

(12) STANDARD PATENT
(19) AUSTRALIAN PATENT OFFICE

(11) Application No. **AU 2013277468 B2**

(54) Title
Prepaid wallet for merchants

(51) International Patent Classification(s)
G06Q 20/36 (2012.01) **G06Q 20/40** (2012.01)

(21) Application No: **2013277468** (22) Date of Filing: **2013.06.14**

(87) WIPO No: **WO13/192041**

(30) Priority Data

(31) Number	(32) Date	(33) Country
13/525,575	2012.06.18	US

(43) Publication Date: **2013.12.27**

(44) Accepted Journal Date: **2016.05.19**

(71) Applicant(s)
PayPal, Inc.

(72) Inventor(s)
Chaitanya, Somisetty Krishna

(74) Agent / Attorney
Freehills Patent Attorneys, ANZ Tower 161 Castlereagh Street, Sydney, NSW, 2000

(56) Related Art
US 2007/0244757 A1
US 2003/0105710 A1
US 2003/0061170



(43) International Publication Date
27 December 2013 (27.12.2013)

- (51) International Patent Classification:
G06Q 20/36 (2012.01) G06Q 20/40 (2012.01)
- (21) International Application Number:
PCT/US2013/045932
- (22) International Filing Date:
14 June 2013 (14.06.2013)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
13/525,575 18 June 2012 (18.06.2012) US
- (71) Applicant: EBAY INC. [US/US]; 2145 Hamilton Avenue,
San Jose, California 95125 (US).
- (72) Inventor: CHAITANYA, Somisetty Krishna; Ebay Inc.,
2145 Hamilton Avenue, San Jose, California 95125 (US).
- (74) Agent: KINDER, JR., Darrell D.; Haynes and Boone,
LLP, IP Section, 2323 Victory Avenue, Suite 700, Dallas,
Texas 75219 (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, 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,
KM, 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))

(88) Date of publication of the international search report:
27 February 2014

(54) Title: PREPAID WALLET FOR MERCHANTS

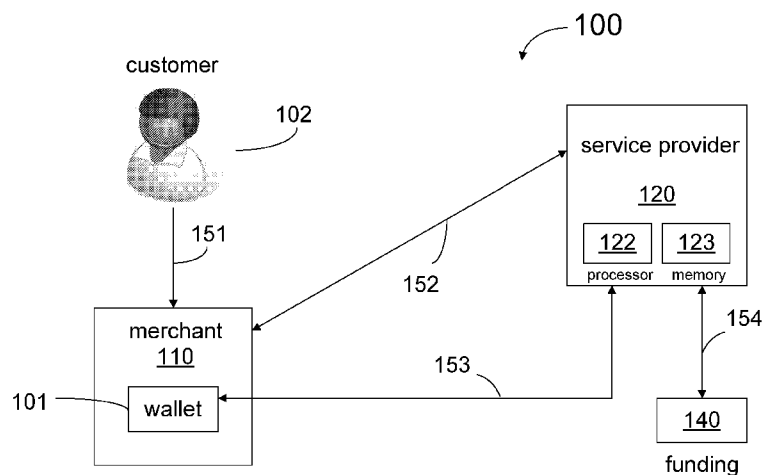


FIG. 1

(57) Abstract: A system including a memory storing user account information with a payment provider associated with specific merchants, and a method for use of the system are provided. The system includes one or more processors in communication with the memory and adapted to: receive login information from a user from a merchant website; access an account of the user with the payment provider; cause information for the account of the user to be displayed on the merchant website; and process a payment to the merchant from the account of the user.

WO 2013/192041 A3

PREPAID WALLET FOR MERCHANTS

Somisetty Krishna Chaitanya

Related Applications

5 [0001] This application claims priority to U.S. Nonprovisional Application No. 13/525,575, filed June 18, 2012, the entire contents of which is hereby incorporated by reference in its entirety.

Background

1.- Field of the Invention

10 [0002] Embodiments described herein relate to the field of online commerce. More particularly, embodiments described herein are related to the field of remote vending transactions using alternative payment methods.

2.- Description of Related Art

15 [0003] With the rapid evolution of online commerce, buyers have greater accessibility to products from a larger pool of merchants. Buyers have gained access to products for sale during a wide range of time periods and locations, which adds a pressure to make payment methods available to buyers at the time of purchase selection. In many instances, buyers may not be able to instantly provide payment for a selected product, while still interested in the purchase. In those situations, state-of-the-art systems typically release the selected product from the buyer and the sale opportunity is essentially lost.

20

[0004] What is needed is an alternative method of payment for online commerce that is flexible and increases a sales opportunity for the buyer and the merchant.

Summary

25 [0005] In one aspect the present invention provides a system comprising: a non-transitory memory; and one or more hardware processors coupled to the non-transitory memory to cause the system to perform operations comprising receiving login information for a user of a payment provider from a merchant website via a first communication link; retrieving, from the non-transitory memory and in response to receiving the login information, a balance for a wallet account associated with the user and associated with a merchant identifier corresponding to the merchant website;

30

transmitting, using the first communication link, the balance for the wallet account to the merchant website, the transmitting causing the merchant website to display the balance for the wallet account; receiving, via the first communication link, a payment request from a merchant associated with the merchant website; transmitting, to a mobile device of the user, a confirmation request via a second communication link and without using the merchant website, the second communication link being different from the first communication link; receiving, via the second communication link and in response to transmitting the confirmation request, a confirmation from the mobile device of the user; and processing a payment to an account of the merchant from the wallet account, in response to receiving the confirmation from the mobile device of the user.

[0006] In a second aspect the present invention provides a non-transitory machine-readable medium having stored thereon machine-readable instructions executable to cause a machine to perform operations ; receiving login information for a user from a merchant website via a first communication link; retrieving, from the non-transitory memory and in response to receiving the login information, a balance for a wallet account associated with the user and associated with a merchant identifier corresponding to the merchant website; transmitting via the first communication link, the balance for the wallet account to the merchant website; receiving, via the first communication link, a payment request from a merchant associated with the merchant website; transmitting, to a mobile device of the user, a confirmation request via a second communication link in response to receiving the payment request and without using the merchant website, the second communication link being different from the first communication link; receiving, via the second communication link and in response to transmitting the confirmation request, a confirmation from the mobile device of the user; and processing a payment to an account of the merchant from the wallet account in response to receiving the confirmation from the mobile device of the user.

[0007] In a further the present invention provides a method comprising: receiving, at a server having one or more hardware processors and a non-transitory memory, login information for a user from a merchant website via a first communication link; retrieving, by the server in response to receiving the login

information, a balance of a wallet account from the non-transitory memory, the wallet account being associated with the user and associated with a merchant identifier corresponding to the merchant website; transmitting, via the first communication link, the balance of the wallet account to the merchant website; receiving, via the first
5 communication link, a payment request from a merchant associated with the merchant website; transmitting, via a second communication link different from the first communication link, a confirmation request to a mobile device of the user in response to receiving the payment request; receiving, via the second communication link and in response to transmitting the confirmation request, a confirmation from the mobile
10 device of the user; and processing a payment to an account of the merchant from the wallet account in response to receiving the confirmation from the mobile device of the user.

[0008] These and other embodiments of the present invention will be described in further detail below with reference to the following drawings.

15 [0008A] As used herein, except where the context requires otherwise, the term "comprise" and variations of the term, such as "comprising", "comprises" and "comprised", are not intended to exclude further features, components, integers or steps.

Brief Description of the Drawings

20 [0009] FIG. 1 shows a system for remote purchasing using a wallet, according to some embodiments.

[0010] FIG. 2 shows a merchant website including a wallet, according to some embodiments.

25 [0011] FIG. 3 shows a flow chart of a method for signing up a new customer of a wallet, according to some embodiments.

[0012] FIG. 4 shows a flow chart of a method for remote purchasing using a wallet, according to some embodiments.

[0013] FIG. 5 shows a system for remote purchasing using a wallet, according to some embodiments.

[0014] FIG. 6 shows a flow chart of a method for user discovery, according to some embodiments.

[0015] FIG. 7 shows a flow chart of a method for remote purchasing using a wallet, according to some embodiments.

5 [0016] FIG. 8 shows a system for remote purchasing using a wallet, according to some embodiments.

[0017] In the figures, elements having the same reference number have the same or similar functions.

