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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 November 2011 (03.11.2011)

PCT

(10) International Publication Number
WO 2011/137082 A1

(51) International Patent Classification:
*G06Q 40/00* (2006.01)

(21) International Application Number:
PCT/US2011/033828

(22) International Filing Date:
25 April 2011 (25.04.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/328,111 26 April 2010 (26.04.2010) US

(71) Applicant *(for all designated States except US)*: **EBAY, INC.** [US/US]; 2145 Hamilton Avenue, San Jose, California 95125 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TAVEAU, Sebastien** [US/US]; 602 Oak Ridge Drive, Redwood City, California 94061 (US). **DUPRAT, Eric** [FR/US]; 1089 Los Altos Avenue, Los Altos, California 94022 (US).

(74) Agent: **BOWLS, David**; Haynes and Boone, LLP, 2323 Victory Avenue, Suite 700, Dallas, Texas 75219-7673 (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, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

*[Continued on next page]*

(54) Title: REVERSE PAYMENT FLOW

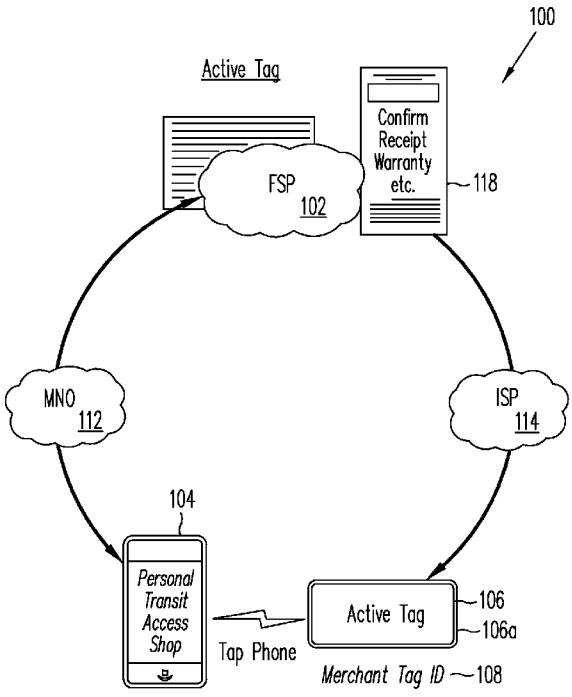



FIG. 1A

(57) Abstract: Systems and methods for facilitating transactions using contactless proximity communication technology include information or payment flows that are reversed from the conventional sense in that information may flow in direction from a merchant via a consumer mobile device to a financial services provider (FSP). Such payment and information flows can be accomplished without needing to modify infrastructure - such as point-of-sale NFC readers, mobile handsets, or advertising tags and may provide "bridge solutions" for quickly implementing mobile proximity purchase payments. Embodiments provide for receiving some transaction information at a financial services provider in response to a contactless proximity communication that occurs between either a consumer proximity tag and a merchant device, consumer mobile device and merchant proximity tag, or consumer mobile device and merchant device, in which some of the transaction information flow is reverse; validating the transaction; sending payment confirmation to the merchant.

WO 2011/137082 A1

**Published**:

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

# REVERSE PAYMENT FLOW

## CROSS REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of United States Provisional Application Number 61/328,111, filed April 26, 2010, which is incorporated by reference. This application is also related to co-pending U.S. Patent Application No. 12/643,972, filed December 21, 2009, titled "Trusted Integrity Manager (TIM)", which is incorporated by reference.

## BACKGROUND

### Technical Field

Embodiments of the present invention generally relate to methods and systems for facilitating commerce and, more particularly, for facilitating the use of mobile devices in commercial and financial transactions.

### Related Art

Mobile proximity payment, e.g., the capability to make a payment at a point of sale with a handheld mobile device – such as a mobile phone – by bringing the mobile device into proximity (typically within about 4 inches) with either a tag or reader device, has been in development for some time, requiring coordination among key stakeholders including, for example, mobile network operators (MNO), merchants, payment processors, banks, and developers. While near field communication (NFC) technology should help further enable mobile payments, successful and established mobile technologies, including SMS (Short Message Service) and USSD (Unstructured Supplementary Service Data), are currently leading the development in payments ecosystems. Delivery of NFC enabled handsets has been limited in volume and accompanied by limited functionalities of those handsets, however, and players in the payments ecosystems have been looking for alternative solutions, also called "bridge solutions".

The most common solutions that have been explored use the contactless sticker (e.g., a radio frequency identification (RFID) tag or NFC-enabled sticker). Many pilot programs using contactless stickers for mobile payment have been conducted around the world. Most of the solutions, however, consistently assume that the consumer is to be the

holder of the sticker and the merchant is to have a point of sale (POS) reader that is enabled to read the sticker, or "tag" as the sticker is commonly referred to. Furthermore, current deployments of stickers are typically for a single provider and limited to a "card emulation mode", in which the NFC device behaves like an existing (e.g., currently known and used technology) contactless card (hence the name "passive" stickers or tags). NFC devices may also be used in a "reader mode", in which the NFC device is active (e.g., able to both transmit and receive information) and reads a passive RFID tag, for example for interactive advertising; and NFC devices may also be used in a "P2P mode" (e.g., "peer-to-peer"), in which two NFC devices are active, communicate together, and exchange information.

## SUMMARY

According to one or more embodiments of the present invention, methods and systems for mobile payments include ways to improve the payment and information flow in mobile proximity payment transactions – e.g., transactions using contactless proximity communication technology, such as near field communication (NFC) – including information or payment flows that are reversed from the conventional sense in that information may flow in a direction from a merchant via a consumer mobile device to a financial services provider. Such payment and information flows in mobile proximity payment transactions may provide innovative ways to process payments on the behalf of a consumer and a merchant that can be accomplished without needing to modify the infrastructure – such as point-of-sale (POS) NFC readers, mobile handsets, or advertising tags and may provide "bridge solutions" for quickly implementing mobile proximity purchase payments.

In one or more embodiments, a system includes: a network computing device of a financial service provider (FSP) for communicating with a consumer mobile device and a merchant device. In response to a contactless proximity communication between either a consumer proximity tag and the merchant device, or the consumer mobile device and a merchant proximity tag, or the consumer mobile device and the merchant device, some transaction information is sent to the FSP via the consumer mobile device; the FSP network computing device validates the transaction information; the FSP network computing device sends a payment credit confirmation to the merchant device; and the FSP network

computing device sends a transaction confirmation message to the consumer mobile device.

