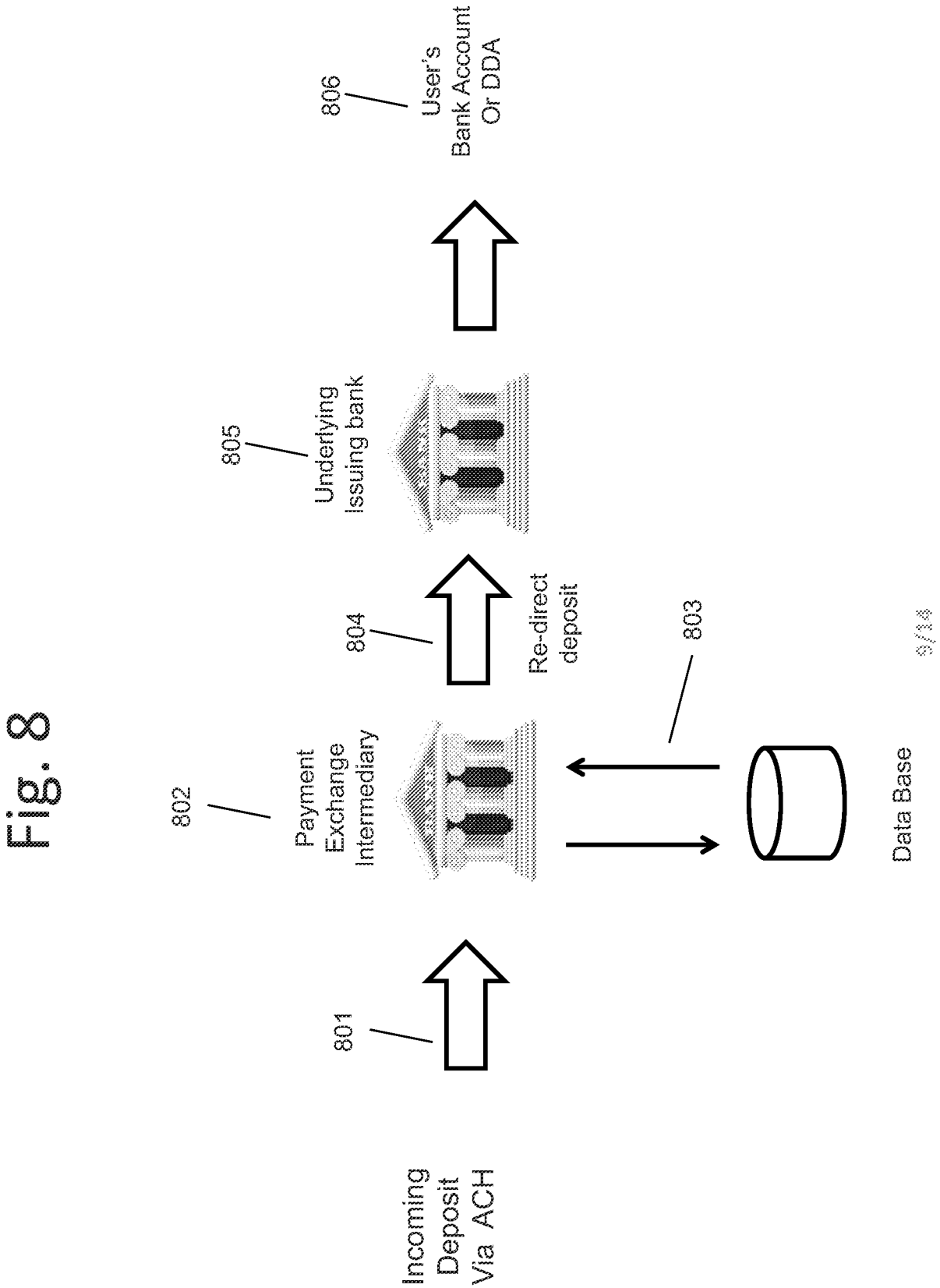

Incoming Deposit Via ACH
801
Payment Exchange Intermediary
802
Data Base
803
804
Re-direct deposit
Underlying Issuing bank
805
User's Bank Account Or DDA
806