Detailed Description

10 [0018] With the increase of network accessibility for multiple consumer electronic devices such as cellular phones and tablet computers, potential buyers have largely enhanced their purchasing capabilities. Availability of private account service providers holding cash resources remotely located from individual customers further increases purchasing opportunities for potential buyers. The present disclosure
15 includes methods and systems providing a pre-paid merchant wallet available for use by consumers for online transactions. Thus, according to embodiments disclosed herein the opportunity to complete a purchase online is increased, together with sales volume, customer and merchant satisfaction.

[0019] According to embodiments disclosed herein a private account service
20 provider creates an account for the customer of a merchant's website using funding instrument information available from the merchant, related to the customer. Funding instrument information may be a bank account number, or a credit card number, associated to the customer. The account created for the customer is a wallet that the customer may use to purchase merchant's items or services listed in the merchant's
25 website. Once the wallet is created, the customer may see wallet's details on the merchant's website each time the customer logs into the merchant website. For example, the user may see the wallet balance, available funds, and history of payments and purchases with the merchant. This may be advantageous for promoting customers to become registered users with the private account service provider. Also,
30 people in distant and remote markets may become familiarized with the services of a private account service provider, prompting people to become registered users.

[0020] According to some embodiments, a plurality of merchants may each include a group of customers registered in their websites. A private account service

provider may thus provide wallet services to customers from each of the plurality of merchants. Thus, a large group of potential users may familiarize with the quality of service and security offered by the private account service provider. In some embodiments the private account service provider may contact the customers that use
5 wallets, offering user registration with full services beyond a wallet for a specific merchant.

[0021] FIG. 1 shows a system 100 for remote purchasing using a wallet 101, according to some embodiments. System 100 includes a customer 102 accessing a merchant's website 110. The merchant's website 110 includes a wallet 101 managed
10 by a private account service provider 120, such as PayPal, Inc. of San Jose, CA. The wallet includes a balance of funds provided by a funding instrument 140 through the private account service provider 120. Service provider 120 may include a server connected to a network, the server including a computer having a processor circuit 122 and a memory circuit 123.

[0022] According to some embodiments, private account service provider 120
15 creates an account or "wallet" 101 for customer 102 of merchant website 110. Wallet 101 includes information related to customer 102 available from merchant's website 110. Once wallet 101 is created, customer 102 is able to see details of the account or wallet 101 each time customer 102 logs into merchant's web site 110. In some
20 embodiments, customer 102 may be able to see the wallet's balance and available funds. System 100 provides a service for merchants to handle purchasing transactions remotely. System 100 may introduce a vast market of potential users to the benefits of private account service provider 120. Thus, potential users may be interested in registering with service provider 120 for a wide range of financial transactions,
25 beyond what is offered in merchant's website 110.

[0023] In some embodiments, private account service provider 120 includes a merchant account. Service provider 120 may also place money into wallet 101 from a funding instrument 140. As the customer uses the balance in the wallet to purchase
30 selected items or services from the merchant, service provider 120 transfers funds form the wallet 101 to the merchant's account with service provider 120. Funding instrument 140 may be a customer bank account or a customer credit card. Information about the customer may be provided to private account service provider 120 by the merchant hosting merchant's website 110. This information may include customer's financial information and transaction records with the merchant.

[0024] In some embodiments, customer 102 accesses merchant's website 110 through a remote link 151. Merchant's website 110 and service provider 120 may communicate through a remote link 152. Service provider 120 may operate wallet 101 in merchant's website 110 through remote link 153. Furthermore, service provider 120 may retrieve customer funds from funding instrument 140 through remote link 154. Remote links 151, 152, 153, and 154 may be part of a network, or each may be included in a separate network. According to some embodiments, the network including either of remote links 151, 152, 153, and 154 may be a wireless network, or a cell phone network.

10 [0025] FIG. 2 shows merchant website 110 including wallet 101 and a balance field 201, according to some embodiments. Merchant's website 110 may display an icon for wallet 101 when the customer logs in merchant's web site 110. The icon for wallet 101 may be operated by private account service provider 120, including balance field 201. Balance field 201 displays the current balance in the wallet, so that customer 102 may decide to make a purchase, or add more funds into wallet 101. In some embodiments, wallet 101 may further include a customer help link 202, to receive input from customer 102 regarding potential conflicts with the vendor.

[0026] When customer 102 having a wallet 101 taps on the customer help link 202, the customer may be able to fill in a field with comments, complaints, and other information related to a potential conflict with the vendor. The data provided by customer 102 through customer help link 202 may be stored by service provider 120 in memory circuit 123. Service provider 120 may place a conflict resolution option in merchant's website 110 to log potential disputes for reference by the merchant, the customer, and the service provider. The customer may thus be able to input conflict information upon tapping on the link. The customer conflict information may be stored in memory circuit 123 by service provider 120.

20 [0027] The customer conflict information may be kept confidential by service provider 120. In some embodiments, the customer conflict information may be provided to the merchant, by service provider 120. Further according to some embodiments, the customer conflict information may be made available to a third party by service provider 120. For example, in some embodiments the customer conflict information may be provided to other customers having similar or related conflicts. In some embodiments the customer conflict information may be provided to a local authority for further processing. According to some embodiments, service

provider 120 may use customer conflict information from a plurality of customers to perform a statistical analysis of the quality of management by the merchant. Service provider 120 may further use the statistical information to either cancel the wallet option with a merchant, or provide the merchant with feedback for improvement of the service.

5 [0028] Private account service provider 120 may offer customer 102 to deposit funds into the wallet from a bank account or using a credit card. Wallet 101 allows customer 102 to pay for a purchase of a selected item or group of items from merchant's website 110. When customer 102 decides to use wallet 101 for a
10 purchase, private account service provider 120 credits a merchant account with service provider 120 in the amount of the purchase transaction, and deducts the amount from customer's wallet 101.

[0029] FIG. 3 shows a flow chart of a method 300 for signing up a new customer to a wallet, according to some embodiments. In some embodiments method 300 may
15 be performed by a merchant hosting merchant's website 110 (cf. FIG. 1). Further according to some embodiments, method 300 may be performed by service provider 120 having links 152 and 153 with merchant's website 110 and having link 154 with funding instrument 140 (cf. FIG. 1). In such embodiments, steps in method 300 may be performed by processor circuit 122 in service provider 120, using information and
20 commands stored in memory circuit 123.

[0030] In step 310, service provider 120 establishes an agreement with the merchant. In the agreement, the merchant may allow service provider 120 to place a wallet such as wallet 101 in merchant's website 110 associated to a customer account with the merchant. Furthermore, the merchant may agree for service provider 120 to
25 place a logo or icon advertising the name and brand of service provider 120 servicing wallet 101. In some embodiments, the merchant may also register as a user in private account service provider 120, in step 310.

[0031] In step 320, a request from customer 102 to enable wallet 101 is received in merchant's website 110. For example, in some embodiments customer 102 may
30 select a link or tap on an icon in merchant's website 110, requesting the merchant to enable wallet 101. In step 330, service provider 120 receives data related to customer 102 exported by the merchant. In some embodiments, the data received by service provider 120 in step 330 may be stored in memory circuit 123. The data may include customer information, such as name, email address, phone number, billing address,

shipping address, and any other relevant information needed by the service provider to create an account. The customer data exported in step 330 by the merchant may include customer financial information such as a bank account number or a credit card number, and a payment history between merchant and customer 102. The bank
5 account number or the credit card number may be used by private account service provider 120 to access funding instrument 140 and transfer funds into wallet 101, upon customer's request and authorization. The payment history enables private account service provider 120 to assess the risk posed by customer 102.

[0032] In step 340, service provider 120 creates a customer account as a wallet
10 and provides the merchant confirmation. The wallet account created by service provider 120 may be linked to the merchant. For example, service provider 120 may include a merchant identifier in the customer account, to recognize a wallet 101 associated with the merchant. Thus, when the customer performs a purchase through wallet 101, service provider 120 may transfer the funds from wallet 101 to a
15 merchant's account with service provider 120. According to some embodiments, wallet 101 is managed by the merchant, through merchant's webpage 110. The account linked to the merchant includes wallet 101 is displayed to the customer on the merchant website, in step 350, when the customer logs into the merchant's website 110. In step 350, service provider 120 may give the merchant information to display
20 balance 201 in wallet 101 for customer 102. The balance may be current balance or available balance for purchasing with the merchant. Once wallet 101 is created, service provider 120 is able to retrieve funds from funding instrument 140 and provide a balance to wallet 101, upon customer's request and confirmation, as detailed below in FIG. 4. According to some embodiments, wallet 101 created in
25 method 300 may be linked to the merchant hosting merchant's website 110. That is, the merchant may still have full authority on the wallet's balance, and access to all information from the customer contained in wallet 101. Thus, in some embodiments service provider 120 is limited to providing funds to wallet 101 from funding instrument 140, and allocating funds from wallet 101 into a merchant's account with
30 service provider 120.