In another embodiment, a computer-implemented method includes: receiving some transaction information at a financial services provider (FSP) in response to a contactless proximity communication that occurs either between a consumer proximity tag and a merchant device, between a consumer mobile device and a merchant proximity tag, or between the consumer mobile device and the merchant device, in which at least a portion of the transaction information flows in a direction from the consumer mobile device to the FSP; validating, by the FSP, the transaction information; sending a payment credit confirmation from the FSP to the merchant device; and sending a transaction confirmation message from the FSP to the consumer mobile device.

In a further embodiment, a computer program product comprises a non-transitory computer readable medium having computer readable and executable code for instructing a processor to perform a method that includes: receiving some transaction information at a financial services provider (FSP) in response to a contactless proximity communication that occurs either between a consumer proximity tag and a merchant device, between a consumer mobile device and a merchant proximity tag, or between the consumer mobile device and the merchant device, wherein at least a portion of the transaction information flows in a direction from the consumer mobile device to the FSP; validating, by the FSP, the transaction information; sending a payment credit confirmation from the FSP to the merchant device; and sending a transaction confirmation message from the FSP to the consumer mobile device.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1A and Figure 1B are system diagrams illustrating a comparison between active tag and passive tag process flows in accordance with one or more embodiments.

Figure 2A is a system diagram illustrating a system for providing a proximity payment using a consumer mobile device with a proximity tag and a merchant device in accordance with an embodiment of the invention;

Figure 2B is a flow chart illustrating a method for providing a proximity payment in a system such as the system illustrated in Figure 2A in accordance with an embodiment;

Figure 3A is a system diagram illustrating a system for providing a proximity payment using a consumer mobile device and a merchant having a proximity tag and a secondary device in accordance with an embodiment of the invention;

Figure 3B is a flow chart illustrating a method for providing a proximity payment in a system such as the system illustrated in Figure 3A in accordance with an embodiment;

Figure 4A is a system diagram illustrating a system for providing a proximity payment using a consumer mobile device and a merchant device in accordance with an embodiment of the invention; and

Figure 4B is a flow chart illustrating a method for providing a proximity payment in a system such as the system illustrated in Figure 4A in accordance with an embodiment.

## DETAILED DESCRIPTION

Embodiments of the present invention relate to methods and systems for providing a service that facilitates purchases via mobile proximity payments using, for example, a mobile phone handset or other personal digital device, a sticker or RFID tag, which may be active or passive, and a reader or tag which may be active or passive, at a point of sale (POS) for example, or advertising display. One or more embodiments may provide the "bridge solutions" referred to above and may provide solutions without the need to modify the infrastructure – such as POS NFC readers, mobile handsets, or tags embedded in advertising displays.

In one or more embodiments, a mobile proximity payments service may be provided by a financial service provider (FSP) – such as PayPal, Inc. of San Jose, California – in which a consumer or vendor using the service may have an account with the FSP (referred to as an "FSP account"). Using such a service, according to one or more embodiments, payments may be accomplished using payment and information flows that conventionally would not be expected – such as flows between the consumer and FSP instead of a flow for the same information between the vendor and the FSP, for example, or a flow of information from the vendor through the consumer device to the FSP that is "reverse" in direction from what would be conventionally expected. Broadly, there are three cases that may be described for solutions using these proximity payment information flows in accordance with one or more embodiments.

In a first case, consumers may receive a sticker having an RFID or NFC capability (various NFC-enabled form factors – such as tags, stickers, key fobs, or cards that do not require batteries, for example – all may be referred to herein as "proximity tags") and merchants may have the infrastructure to read the tag (e.g., tag reader, devices for processing information from the tag, lines of communication to the FSP, and established accounts). For example, the consumer proximity tag may operate in card emulation mode and the merchant infrastructure may operate in reader mode. A novel aspect of a solution according to the first case is that it may accept or create an acceptance network of the FSP at the merchant side of a transaction, in accordance with one or more embodiments.

In a second case, the merchant may be provided with the proximity tag (e.g., a sticker having an RFID or NFC capability) and the transaction is controlled through a consumer handset that is enabled for reader mode and can read the merchant proximity tag. For example, the consumer may input some data into the handset that usually is automatically inserted by the POS device (e.g., purchase amount, tips); the merchant may have to trust the consumer is entering the correct data; but this is compensated for by instant confirmation to the merchant via a secondary device which may be connected (e.g., via an internet protocol (IP) network) to the FSP, hence the name "reverse flow" of payments or information.

The novel "reverse flow" solution may allow a quick deployment of both merchant location and consumer devices for payment, providing essential elements of matching a merchant to a consumer based on location and identification. The consumer handset need not be a fully NFC integrated handset, but may be, for example, a phone with an NFC micro-SD (Secure Digital) card that is enabled for reader mode or P2P. The consumer handset may thus provide information such as the merchant tag number identification (ID) and the consumer's (which will also be the merchant's) location that may used, for example, for authenticating the consumer, the merchant, and the transaction by the FSP. The merchant proximity tag may be passive (e.g., simply responding to received input signals) or active (e.g., able to transmit information back to the system). The merchant may be registered with the FSP as having and using the merchant proximity tag unique to the merchant (for example, tags may be numbered). The merchant may also have a secondary, IP-connected device (e.g., personal computer (PC), tablet, or non-NFC enabled phone) to concurrently connect to the FSP and receive the confirmation that the payment

has been sent to the merchant's FSP account by the consumer that just read the merchant's proximity tag.

In one embodiment, for example, using a passive proximity tag, the consumer may feel some inconvenience at having to input some data (e.g., payment amount, tips) that may automatically be inserted by the POS using an active proximity tag (which may be BlueTooth® enabled, or Wi-Fi®, for example) or using any other wireless or contactless means. Passive tags may well-suited, however, for fixed price purchases – such as fixed menus in fast-food restaurants, transit fares, charitable contributions, or museum tickets, to name a few examples. In other embodiments, the consumer may feel less inconvenience as an active proximity tag may be able to provide the necessary input. In another embodiment, the consumer may acquire the merchant ID tag number and send that information back to the FSP; the FSP may then pull from the merchant's secondary, IP-connected device the amount of the transaction and itemization of products purchased, send that information back to the consumer for validation and approval, and deliver confirmation immediately to the merchant. Solutions – including bridge solutions and other solutions for early deployment, fast enabling, and parallel technology –employing embodiments with such back-and-forth intensive usage of network connectivity (e.g., public switched telephone network (PSTN) and Internet), while once seemingly impractical, have become achievable with the advent of always-on, data intensive portable devices.