Fig. 9

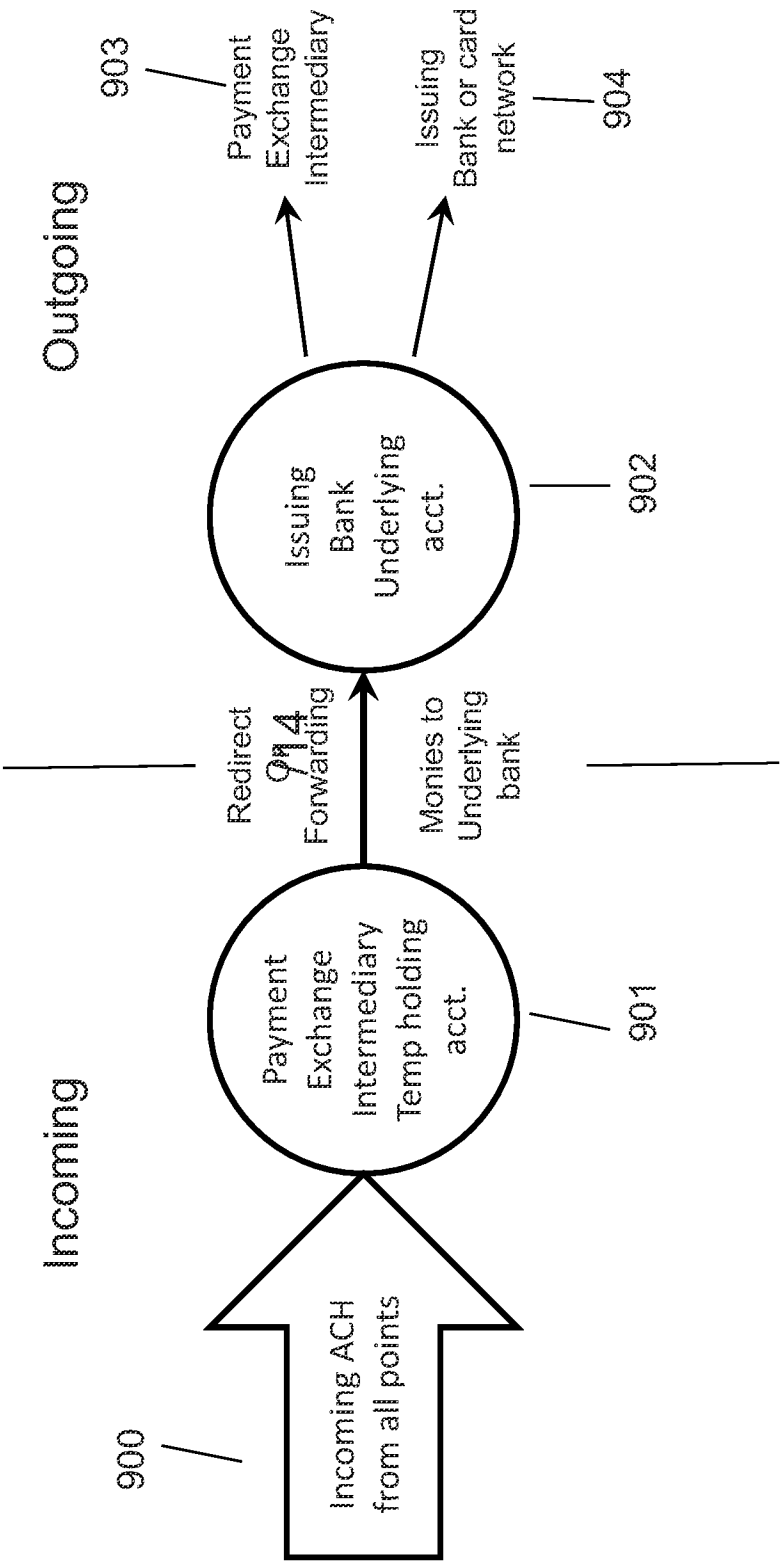

Incoming
Outgoing
900
Incoming ACH from all points
Payment Exchange Intermediary Temp holding acct.
901
Redirect Forwarding
914
Monies to Underlying bank
Issuing Bank Underlying acct.
902
903
Payment Exchange Intermediary
904
Issuing Bank or card network