[0033] In some embodiments, some of the steps described in detail above in relation to method 300 may be performed by the merchant using an application program interface (API) provided by service provider 120. Service provider 120 presents the newly created account as a wallet 101 that shows in the customer's login

account in merchant's website 110. The newly created wallet 101 may have limited services with service provider 120, as it is accessed through the merchant's website. According to some embodiments, wallet 101 created as in method 300 may be under care of merchant's website 110. Thus, the merchant may deduct a balance in wallet

5 101 on behalf of the customer, for purchases. In some embodiments, wallet 101 may be under direct management of service provider 120 since custom wallets may be risky and costly to maintain for a single merchant. Thus, service provider 120 may offer its expertise and reliability to operate and maintain wallet 101 for merchant's website 110.

10 **[0034]** According to some embodiments of method 300, a merchant may save the fee paid a bank or credit card on multiple transactions. Thus, once a money amount is placed in wallet 101, several purchases in merchant's website 110 may be performed without paying a transaction fee to a bank or a credit card, from the merchant. Customer 102 also saves fee's levied by a bank (e.g., IRCTC) or credit

15 card, upon multiple transactions.

[0035] Embodiments of method 300 provide a mass signup of potential users into service provider 120 since all of merchant's customers are potential users of service provider 120. The merchant will also be a user of service provider 120, according to some embodiments. Thus, in some embodiments service provider 120

20 may offer discounted services to the merchant in order to be able to manage wallets 101 for the merchant's customers. In this manner, service provider 120 may advertise its services in new markets by leveraging the merchant's popularity. Thus, marketing costs for service provider 120 to enter new geographic areas are reduced. Embodiments consistent with method 300 are desirable for service provider 120, since

25 fraud risk with new customer signups is directly assessed through the customer's payment history with merchant.

[0036] In some embodiments, method 300 for signing up a new user of a wallet may include service provider 120 returning the funds in wallet 101 to funding instrument 140. For example, service provider 120 may return funds in wallet 101 to

30 customer 102 through funding instrument 140 when the merchant hosting merchant's website 110 decides to cut ties with service provider 120.

[0037] FIG. 4 shows a flow chart of a method 400 for remote purchasing using a wallet on a merchant site, according to some embodiments. Method 400 may be performed by the merchant hosting merchant's website 110. Further according to

some embodiments, method 400 may be performed by service provider 120 having links 152 and 153 with merchant's website 110 and having link 154 with funding instrument 140 (cf. FIG. 1). In such embodiments, steps in method 400 may be performed by processor circuit 122 in service provider 120, using information and commands stored in memory circuit 123.

[0038] In step 410, a login request is received from customer 102. Customer 102 may have a wallet account 101 with service provider 120. According to some embodiments, a login request may include the use of a customer identification information, such as a user name, e-mail address, or phone number, and a password or personal identification number (PIN) for a customer account in merchant's website 110. In some embodiments wallet 101 may be a pre-paid wallet, so that there is a positive balance in the wallet, and the customer may purchase an item when there is enough balance in wallet 101 to do so. In some embodiments, depending on the customer payment history with the merchant, the merchant may allow the customer to make a purchase for an item as long as a pre-established purchase limit is not exceeded. Thus, in some embodiments the customer may use wallet 101 to purchase an item that exceeds the balance available in the wallet. In such embodiments, the merchant may request customer 102 to further authorize service provider 120 to retrieve funds from funding instrument 140 to complete the balance of wallet 101 in the transaction. In step 420, service provider 120 provides the wallet balance to display in merchant's website 110, for customer 102.

[0039] In step 430 an item selected by customer 102 is added into a shopping cart. The shopping cart may also be displayed in merchant's website 110. In step 440 a balance is deducted from wallet 101 according to the sum of the cost of the items in the shopping cart, after customer 102 decides to make a purchase. In step 440, a link to service provider 120 using a transaction identifier (ID) may be created, so that service provider 120 may store the purchase information in memory circuit 123, for reference. The link may include information about the purchase to be stored by service provider 120. Thus, service provider 120 may transfer funds from wallet account 101 to a merchant's account, in the amount of the transaction. In step 450, service provider 120 provides the merchant with a purchase confirmation once the funds have been transferred from wallet 101 to the merchant's account. In step 460 a message is sent to customer 102 confirming balance deduction and including a receipt for the purchase. According to some embodiments, the message in step 460 is sent by

the merchant. In some embodiments, the message in step 460 is sent by service provider through the merchant, using links 152 and 151 (cf. FIG. 1).

[0040] According to some embodiments, a merchant may find method 400 for remote purchasing convenient. Indeed, the number of failed transactions due to bad network or busy merchant website 110 is reduced. In fact, service provider 120 may enable security options and safe wards to restore the transaction in case of a network failure. Furthermore, service provider 120 may offer a safe network of servers that guarantees data security and transaction reliability. Customer 102 may also find method 400 for remote purchasing convenient, since it offers a faster checkout process, essentially instantaneous. Also, according to embodiments consistent with method 400 the purchase is completed by only a tap by the user. The user does not need to input any further information or code to complete the transaction.

[0041] FIG. 5 shows a system 500 for remote purchasing using wallet 101, according to some embodiments. FIG. 5 illustrates a registered user 502 which may have an account 121 with private account service provider 120. Registered user 502 may also have a wallet account 101 in merchant's website 110, serviced by service provider 120. FIG. 5 illustrates link 151 between registered user 502 and merchant's website 110, link 152 between merchant's website 110 and service provider 120, link 153 between wallet 101 in merchant's website 110 and service provider 120, and link 154 between funding instrument 140 and user account 121. Links 151, 152, 153, and 154 are as described in detail above, in relation to FIG. 1. According to some embodiments, system 500 may include link 550 between registered user 502 and service provider 120. Link 550 may include an internet link, or a wireless link such as provided by a cell phone network.

[0042] FIG. 5 also illustrates funding instrument 140 coupled to service provider 120 through user account 121. User account 121 includes information about wallet 101, such as purchase history between registered user 502, the merchant hosting merchant's website 110, and balance information about wallet 101. User account 121 may also include information about funds available for registered user 502 to purchase items or services other than those offered in merchant's website 110. Thus, funding instrument 140 may be used by registered user 502 to pull funds into user account 121, and the funds may be used for any purchasing transaction of registered user 502, regardless of whether or not the item or service selected for the transaction is offered in merchant's website 110.

[0043] In some embodiments, when service provider 120 creates wallet 101 for customer 102, service provider 120 may offer customer 102 to become a registered user with service provider 120. Customer 102 may thus become a registered user with service provider 120. The registered user account may include further personal information provided by customer 102 to service provider 120. Personal information for the registered user may be stored in a database within service provider 120. The registered user may use the account in service provider 120 for financial transactions and purchases other than the merchant's items and services. In such embodiments the user of service provider 120 may still have an account in merchant's website 110, including wallet 101. Wallet 101 may be linked to the user account 121 with service provider 120, such that funds may be transferred into wallet 101 by service provider 120 per registered user's request. User 502 may access user account 121 through link 550, by providing a personal identification number (PIN) unique for user's account 121 in service provider 120. The PIN used by user 502 to access account 121 in service provider 120 may be the same as the PIN used by user 502 to access wallet 101, according to some embodiments. In some embodiments, user 501 may access wallet 101 in vendor's webpage 110 using a PIN, and once user 502 is logged into wallet 101, service provider 120 may recognize the PIN and provide user 502 with access to account 121.

[0044] Further according to some embodiments, user 502 may already be a registered user of service provider 120 before enabling wallet 101 in merchant's website 110. Thus, in some embodiments service provider 120 may include user account 121 prior to enabling wallet 101. In such embodiments, service provider 120 may link user account 121 to wallet 101, upon request from user 502. In such embodiments, user 502 may be given fully enabled wallet features, as described in detail below in relation to FIG. 6.

[0045] FIG. 6 shows a flow chart of a method 600 for user discovery according to some embodiments. In some embodiments, method 600 is performed by private account service provider 120 once customer 102 has created wallet 101 through merchant's website 110. In step 610 service provider 120 provides information to customer 102, regarding account registration with service provider 120. In some embodiments, service provider 120 performs step 610 once customer 102 has logged in to an account with merchant website 110. For example, customer 102 may log into an account in merchant's website 110 providing a login name, a user name, an e-mail

address, or a phone number. Further, customer 102 may use a password, or a PIN, to access the customer account in merchant's website 110.