In a third case, both consumer and merchant may have an NFC, or other contactless, communication-enabled device. Contrary to conventional transactions, however, embodiments may employ "reverse flow" of information and payments in which the consumer may be in control the transaction from the consumer's device by entering information that is sent to the FSP, providing, for example, an entry point to the consumer's virtual "wallet" maintained by the FSP in the "cloud". In this case of reverse flow, however, in which both consumer and merchant devices may operate in P2P mode, the merchant may be able to share data with the consumer in a more robust and constant state. For example, a device state of being always-on and connected to the system of the FSP may enable the FSP to provide services to both merchant and consumer that may include, for example, allowing the management by the FSP of a real dynamic "wallet" for the consumer. Services provided by the FSP may include ID management, transaction logs

and storage, automatic warranty enrollment, and products data information and registration, for example. In an alternative embodiment in which both consumer and merchant devices may operate in P2P mode, the merchant may be in control of the transaction, depending, for example, on a relative advantage provided by either the merchant or the consumer device. Thus, the FSP may be enabled to provide a best choice option of information flow for the consumer, the merchant, and the FSP that can be used to customize information flow in each situation as needed.

Figure 1A and Figure 1B show a system 100 for facilitating the use of mobile devices in commercial and financial transactions (including response to advertising) using contactless proximity communication technology such as NFC tags and readers. System 100 may include a financial services provider (FSP) 102 that may provide a number of services enabling, for example, mobile proximity payments and other types of transactions from a consumer mobile device 104 (such as a mobile phone). Proximity tag 106 may be either an active tag 106a (Figure 1A) or a passive tag 106b (Figure 1B). Data may be retrieved from the proximity tag 106 by bringing the mobile device 104 into proximity (typically less than 4 inches) with the proximity tag 106 as indicated in the figures by the lightning bolt and the legend "tap phone". Data retrieved from the proximity tag 106 may include a unique identifying symbol sequence indicated in the figures as "merchant tag ID" 108. The unique identifying symbol sequence of merchant tag ID 108 may be in either a hard or soft format (e.g., either "hard-coded" into each tag or programmable into each tag as the tag is deployed).

Upon retrieving the merchant tag ID 108, the mobile device 104 (connected to FSP 102 via a mobile network operator (MNO) 112) may send the merchant tag ID 108 and additional information – such as the value of a counter in the passive or active proximity tag 106, the consumer's FSP account number, authentication, and geo-location – to the FSP 102 for matching, e.g., validation and authentication. The merchant (or other party, e.g., advertiser) user of proximity tag 106 may also be able to communicate with FSP 102 via an IP-connected, secondary device 110 via either of MNO 113 or internet service provider (ISP) 114. Each party (e.g., the consumer or user of mobile device 104 and the merchant or user of active or passive tag 106) may have a registered account with the FSP 102 and a sticker (e.g. proximity tag 106) registered to a specific account, either for the merchant or for the consumer or both. For example, the merchant may receive the confirmation via

secondary device 110 that a payment has been sent to the merchant's FSP account by the consumer that just read the merchant's proximity tag; or , in the case of an active tag 106a, there may be direct communication between the active tag 106a and FSP 102 via ISP 114. Successfully completing transactions in a timely manner may require quick, accurate matching, and the FSP account of each party (e.g., the consumer or user of mobile device 104 and the merchant or user of active or passive tag 106) should be credited or debited the proper amount to or from the proper party so that all accounts reconcile. In order to achieve such real-time reconciliation, a system architecture that implements various modules may be implemented by FSP 102. A number of key functions of such a system architecture can be found in co-pending U.S. Patent Application No. 12/643,972, filed December 21, 2009, titled "Trusted Integrity Manager (TIM)", which is incorporated by reference.

Data retrieved – by the mobile device 104, for example, in the case of using a merchant proximity tag, or by the merchant tag reader or active tag 106a in the case of using a consumer device proximity tag – from a proximity tag 106 (which may be in use, for example, by a merchant, an advertiser, or a consumer) may include a unique tag identifier assigned to only that proximity tag (for example, the merchant tag ID 108 belonging to a merchant tag 106 or a consumer tag ID belonging to a consumer tag). The unique tag identifier may, for example, include a number that is physically internal to the tag to avoid its possible duplication or theft and may be included, for example, during manufacture of each tag or programmed in later. Data retrieved from a proximity tag 106 may also include a unique identifier assigned to the entity receiving the tag (e.g., merchant's individual electronic cash register (ECR), a store, a location, or an individual merchant, for example). Data retrieved from a proximity tag 106 may also include a unique identifier to specify the physical (geographical) location of the tag. In addition, in the case of a fixed transaction amount tag, the value (e.g., $5, $10, for example) assigned to the tag may be retrieved.

The foregoing data may be assigned to and included in a passive tag. For an active tag, e.g., proximity tag 106a, additional data may also include a "dynamic" value assigned at the time the transaction amount is compounded. Such a dynamic value may be transmitted to the proximity tag 106a via a channel other than NFC (e.g., BlueTooth).

Additional data may also include an element of "authentication" or "validation" that may vary based on the type of reader in the mobile device 104 used by the consumer.

Data read from the proximity tag 106, along with data from the mobile device 104 – such as the mobile device ID or ID of a proximity tag attached to the mobile device 104, the consumer ID or password entered, or current geo-location, for example – may be sent by the mobile device 104 to the FSP 102. This data may then be "matched" (e.g., processed for authentication, validation, and accounting) by the FSP 102 between the two FSP accounts – one for the consumer and one for the merchant. The transaction processing by the FSP 102 may include more than that for a standard two-account transaction. For example, a pre-registration for risk consideration and to be accepted by the system 100 may be required. Monitoring for legitimate usage of the proximity tag and accurate consumer input of the transaction information to the mobile device 104 may be required. Additional processing, beyond that for a standard two-account transaction, may be required by the FSP 102 for return and chargeback. Because the consumer will be in charge of the transaction, FSP 102 may be required to keep a transactions log on behalf of each merchant. Consumers may be able to review their history, for example, but the merchants may need to be able to go back to their history and modify it for return or refund, for example. Such issues may be addressed by an adaptive payment or adaptive accounts mechanism implemented by the FSP 102.