Fig. 10

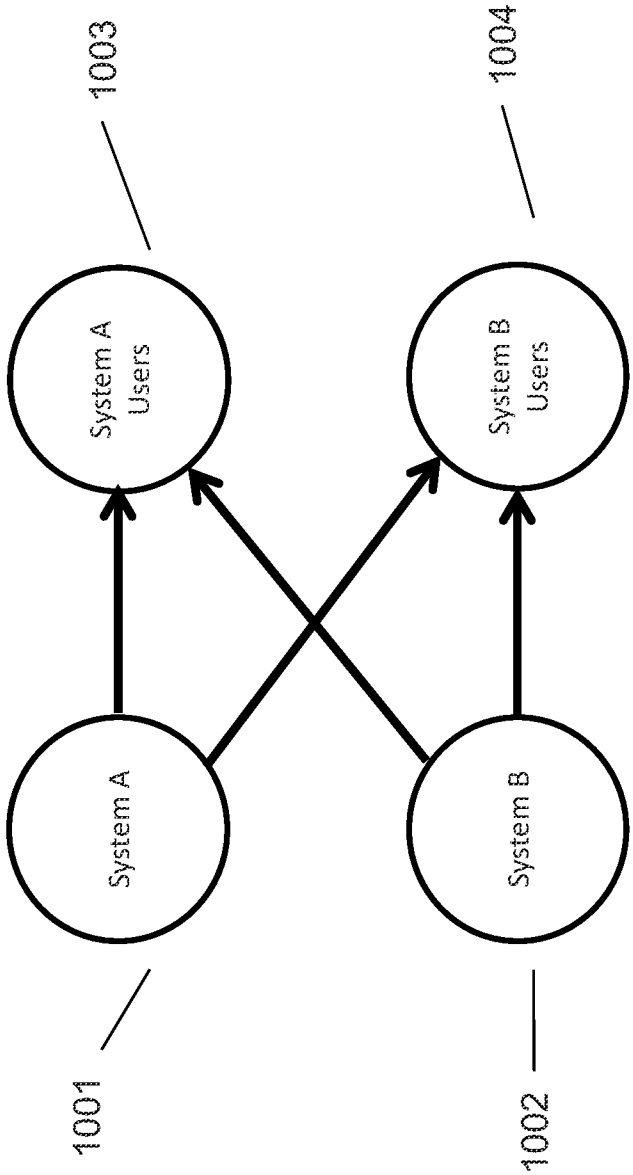

1003
1004
System A Users
System B Users
System A
System B
1001
1002

Fig. 11

Details need to make a payment

Needed Information