5 [0046] In step 620, service provider 120 receives a request from customer 102 to register as a user with service provider 120. In some embodiments, step 620 may include importing user data via an API provided to customer 102 by service provider 120. In step 630 service provider 120 registers customer 102 as a user. In some embodiments step 630 includes the user agreeing to the terms of service (T&S) of service provider 120.

10 [0047] In step 640, service provider 120 removes any account limitations that the newly registered user may have had in wallet 101. According to some embodiments consistent with the present disclosure, when a user is already a registered user of service provider 120, method 600 may start with step 640, including service provider 120 linking a wallet 101 with user account 121. Step 640 may include giving wallet 101 all privileges and access to user account 121.

15 [0048] In step 650, service provider 120 provides a wallet service to the registered user and to the merchant. Step 650 may include supporting merchant's website 110 in performing steps 410 through 460, described in detail above in relation to method 400 (cf. FIG. 4).

20 [0049] FIG. 7 shows a flow chart of a method 700 for remote purchasing using a wallet, according to some embodiments. Method 700 may be performed by service provider 120 when a registered user having wallet 101 selects an item or service from merchant's website 110 for purchase. Thus, according to some embodiments, method 700 includes registered user 502 having an account 121 with service provider 120 and also a wallet 101 in a merchant's website 110 (cf. FIG. 5). According to some 25 embodiments, registered user 502 may be a customer of a merchant, as customer 102. In step 710 service provider 120 provides a wallet balance to the registered user 502 upon registered user 502 login into merchant's website 110. In some embodiments, registered user 502 may log into merchant's website 110 using a login name, an e-mail address, or a phone number including a password or a PIN.

30 [0050] In step 720 service provider 120 requests from registered user 502 a purchase authentication. Step 720 may be performed by a direct communication between service provider 120 and registered user 502. In some embodiments, while registered user 502 may request the purchase using link 151 to merchant's website 110, service provider 120 may request confirmation from registered user 502 through

communication link 550. For example, while registered user 502 may connect to merchant's website 110 through network link 151, service provider 120 may call registered user 502 through a cell phone or e-mail link 550 in step 720.

[0051] In step 730, service provider 120 provides the merchant with a purchase confirmation by registered user 502, including the new balance in wallet 101 for registered user 502. In step 740 service provider 120 sends a message to registered user 502 confirming the balance reduction in wallet 101, including a purchase receipt. In some embodiments the message may be a short-message-service (SMS) message to the registered user, or a phone message through a cell phone network, or an e-mail message through a network.

[0052] FIG. 8 shows a system 800 for remote purchasing using a prepaid wallet 101, according to some embodiments. FIG. 8 illustrates service provider 120 and a plurality of websites 110-1 through 110-6 (collectively referred to as websites 110). Each one of websites 110 may be hosted by a different merchant offering different types of items and services. Also, each website 110 in FIG. 8 may have a group of customers 102, each customer having a wallet 101 such as described above in relation to FIGS. 1 and 5. Furthermore, as illustrated in FIG. 8, some customers may also be registered users of service provider 120, such as registered users 502-1, 502-2, 502-3, and 502-5.

[0053] FIG. 8 illustrates links 852-1, 852-1, 852-3, 852-3, 852-5, and 852-6, collectively referred to as links 852. Links 852 couple websites 110 to source provider 120, as link 152, described in detail above (cf. FIG. 1). FIG. 8 also illustrates links 851 between customers 102 and wallets 101. Links 851 may be as link 151 described in detail above (cf. FIG. 1). Links 550-1, 550-2, 550-3 and 550-5 may be as link 550, described in detail above (cf. FIG. 5).

[0054] Some embodiments of system 800 may include registered users 802-1 and 802-2, collectively referred to as registered users 802. Registered users 802 may have an account with service provider 120 through which registered users 802 may operate more than one wallet 101 for more than one merchant. For example, registered user 802-1 may have a wallet 101-5 with merchant's website 110-5, and a wallet 101-6 with merchant's website 110-6. Each of wallets 110-5 and 110-6 may be handled separately by service provider 120. In some embodiments, service provider 120 may transfer funds from wallet 101-5 to wallet 101-6 and vice-versa, upon request by registered user 802-1. Furthermore, according to some embodiments,

service provider 120 may transfer funds from a different account of registered user 802-1 into either of wallets 101-5 and 101-6. Service provider 120 may provide similar flexibility in management of wallets 101-4 and 101-3 for registered user 802-2. Thus, in some embodiments a registered user 802 may handle multiple wallets 101 with multiple merchants, through service provider 120, independently of one another. For example, a merchant hosting merchant's website 110-4 may have access to customer data related to wallet 101-4, such as account balance and payment history. However, the merchant hosting merchant's website 110-4 may not have access to customer data related to wallet 101-3 in merchant's website 110-3, even though wallets 101-3 and 101-4 are associated to registered user 802-2.

[0055] As FIG. 8 shows, some embodiments of system 800 enable service provider 120 to access a large network of customers 102 that may become registered users 802. In order to incentivize adoption of the use of wallet 101 through service provider 120, service provider 120 may offer customers 102 credit points for certain amount of money spent in merchant's website 110 through wallet 101.

[0056] In geographic areas where service provider 120 desires to open new markets, some embodiments consistent with the present disclosure may enable wallet 101 for a limited amount of time, according to local banking regulations. In such configuration, either the merchant or service provider 120 may return the funds left in wallet 101 upon expiration time to funding instrument 140. Further, according to local banking regulations, service provider 120 may not allow customers 102 to retrieve money out of wallet 101, and only use wallet 101 for purchasing goods and services.

[0057] In some embodiments, service provider 120 may provide an 'opt-me-out' option to customers 102. Thus, for a customer 102 that desires to stay out of the network of service provider 120, customer 102 may still have wallet 101 with merchant's website 110. In such embodiments service provider 120 may put the balance of 'opt-me-out' customer in a proxy account associated to the merchant, who may have an account with service provider 120. The merchant may handle each of 'opt-me-out' customer's balance in the proxy account.

[0058] In some embodiments of system 800 customer 102 may not be a registered user with service provider 120. Furthermore, in some embodiments a customer 102 may have a wallet 101 with each of two merchants. This is illustrated in FIG. 8 by customer 802-5 having wallet 101-5 in merchant's website 110, and

wallet 101-6 in merchant's website 110-6. In some embodiments, if customer 802-5 is not a registered user of service provider 120, customer 802-5 may not use the balance in wallet 101-5 to pay for an item in merchant's website 110-6. In some embodiments, if customer 802-5 is a registered user of service provider 120, and if
5 wallets 101-5 and 101-6 are offered by service provider 120, customer 802-5 may use the balance in wallet 101-5 to purchase an item in merchant's website 110-6.

[0059] Embodiments of the invention described above are exemplary only. One skilled in the art may recognize various alternative embodiments from those specifically disclosed. Those alternative embodiments are also intended to be within
10 the scope of this disclosure. As such, the invention is limited only by the following claims.

Claims

What is claimed is:

1. A system comprising:
- a non-transitory memory; and
- 5 one or more hardware processors coupled to the non-transitory memory and configured to read instructions from the non-transitory memory to cause the system to perform operations comprising:
- receiving login information for a user of a payment provider from a merchant website via a first communication link;
- 10 retrieving, from the non-transitory memory and in response to receiving the login information, a balance for a wallet account associated with the user and associated with a merchant identifier corresponding to the merchant website;
- transmitting, using the first communication link, the balance for
- 15 the wallet account to the merchant website, the transmitting causing the merchant website to display the balance for the wallet account;
- receiving, via the first communication link, a payment request from a merchant associated with the merchant website;
- transmitting, to a mobile device of the user, a confirmation
- 20 request via a second communication link and without using the merchant website, the second communication link being different from the first communication link;
- receiving, via the second communication link and in response to transmitting the confirmation request, a confirmation from the
- 25 mobile device of the user; and
- processing a payment to an account of the merchant from the wallet account, in response to receiving the confirmation from the mobile device of the user.
- 30 2. The system of Claim 1 wherein the operations further comprise accessing a funding instrument having user funds, and transferring funds into the wallet account.

3. The system of Claim 1 wherein the wallet account includes a balance for purchasing items.

4. The system of Claim 1 wherein the operations further comprise:

- 5 receiving a personal identification number (PIN) associated with the wallet account; and
- processing user payments through a network.