Figure 2A illustrates a portion of a system 100 (see Figure 1) for facilitating the use of mobile devices in commercial and financial transactions (including response to advertising) using contactless proximity communication technology. As shown in Figure 2A, a consumer mobile device 104 may be provided with a proximity tag 116, which may be a passive tag. The consumer proximity tag 116 may have a consumer passive tag ID 107 that is uniquely assigned to the consumer proximity tag 116; the passive tag ID 107 may be internal to the consumer proximity tag 116; and the consumer proximity tag 116 may be readable, for example, by merchant secondary, IP-connected device 110. For example, device 110 may be an NFC device or may be a device with an NFC add-on such as a PC USB (universal serial bus) reader. In general, such a consumer passive proximity tag 116 may be provided to a consumer as a readily implementable "bridge solution" for providing mobile proximity payment capability for a mobile device 104 that is not equipped for contactless proximity communication, e.g., not NFC-enabled.

Figure 2B shows a flow chart for a transaction according to a method 200 that may be accomplished in the embodiment shown in Figure 2A. At step 201, a consumer (e.g., a user of mobile device 104) may bring the consumer proximity tag 116 into close proximity with a device capable of reading the consumer proximity tag 116 (e.g., merchant device 110, which may have a connection to FSP 102 via an ISP 114 or MNO 113, as shown, or other means) sufficient for the device 110 to read the tag 116. At step 202, the merchant (e.g., merchant device 110 may send transaction information – such as the dollar amount of the transaction and consumer ID, which may be passive tag ID 107, for example – to FSP 102.

At step 203, FSP 102 may authenticate and validate the transaction between the merchant and consumer, for example, by matching the consumer ID with an FSP account of the consumer, matching the merchant ID – which may be provided by device 110 or by a device ID of device 110, for example, with an FSP account of the merchant, and by matching the known location of the merchant (e.g., from merchant's FSP account information) with the location of the purchase derived, for example, from the IP address of IP-connected merchant device 110 or by a Global Positioning System (GPS) geo-location capability of either of consumer device 104 or merchant device 110.

At step 204, the FSP 102 may send a payment credit confirmation to the merchant device 110 via either of ISP 114 or MNO 113. For example, because the FSP 102 may provide accounts to both the consumer and the merchant, the FSP 102 may be able to debit one account and credit the other, and thus provide credit confirmation to the merchant via merchant device 110. Likewise, at step 205, FSP 102 may send the consumer a transaction confirmation message to consumer mobile device 104 to inform the consumer of the debit on the consumer's FSP account. The transaction confirmation message may be sent from a network computing device of FSP 102, for example, to consumer mobile device 104 via a text message using Short Message Service (SMS) or using e-mail. At step 206, FSP 102 may generate a receipt of the transaction for either or both of the consumer's and merchant's FSP account records, with merchant information placed in the consumer's FSP online account for potential refunds or returns.

Figure 3A illustrates a portion of a system 100 (see Figure 1) for facilitating the use of mobile devices in commercial and financial transactions (including response to advertising) using contactless proximity communication technology.

As shown in Figure 3A, a merchant may be provided with a proximity tag 106, which may be either a passive or active tag (e.g., active tag 106a or passive tag 106b as shown in Figure 1). The merchant proximity tag 106 may have a merchant tag ID 108 that is uniquely assigned to the merchant proximity tag 106 or to the merchant. The merchant tag ID 108 may be internal to the merchant proximity tag 106, and the merchant proximity tag 106 may be readable by consumer mobile device 104. For example, consumer mobile device 104 may be an NFC-enabled device or may be a device with an NFC add-on such as a PC USB (universal serial bus) reader. In general, merchant active or passive proximity tags such as tag 106 may be provided to merchants as a readily implementable "bridge solution" for providing mobile proximity payment capability for consumer mobile devices 104 that are equipped for contactless proximity communication when the merchant may not have or be able to readily obtain a device equipped for contactless proximity communication, e.g., an NFC reader.

Figure 3B shows a flow chart for a transaction according to a method 300 that may be accomplished in the embodiment shown in Figure 3A. At step 301, a consumer (e.g., a user of mobile device 104) may launch an "app" (application) on consumer mobile device 104. The app may be provided by the FSP 102. The app may, for example, place the consumer mobile device 104, which may be capable of reading a proximity tag 106 using contactless proximity communication technology such as NFC, in a state in which it is ready to read the merchant proximity tag 106 and process the information read from the merchant proximity tag 106, such as storing the information or sending it to FSP102. The consumer may then bring the consumer mobile device 104 into close proximity with merchant tag 106 sufficient for the consumer mobile device 104 to read the tag 106. Method 300 may then continue according to one of either of two scenarios. In a first scenario ("Scenario 1") the merchant proximity tag 106 may provide consumer mobile device 104 with a merchant tag ID 108 and, for example, a fixed amount (denoted in a currency, e.g., dollar) for the transaction. Such a fixed amount may come from an advertising poster incorporating a merchant proximity tag 106, for example, a poster advertising a concert or event; or may come, for another example, from a choice of a specific item from a fast food menu. In a second scenario("Scenario 2") the merchant proximity tag 106 may provide consumer mobile device 104 with a merchant tag ID 108.

In the first scenario, at step 302, the consumer mobile device 104 may acquire (e.g., via NFC between mobile device 104 and proximity tag 106) the merchant ID (e.g., merchant tag ID 108) and the fixed (e.g., pre-set) amount from the merchant proximity tag 106.

In the second scenario, at step 303, the consumer mobile device 104 may acquire (e.g., via NFC between mobile device 104 and proximity tag 106) the merchant ID (e.g., merchant tag ID 108) from the merchant proximity tag 106. At step 305, merchant information fields of the FSP app launched in step 301 may be populated automatically. Such fields may include information such as the merchant ID, location, product identification, and purchase price, for example. At step 307, in the second scenario, the consumer may manually enter additional information into the FSP app, such as the transaction amount, for example, if not already entered automatically.

In either of the first or second scenarios, at step 308 or step 309, data collected from the merchant (e.g., the information from the merchant proximity tag 106 or information either populated automatically by the FSP app or manually entered into the FSP app) and the credentials from the consumer device (e.g., consumer ID, mobile device 104 ID, or tag ID 107, for example) are sent to the FSP 102. This transaction information may be sent, for example, from consumer mobile device 104 via MNO 112 to FSP 102.

At step 310 or step 311, in scenario 1 or scenario 2, respectively, FSP 102 may authenticate and validate the transaction between the merchant and consumer, as described above. For example, FSP 102 may match the consumer ID with the consumer FSP account and the merchant ID with the merchant FSP account; may validate the location of the consumer with the location of the purchase and the known location of the merchant using, for example, IP addresses or GPS geo-location, as described above.