1101. Who to
1102. How (much)
1103. What (memo)
1104. When

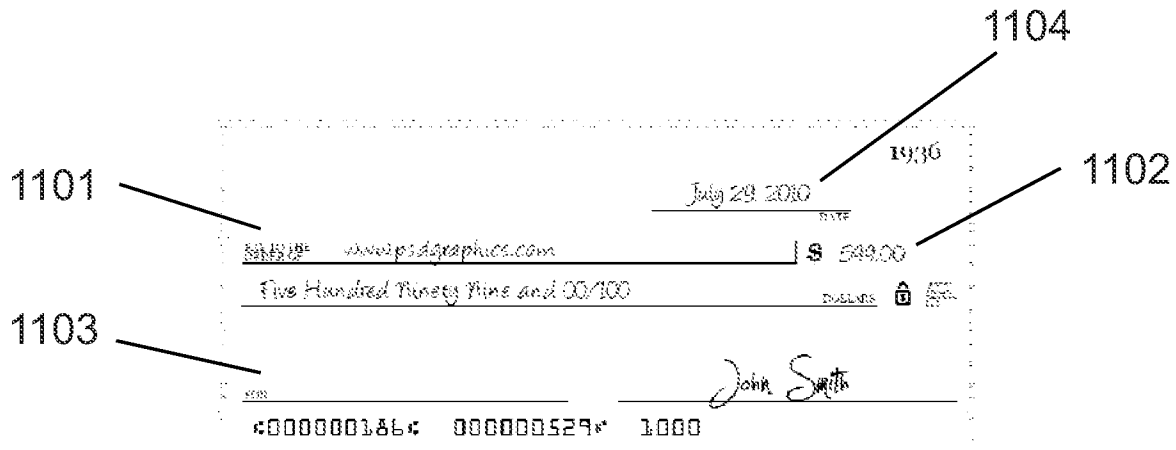
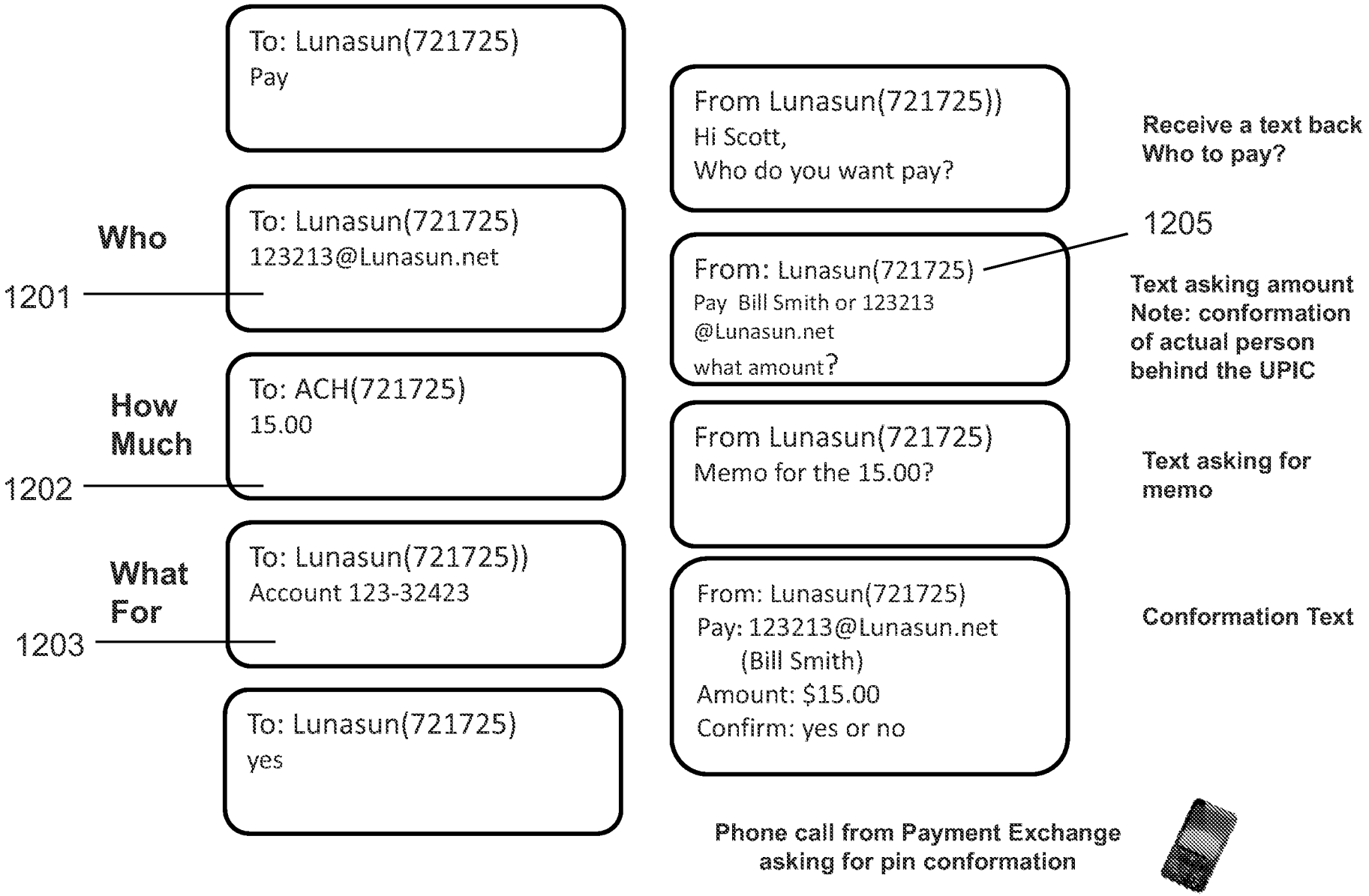
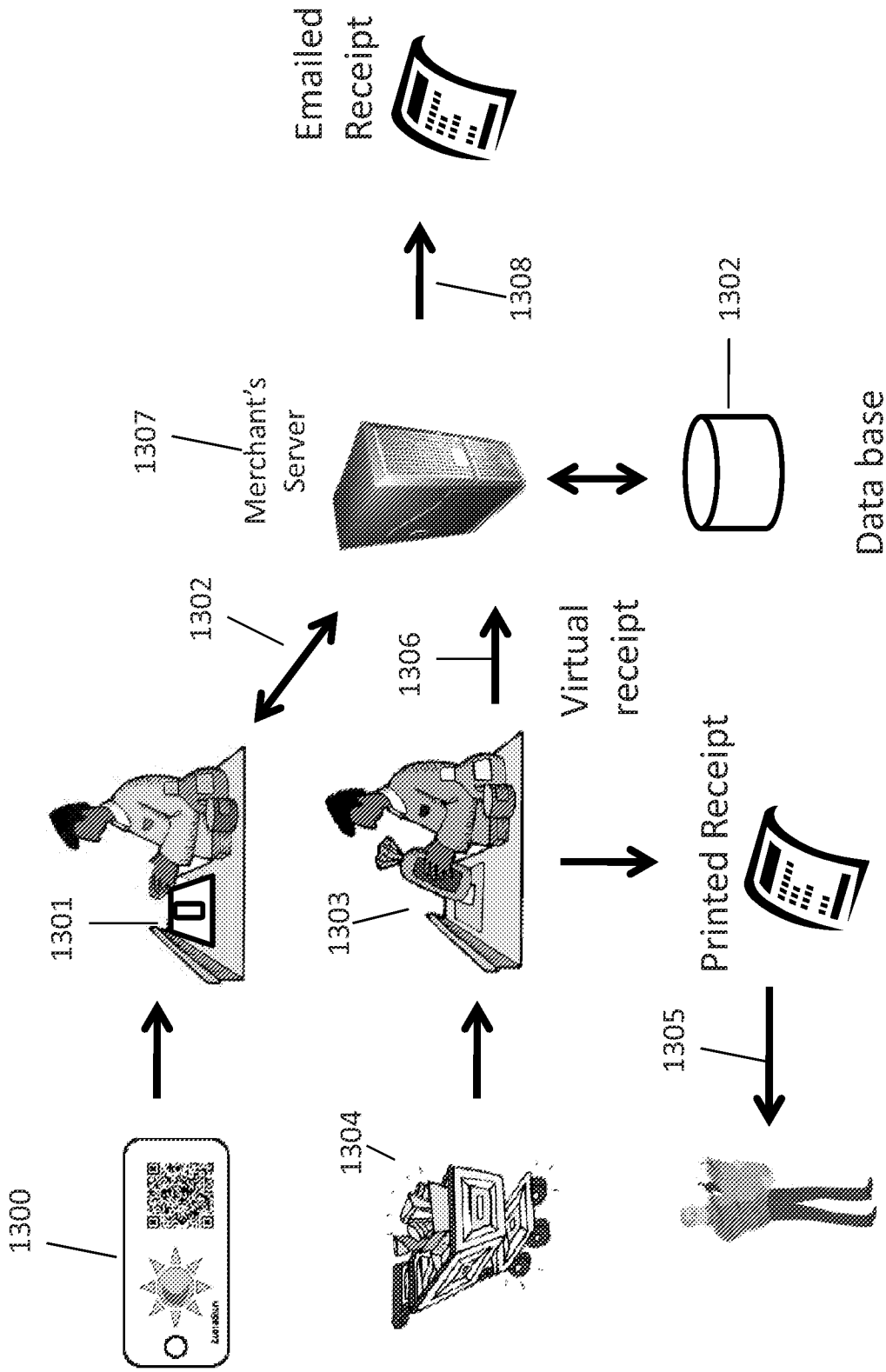