5. A non-transitory machine-readable medium having stored thereon machine-readable instructions executable to cause a machine to perform operations comprising:

- 10 receiving login information for a user from a merchant website via a first communication link;
- retrieving, from the non-transitory memory and in response to receiving the login information, a balance for a wallet account associated with the user and associated with a merchant identifier corresponding to the merchant website;
- 15 transmitting, via the first communication link, the balance for the wallet account to the merchant website;
- 20 receiving, via the first communication link, a payment request from a merchant associated with the merchant website;
- transmitting, to a mobile device of the user, a confirmation request via a second communication link in response to receiving the payment request and without using the merchant website, the second communication link being
- 25 different from the first communication link;
- receiving, via the second communication link and in response to transmitting the confirmation request, a confirmation from the mobile device of the user; and
- 30 processing a payment to an account of the merchant from the wallet account in response to receiving the confirmation from the mobile device of the user.

6. The non-transitory machine-readable medium of Claim 5 wherein the wallet account includes a balance for purchasing items displayed in the merchant website.

7. The non-transitory machine-readable medium of Claim 5 further wherein the operations further comprise transferring funds from a user funding instrument to the wallet account.
- 5
8. The non-transitory machine-readable medium of Claim 5 further wherein the operations further comprise:
- providing information to the user regarding a service provided by the payment provider;
 - 10 receiving a request from the user to register as a user of the service;
 - and
 - removing account limitations for the user in the wallet account.
9. The non-transitory machine-readable medium of Claim 5 wherein the user is a
- 15 registered user of the payment provider.
10. A method comprising:
- receiving, at a server having one or more hardware processors and a non-transitory memory, login information for a user from a merchant website
 - 20 via a first communication link;
 - retrieving, by the server in response to receiving the login information, a balance of a wallet account from the non-transitory memory, the wallet account being associated with the user and associated with a merchant identifier corresponding to the merchant website;
 - 25 transmitting, via the first communication link, the balance of the wallet account to the merchant website;
 - receiving, via the first communication link, a payment request from a merchant associated with the merchant website;
 - transmitting, via a second communication link different from the first
 - 30 communication link, a confirmation request to a mobile device of the user in response to receiving the payment request;
 - receiving, via the second communication link and in response to transmitting the confirmation request, a confirmation from the mobile device of the user; and

processing a payment to an account of the merchant from the wallet account in response to receiving the confirmation from the mobile device of the user.

5

11. The method of Claim 10 further comprising:

transmitting, via the first communication link, a purchase confirmation to the merchant, the purchase confirmation including a new balance for the wallet account; and

10

transmitting, via the second communication link, a message to the mobile device of the user confirming the new balance for the wallet account.

12. The method of Claim 11 further comprising transferring, funds from a user funding instrument to the wallet account.

15

13. The method of Claim 10 wherein the user is a registered user of a payment provider operating the server.

20

14. The method of Claim 10 wherein transmitting the confirmation request to the mobile device of the user comprises one or more selected from a group consisting of transmitting a short message system message, transmitting an email, and making a phone call.

25

15. The method of Claim 10 wherein receiving the confirmation from the mobile device of the user comprises receiving, a PIN, the PIN being associated with the wallet account.

30

16. The method of Claim 10 wherein receiving the confirmation from the mobile device of the user comprises one or more selected from a group consisting of receiving a short message system message, receiving an email, and receiving the confirmation over a phone line.

17. The method of Claim 16 further comprising providing a customer help line accessible through a link on the merchant website.