In either scenario 1 or 2, at step 312 or step 313, the FSP 102 may send a payment credit confirmation to the merchant. As described above, because the FSP 102 may provide accounts to both the consumer and the merchant, the FSP 102 may be able to debit one account and credit the other, and thus provide credit confirmation to the merchant via merchant device 110, and likewise, provide a transaction confirmation message to the consumer via consumer mobile device 104. The payment credit confirmation may include, for example, the amount credited to the merchant's FSP account, with the consumer ID, and the inventory purchased. The payment credit confirmation may be sent, for example,

to IP-connected, secondary merchant device 110 using SMS or e-mail. At step 314 or step 315, in scenario 1 or scenario 2 respectively, the FSP 102 may send a transaction confirmation message to the consumer to inform the consumer of the debit on consumer's FSP account. The transaction confirmation message may be sent to consumer mobile device 104, for example, using SMS or email via MNO 112. At step 316 or step 317, respectively in scenario 1 or scenario 2, the FSP 102may generate a receipt 118 (see Figure 1) of the transaction for either or both of the consumer's and merchant's FSP account records, with merchant information placed in the consumer's FSP online account for potential refunds or returns, and FSP 102 may update the consumer credentials.

Figure 4A illustrates a portion of a system 100 (see Figure 1) for facilitating the use of mobile devices in commercial and financial transactions (including response to advertising) using contactless proximity communication technology. As shown in Figure 4A, a merchant may provide a contactless proximity communication device, such as merchant device 110, at a point-of-sale. The merchant device 110 may be an NFC-enabled device or may be a device with an NFC add-on such as a PC USB reader. Merchant device 110 may be connected with FSP 102 via an ISP 114 as shown. Similarly, in this case, consumer mobile device 104 may be an NFC-enabled device or may be a device with an NFC add-on such as a PC USB reader. Both the merchant and the consumer may have accounts with the FSP 102 and both may be able to provide credentials, such as a consumer ID and device ID for consumer mobile device 104, or a merchant ID and geo-location and device ID for merchant device 110.

Figure 4B shows a flow chart for a transaction according to a method 400 that may be accomplished in the embodiment shown in Figure 4A. At step 401, a consumer (e.g., a user of mobile device 104) may launch an "app" (application) on consumer mobile device 104. The app may be provided by the FSP 102. The app may, for example, place the consumer mobile device 104, which may be capable of communicating with merchant device 110 using contactless proximity communication technology such as NFC, in a state in which it is ready to communicate information with the merchant device 110 and process the information, such as storing the information or sending it to FSP102. The consumer may then bring the consumer mobile device 104 into close proximity with merchant device 110 sufficient for the consumer mobile device 104 to communicate with merchant device 110. For example, consumer "taps" consumer mobile device 104 to merchant device 110.

Method 400 may then continue according to one of either of two scenarios. In a first scenario ("Scenario 1") the consumer may control the flow of information in that transaction information flow travels via consumer mobile device 104 to FSP 102. In a second scenario("Scenario 2") the merchant may control the flow of information in that transaction information flow travels via merchant device 110 to FSP 102.

In the first scenario, at step 402, the consumer mobile device 104 may acquire (e.g., via NFC between consumer mobile device 104 and merchant device 110) the merchant ID (e.g., a device ID from device 110) and a transaction amount, which may be a fixed or pre-set amount from the merchant device 110.

In the second scenario, at step 403, the merchant device 110 may acquire (e.g., via NFC between consumer mobile device 104 and merchant device 110) the consumer ID (e.g., device ID from device 104) or other pre-authorized consumer credentials. At step 405, in the second scenario, the consumer may confirm information, such as the transaction amount, on the merchant device 110, for example, by entering information on a keypad or touch screen.

In either of the first or second scenarios, at step 408 or step 409, data collected from the merchant (e.g., the information from the merchant device 110 or information from the consumer mobile device 104) and the credentials from the consumer device (e.g., consumer ID, mobile device 104 ID, or tag ID 107, for example) may be sent to the FSP 102. This transaction information may be sent, in the first scenario, for example, from consumer mobile device 104 via MNO 112 to FSP 102. The transaction information may be sent, in the second scenario, for example, from merchant device 110 via ISP 114 to FSP 102 or from consumer mobile device 104 via MNO 112 to FSP 102.

At step 410 or step 411, in scenario 1 or scenario 2, respectively, FSP 102 may authenticate and validate the transaction between the merchant and consumer, as described above. For example, FSP 102 may match the consumer ID with the consumer FSP account and the merchant ID with the merchant FSP account; may validate the location of the consumer with the location of the purchase and the known location of the merchant using, for example, IP addresses or GPS geo-location, as described above.

In either scenario 1 or 2, at step 412 or step 413, the FSP 102 may send a payment credit confirmation to the merchant. As described above, because the FSP 102 may provide accounts to both the consumer and the merchant, the FSP 102 may be able to debit

one account and credit the other, and thus provide credit confirmation to the merchant via merchant device 110, and likewise, provide a transaction confirmation message to the consumer via consumer mobile device 104. The payment credit confirmation may include, for example, the amount credited to the merchant's FSP account, with the consumer ID, and the inventory purchased. The payment credit confirmation may be sent, for example, to IP-connected, secondary merchant device 110 using SMS or e-mail. At step 414 or step 415, in scenario 1 or scenario 2 respectively, the FSP 102 may send a transaction confirmation message to the consumer to inform the consumer of the debit on consumer's FSP account. The transaction confirmation message may be sent to consumer mobile device 104, for example, using SMS or email via MNO 112. At step 416 or step 417, respectively in scenario 1 or scenario 2, the FSP 102 may generate a receipt 118 (see Figure 1) of the transaction for either or both of the consumer's and merchant's FSP account records, with merchant information placed in the consumer's FSP online account for potential refunds or returns, and the FSP 102 may update the consumer credentials.

In implementation of the various embodiments, embodiments of the invention may comprise a personal computing device, such as a personal computer, laptop, PDA, cellular phone or other personal computing or communication devices. The payment provider system may comprise a network computing device, such as a server or a plurality of servers, computers, or processors, combined to define a computer system or network to provide the payment services provided by a payment provider system.

In this regard, a computer system may include a bus or other communication mechanism for communicating information, which interconnects subsystems and components, such as processing component (e.g., processor, micro-controller, digital signal processor (DSP), etc.), system memory component (e.g., RAM), static storage component (e.g., ROM), disk drive component (e.g., magnetic or optical), network interface component (e.g., modem or Ethernet card), display component (e.g., CRT or LCD), input component (e.g., keyboard or keypad), and/or cursor control component (e.g., mouse or trackball). In one embodiment, disk drive component may comprise a database having one or more disk drive components.