Fig. 12



WO 2012/138432
PCT/US2012/026612

Fig. 13


Emailed Receipt
1308
1302
1307
Merchant's Server
Data base
1302
1306
Virtual receipt
1301
1303
Printed Receipt
1305
1304
1300

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/026612

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/00 (2012.01)
USPC - 705/44
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, 20/02, 20/08, 40/00 (2012.01)
USPC - 705/35, 41, 44, 75

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)
MicroPatent, Questel Orbit, Google Patent, ProQuest

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,715,679 B1 (INFOSINO) 06 April 2004 (06.04.2004) entire document	1-20
Y	US 2002/0016764 A1 (HOFFMAN) 07 February 2002 (07.02.2002) entire document	1-20
Y	US 2009/0106118 A1 (PELEGERO et al) 23 April 2009 (23.04.2009) entire document	1-20
Y	US 2006/0161789 A1 (DOUGHTY et al) 20 July 2006 (20.07.2006) entire document	2
Y	US 2010/0042538 A1 (DHEER et al) 18 February 2010 (18.02.2010) entire document	9-19
Y	US 2004/0019564 A1 (GOLDTHWAITE et al) 29 January 2004 (29.01.2004) entire document	15-16
A	US 2010/0241572 A1 (YUAN) 23 September 2010 (23.09.2010) 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 May 2012	23 MAY 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774