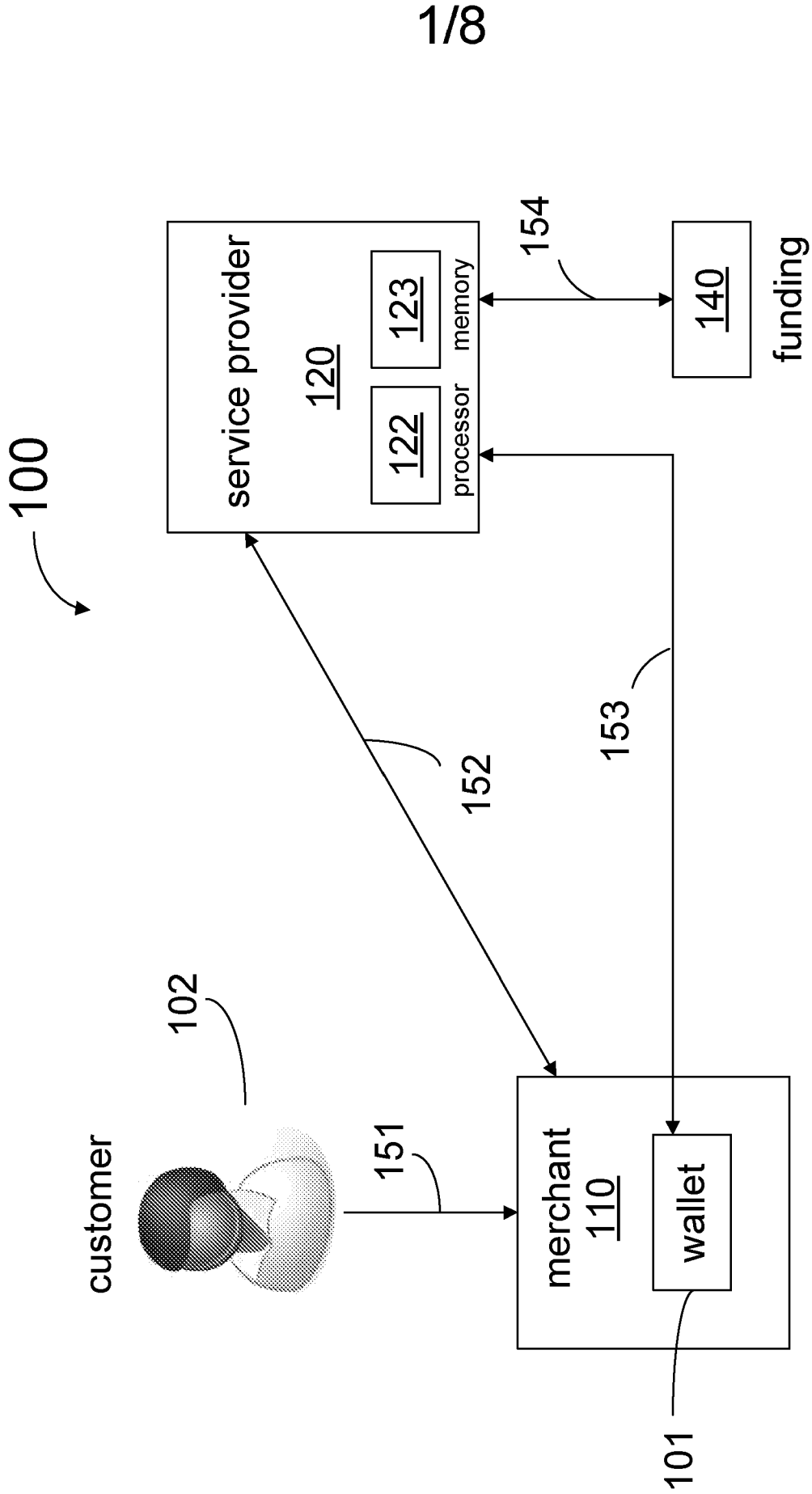


FIG. 1

2/8

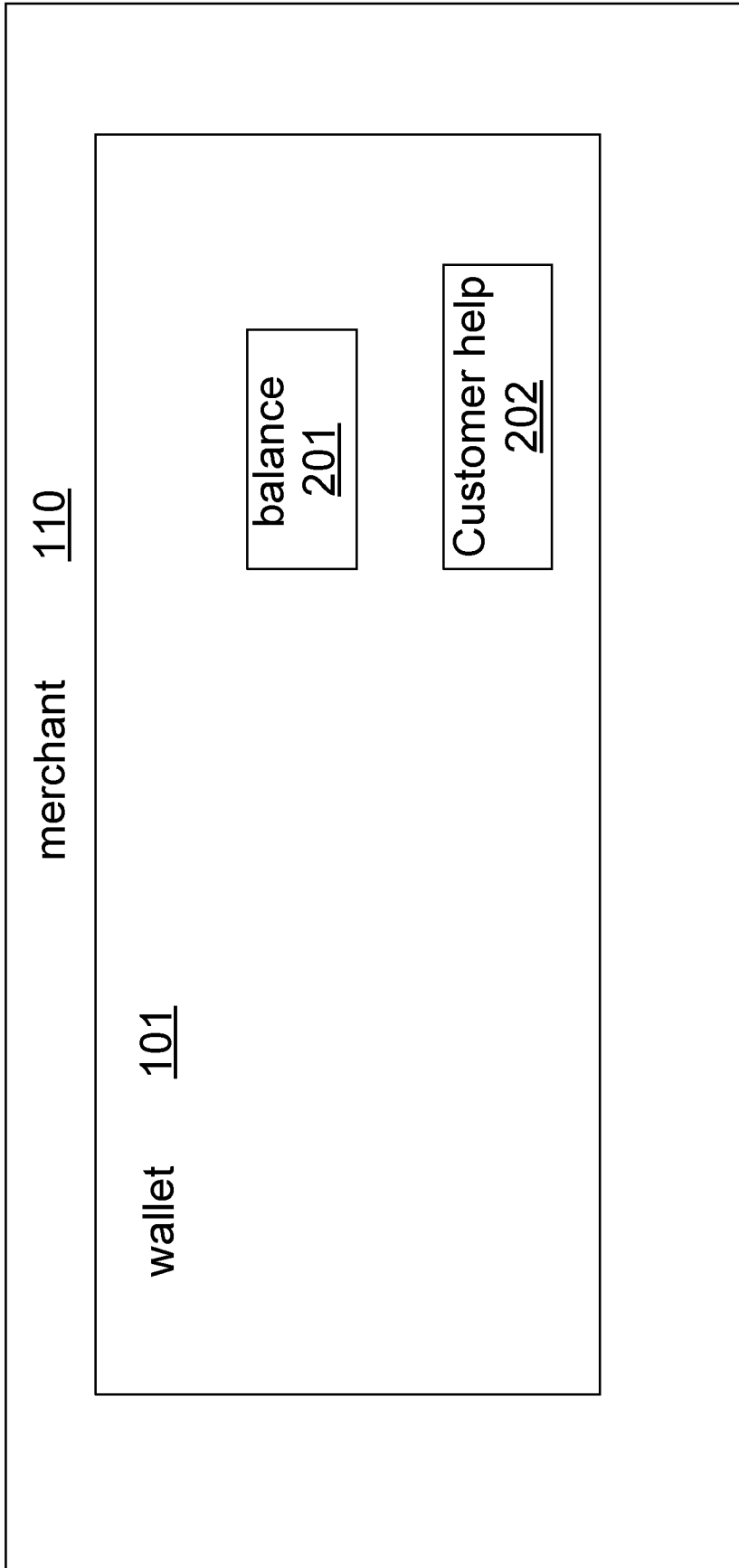


FIG. 2

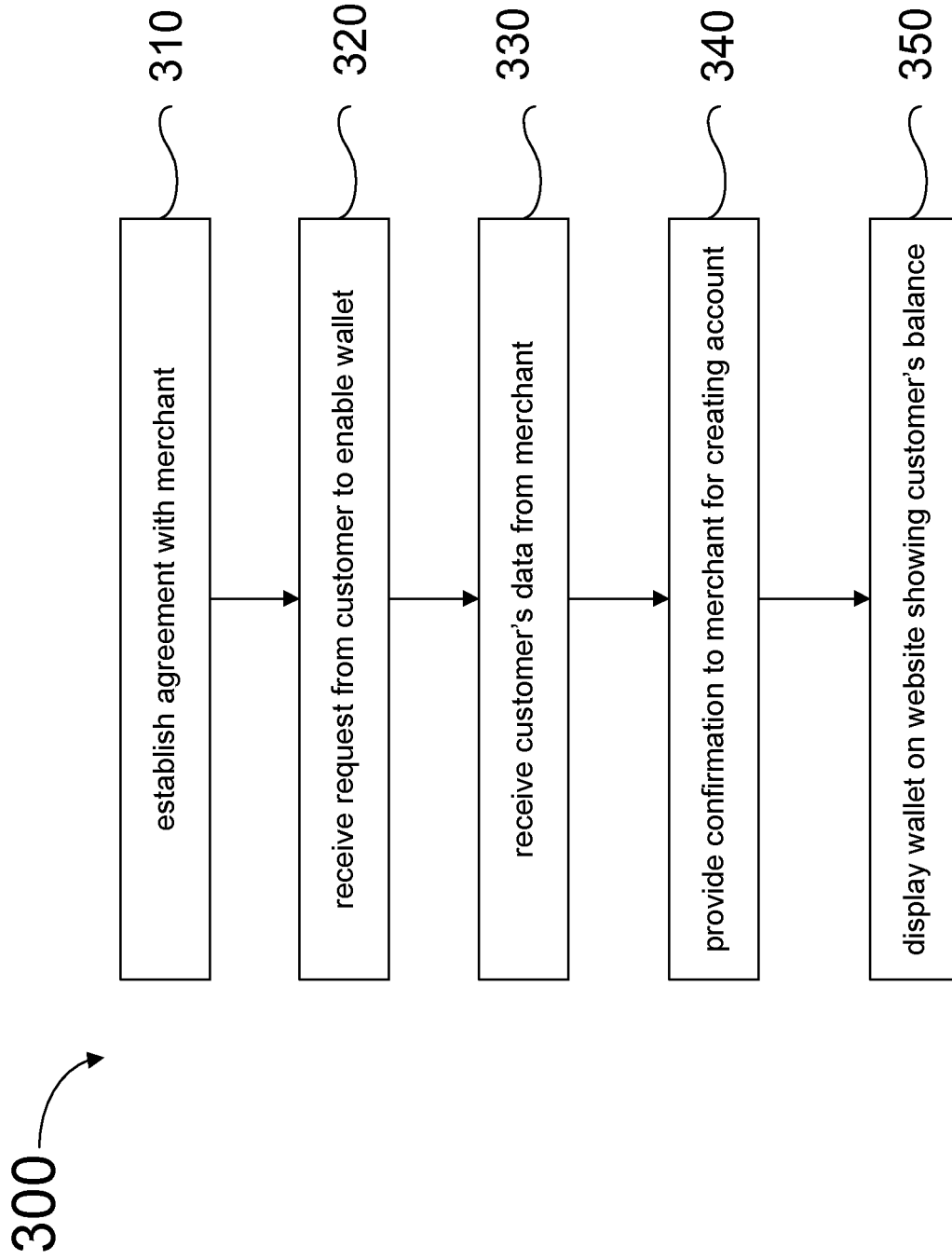