The computer system may perform specific operations by processor and executing one or more sequences of one or more instructions contained in a system memory component. Such instructions may be read into the system memory component from

another computer readable medium, such as static storage component or disk drive component. In other embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention.

Logic may be encoded in a computer readable and executable medium, which may refer to any medium that participates in providing instructions to the processor for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. In one embodiment, the computer readable medium is non-transitory. In various implementations, non-volatile media includes optical or magnetic disks, such as disk drive component, volatile media includes dynamic memory, such as system memory component, and transmission media includes coaxial cables, copper wire, and fiber optics, including wires that comprise bus. In one example, transmission media may take the form of acoustic or light waves, such as those generated during radio wave and infrared data communications.

Some common forms of computer readable and executable media include, for example, floppy disk, flexible disk, hard disk, magnetic tape, any other magnetic medium, CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, RAM, ROM, E2PROM, FLASH-EPROM, any other memory chip or cartridge, carrier wave, or any other medium from which a computer is adapted.

In various embodiments, execution of instruction sequences for practicing the invention may be performed by a computer system. In various other embodiments, a plurality of computer systems coupled by communication link (e.g., LAN, WLAN, PTSN, or various other wired or wireless networks) may perform instruction sequences to practice the invention in coordination with one another.

Computer system may transmit and receive messages, data, information and instructions, including one or more programs (i.e., application code) through communication link and communication interface. Received program code may be executed by processor as received and/or stored in disk drive component or some other non-volatile storage component for execution.

Where applicable, various embodiments provided by the present disclosure may be implemented using hardware, software, or combinations of hardware and software. Also, where applicable, the various hardware components and/or software components set forth herein may be combined into composite components comprising software, hardware,

and/or both without departing from the spirit of the present disclosure. Where applicable, the various hardware components and/or software components set forth herein may be separated into sub-components comprising software, hardware, or both without departing from the scope of the present disclosure. In addition, where applicable, it is contemplated that software components may be implemented as hardware components and vice-versa – for example, a virtual Secure Element (vSE) implementation or a logical hardware implementation.

Software, in accordance with the present disclosure, such as program code and/or data, may be stored on one or more computer readable and executable mediums. It is also contemplated that software identified herein may be implemented using one or more general purpose or specific purpose computers and/or computer systems, networked and/or otherwise. Where applicable, the ordering of various steps described herein may be changed, combined into composite steps, and/or separated into sub-steps to provide features described herein.

The foregoing disclosure is not intended to limit the present invention to the precise forms or particular fields of use disclosed. It is contemplated that various alternate embodiments and/or modifications to the present invention, whether explicitly described or implied herein, are possible in light of the disclosure. Having thus described various example embodiments of the disclosure, persons of ordinary skill in the art will recognize that changes may be made in form and detail without departing from the scope of the invention. Thus, the invention is limited only by the claims.

# CLAIMS

What is claimed is:

1. A system comprising:

a network computing device of a financial service provider (FSP) for communicating with a consumer mobile device and a merchant device, wherein:

in response to a contactless proximity communication between either a consumer proximity tag and the merchant device, or the consumer mobile device and a merchant proximity tag, or the consumer mobile device and the merchant device:

transaction information is sent to the FSP via the consumer mobile device;

the network computing device validates the transaction information;

the network computing device sends a payment credit confirmation to the merchant device; and

the network computing device sends a transaction confirmation message to the consumer mobile device.

2. The system of claim 1, wherein:

the contactless proximity communication is between the consumer proximity tag and the merchant device;

the consumer proximity tag is a passive tag having a unique consumer identification (ID); and

the transaction information sent to the FSP includes the consumer ID associated with the consumer proximity tag, and a geo-location of the transaction.

3. The system of claim 1, wherein:

the contactless proximity communication is between the consumer mobile device and the merchant proximity tag;

the consumer mobile device has a mobile device ID;

the merchant proximity tag is a proximity tag having a unique merchant ID; and

the transaction information sent to the FSP includes the mobile device ID, the unique merchant ID associated with the merchant proximity tag, and a geo-location of the transaction.

4. The system of claim 1, wherein:

the contactless proximity communication is between the consumer mobile device and the merchant device;

the consumer mobile device has a mobile device ID;

the merchant device has a unique merchant ID; and

the transaction information sent to the FSP includes the mobile device ID, the unique merchant ID associated with the merchant device, and a geo-location of the transaction.

5. The system of claim 1, wherein:

the FSP validates the transaction information by matching a consumer ID with a consumer FSP account, matching a merchant ID with a merchant FSP account, and matching a geo-location sent to the FSP via the consumer mobile device with a known location for the merchant.

6. The system of claim 1, wherein:

the merchant device is an internet protocol (IP)-connected device; and

the FSP sends the payment credit confirmation to the merchant device via IP.

7. The system of claim 1, wherein:

the consumer mobile device has either an e-mail or Short Message Service (SMS) capability; and

the FSP sends the transaction confirmation message to the consumer mobile device using SMS or e-mail.

8. A computer-implemented method comprising:

receiving a transaction information at a financial services provider (FSP) in response to a contactless proximity communication that occurs either between a consumer proximity tag and a merchant device, between a consumer mobile device and a merchant proximity tag, or between the consumer mobile device and the merchant device, wherein at

least a portion of the transaction information flows in a direction from the consumer mobile device to the FSP;

validating, by the FSP, the transaction information;

sending a payment credit confirmation from the FSP to the merchant device; and

sending a transaction confirmation message from the FSP to the consumer mobile device.

9. The method of claim 8, wherein:

the contactless proximity communication is between the consumer proximity tag and the merchant device;

the consumer proximity tag is a passive tag having a unique consumer identification (ID); and

the transaction information received by the FSP includes the consumer ID associated with the consumer proximity tag, and a geo-location of the transaction.

10. The method of claim 8, wherein:

the contactless proximity communication is between the consumer mobile device and the merchant proximity tag;

the consumer mobile device has a mobile device ID;

the merchant proximity tag is a proximity tag having a unique merchant ID; and

the transaction information received by the FSP includes the mobile device ID, the unique merchant ID associated with the merchant proximity tag, and a geo-location of the transaction.

11. The method of claim 8, wherein:

the contactless proximity communication is between the consumer mobile device and the merchant device;

the consumer mobile device has a mobile device ID;

the merchant device has a unique merchant ID; and

the transaction information sent to the FSP includes the mobile device ID, the unique merchant ID associated with the merchant device, and a geo-location of the transaction.

12. The method of claim 8, wherein:

the FSP validates the transaction information by matching a consumer ID with a consumer FSP account, matching a merchant ID with a merchant FSP account, and matching a geo-location received by the FSP via the consumer mobile device with a known location for the merchant.

13. The method of claim 8, wherein:

the merchant device is an internet protocol (IP)-connected device; and

the FSP sends the payment credit confirmation to the merchant device via IP.

14. The method of claim 8, wherein

the consumer mobile device has either an e-mail or Short Message Service (SMS) capability; and

the FSP sends the transaction confirmation message to the consumer mobile device using SMS or e-mail.

15. A computer program product comprising a non-transitory computer readable medium having computer readable and executable code for instructing a processor to perform a method, the method comprising:

receiving a transaction information at a financial services provider (FSP) in response to a contactless proximity communication that occurs either between a consumer proximity tag and a merchant device, between a consumer mobile device and a merchant proximity tag, or between the consumer mobile device and the merchant device, wherein at least a portion of the transaction information flows in a direction from the consumer mobile device to the FSP;

validating, by the FSP, the transaction information;

sending a payment credit confirmation from the FSP to the merchant device; and

sending a transaction confirmation message from the FSP to the consumer mobile device.

16. The computer program product of claim 15 wherein:

the contactless proximity communication is between the consumer proximity tag and the merchant device;

the consumer proximity tag is a passive tag having a unique consumer identification (ID); and

the transaction information received by the FSP includes the consumer ID associated with the consumer proximity tag, and a geo-location of the transaction.

17. The computer program product of claim 15 wherein:

the contactless proximity communication is between the consumer mobile device and the merchant proximity tag;

the consumer mobile device has a mobile device ID;

the merchant proximity tag is a proximity tag having a unique merchant ID; and

the transaction information received by the FSP includes the mobile device ID, the unique merchant ID associated with the merchant proximity tag, and a geo-location of the transaction.

18. The computer program product of claim 15 wherein

the contactless proximity communication is between the consumer mobile device and the merchant device;

the consumer mobile device has a mobile device ID;

the merchant device has a unique merchant ID; and

the transaction information sent to the FSP includes the mobile device ID, the unique merchant ID associated with the merchant device, and a geo-location of the transaction.

19. The computer program product of claim 15 wherein

the FSP validates the transaction information by matching a consumer ID with a consumer FSP account, matching a merchant ID with a merchant FSP account, and matching a geo-location received by the FSP via the consumer mobile device with a known location for the merchant.

20. The computer program product of claim 15 wherein

the merchant device is an internet protocol (IP)-connected device; and

the FSP sends the payment credit confirmation to the merchant device via IP.

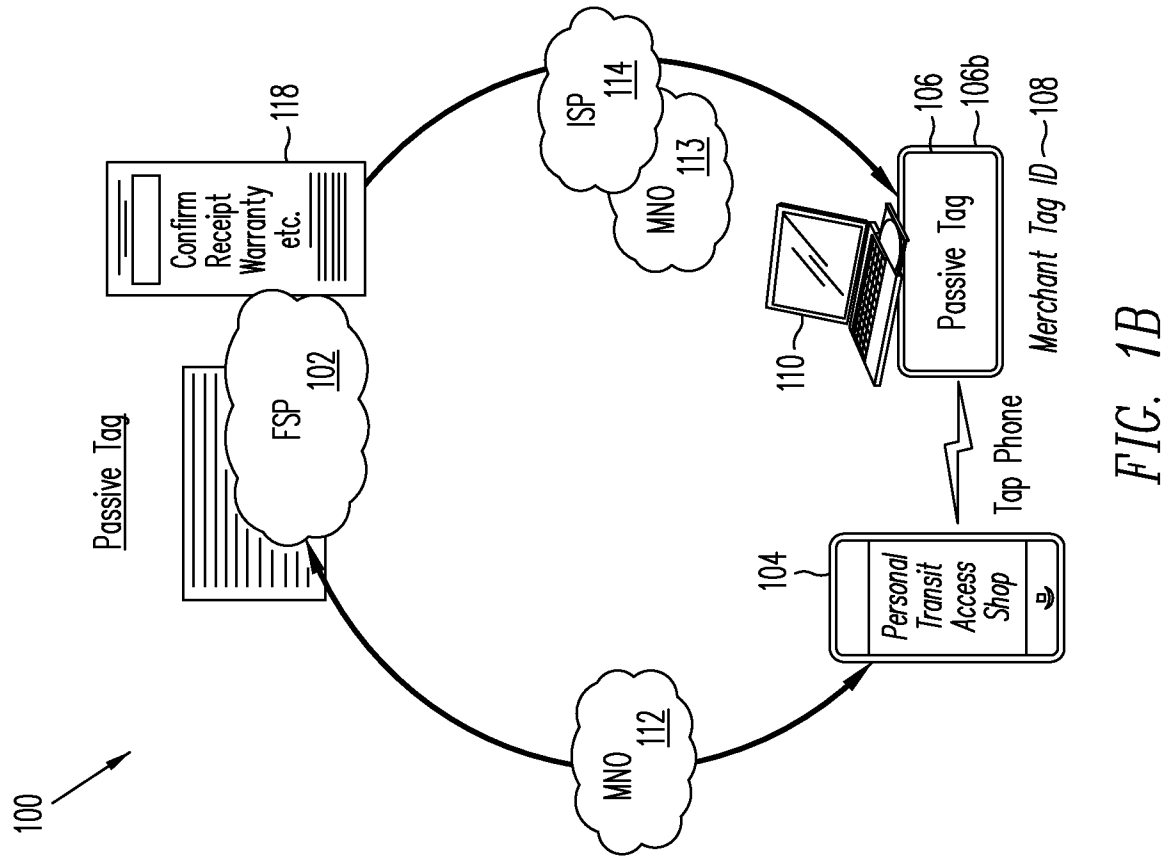

100
Passive Tag
FSP 102
Confirm Receipt Warranty etc.
118
ISP 114
MNO 113
106
106b
Passive Tag
Merchant Tag ID
108
110
Tap Phone
104
Personal Transit Access Shop
MNO 112