FIG. 3

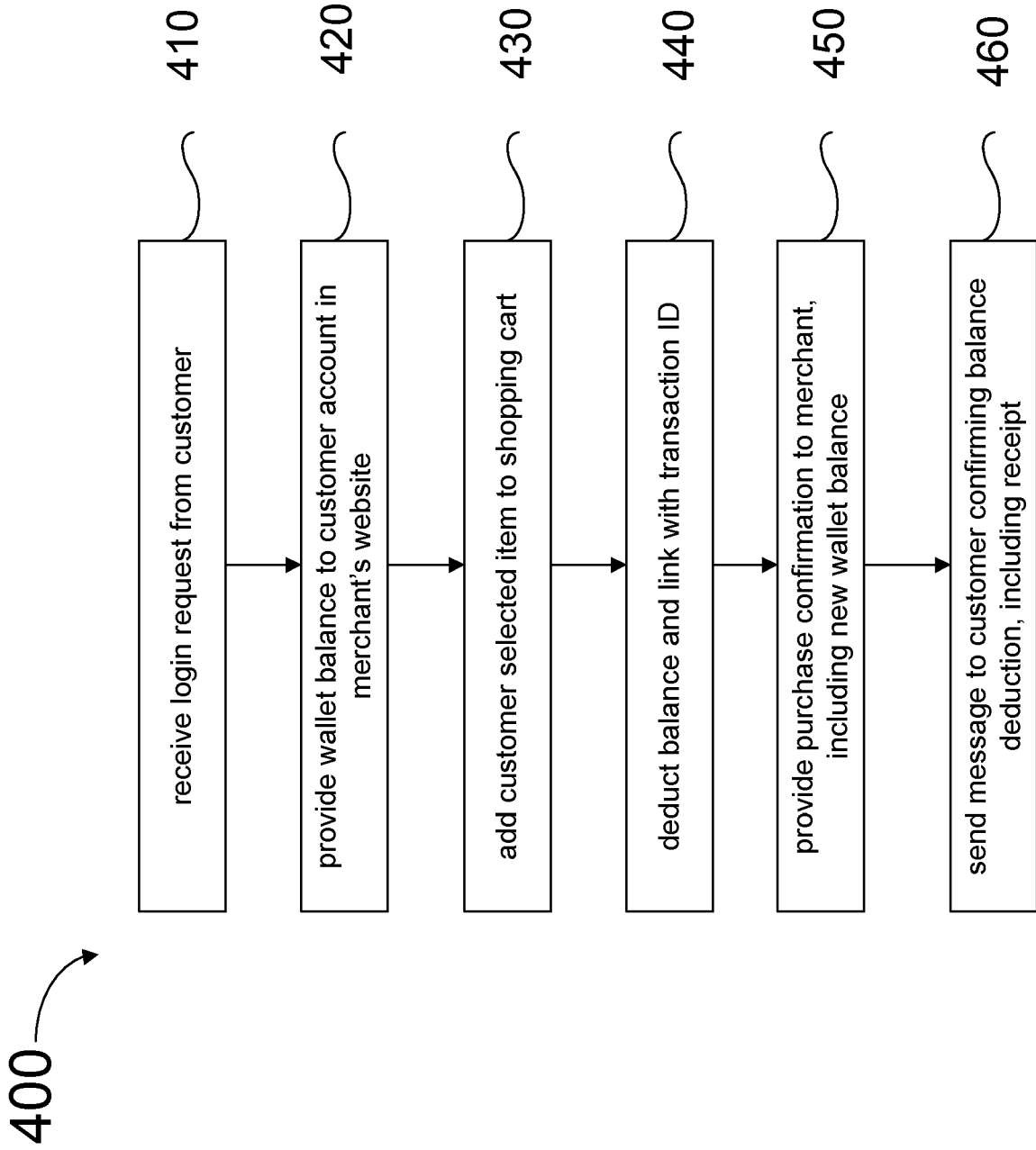


FIG. 4

5/8

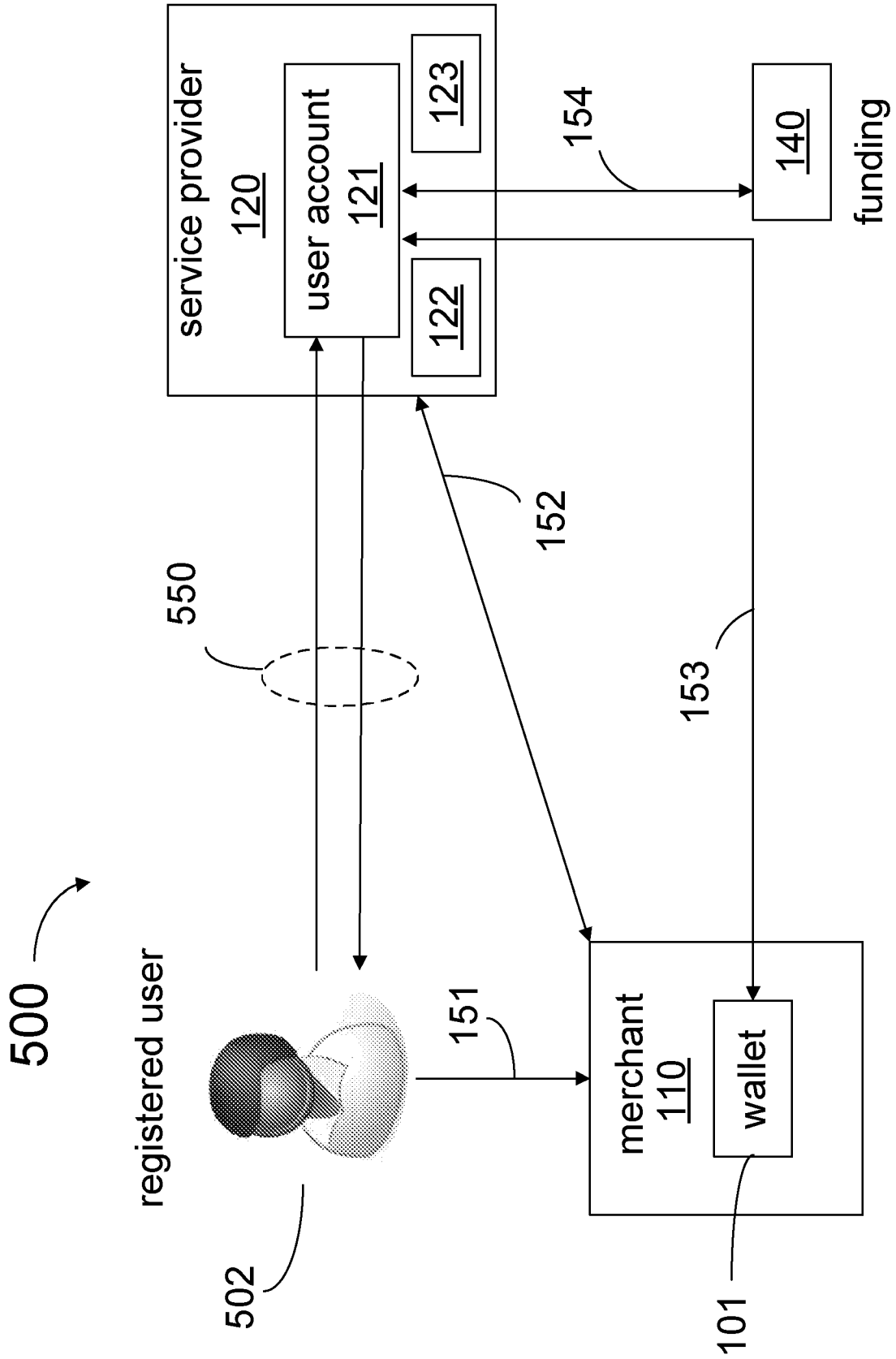


FIG. 5

600 →

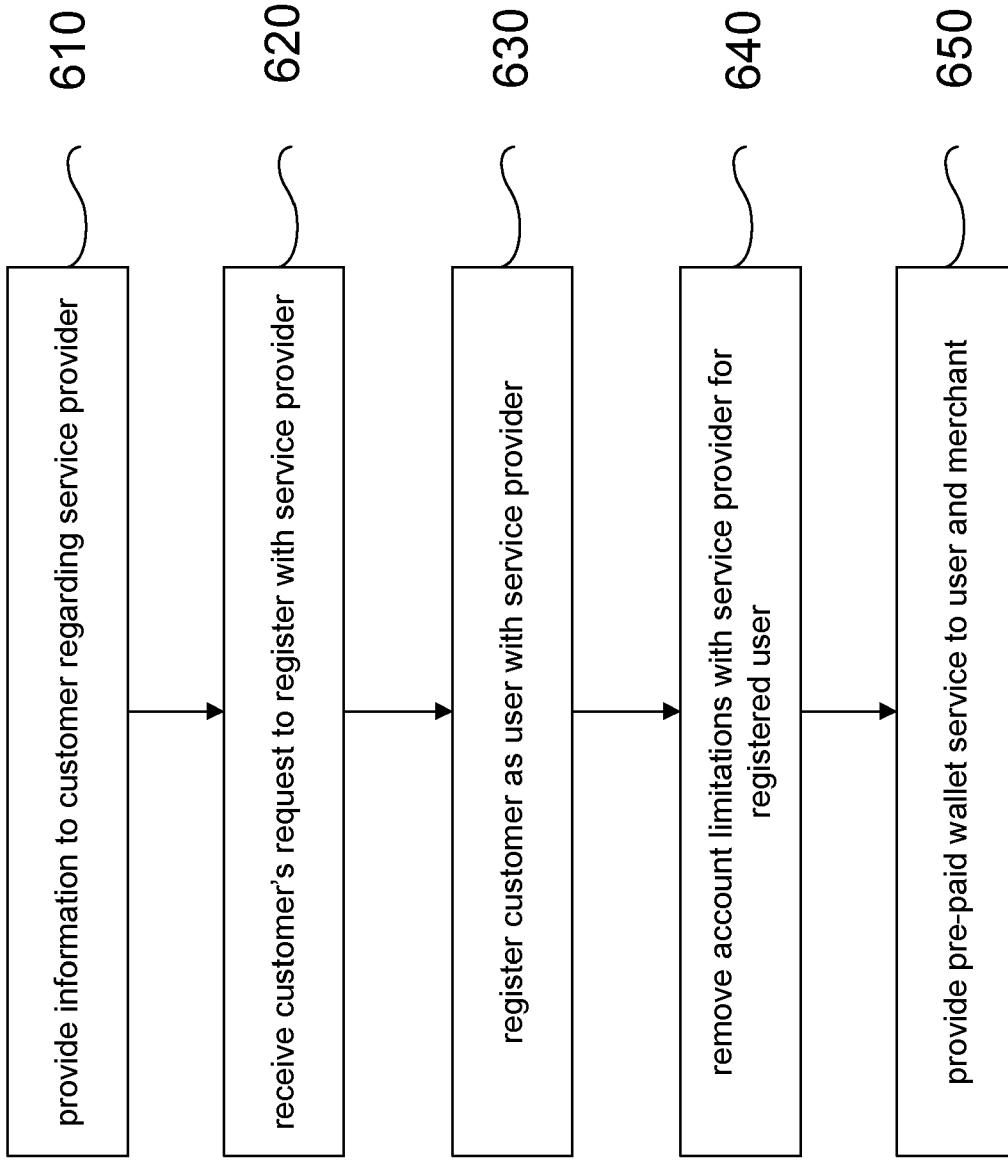


FIG. 6

700 →

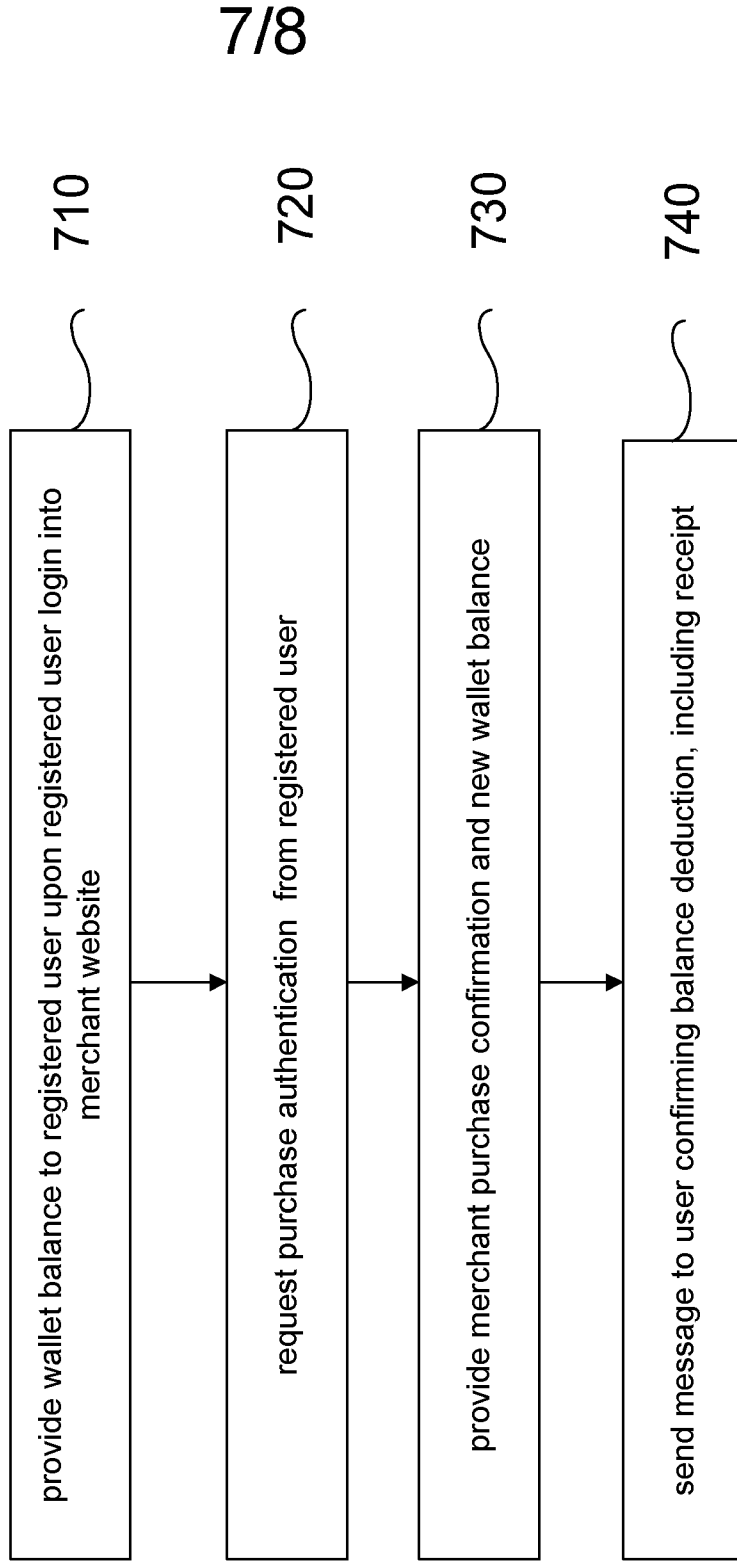


FIG. 7

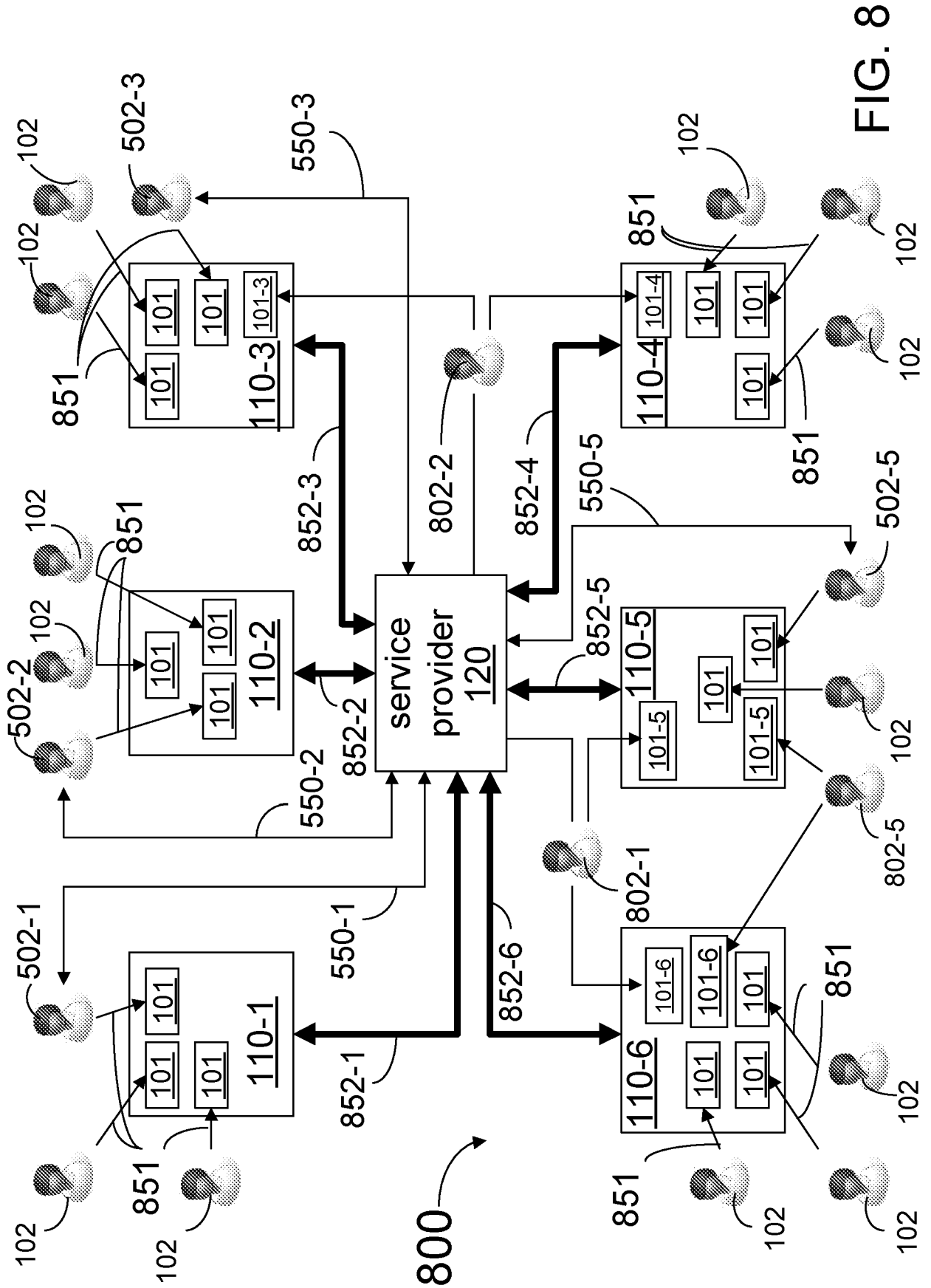


FIG. 8