FIG. 1B

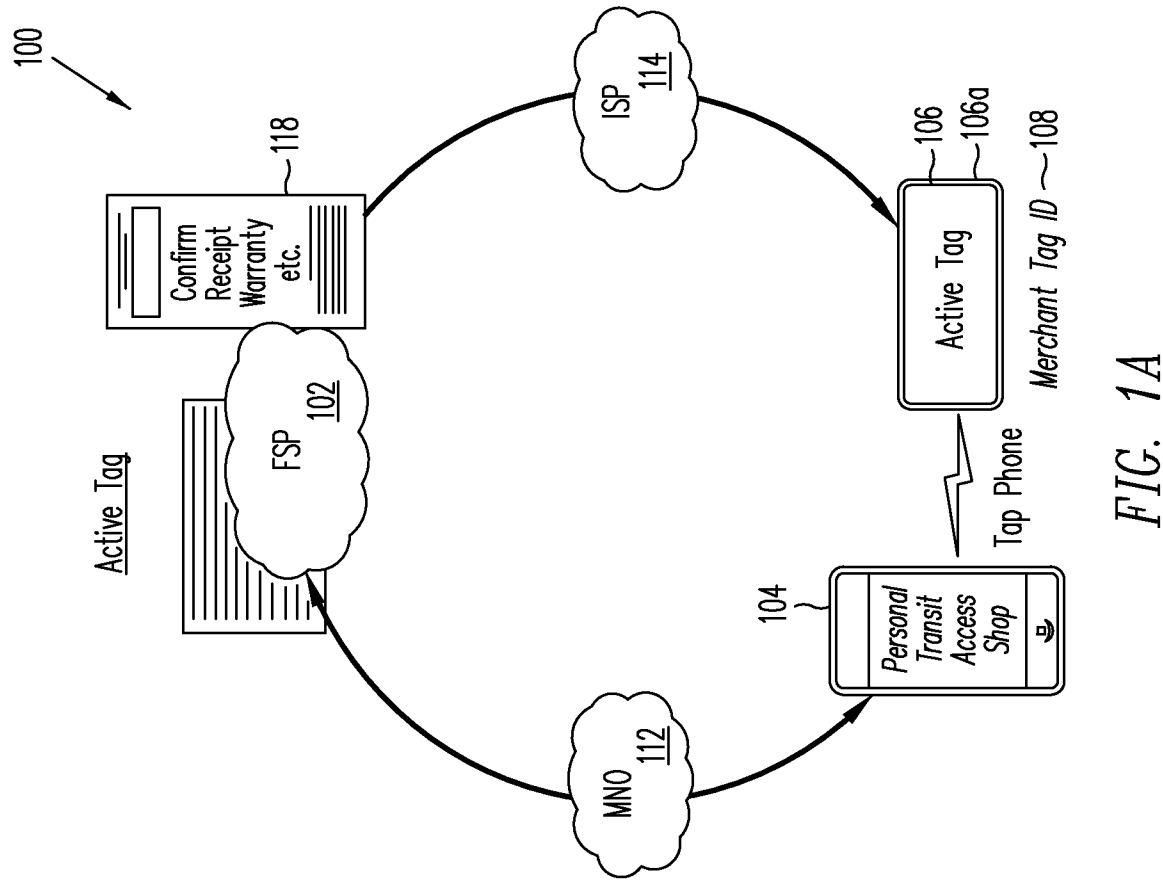

100
Active Tag
FSP 102
Confirm Receipt Warranty etc.
118
ISP 114
106
106a
Active Tag
Merchant Tag ID
108
Tap Phone
104
Personal Transit Access Shop
MNO 112

FIG. 1A

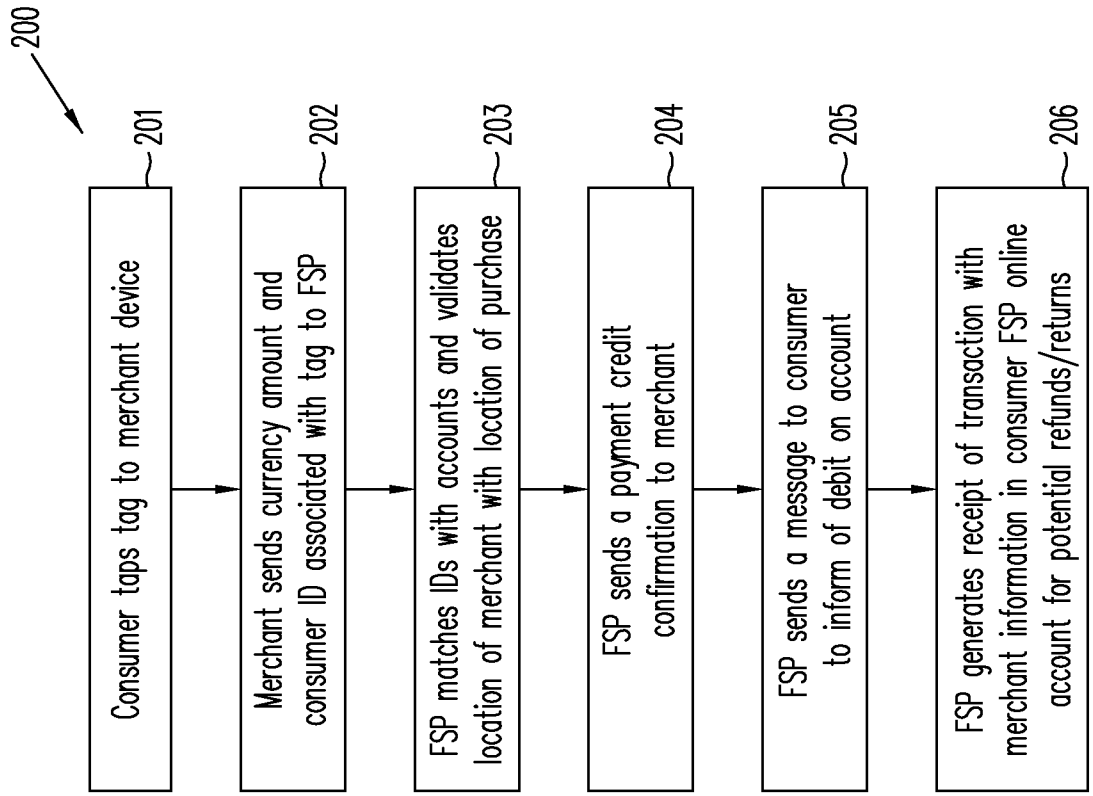

200
201
Consumer taps tag to merchant device
202
Merchant sends currency amount and consumer ID associated with tag to FSP
203
FSP matches IDs with accounts and validates location of merchant with location of purchase
204
FSP sends a payment credit confirmation to merchant
205
FSP sends a message to consumer to inform of debit on account
206
FSP generates receipt of transaction with merchant information in consumer FSP online account for potential refunds/returns

FIG. 2B

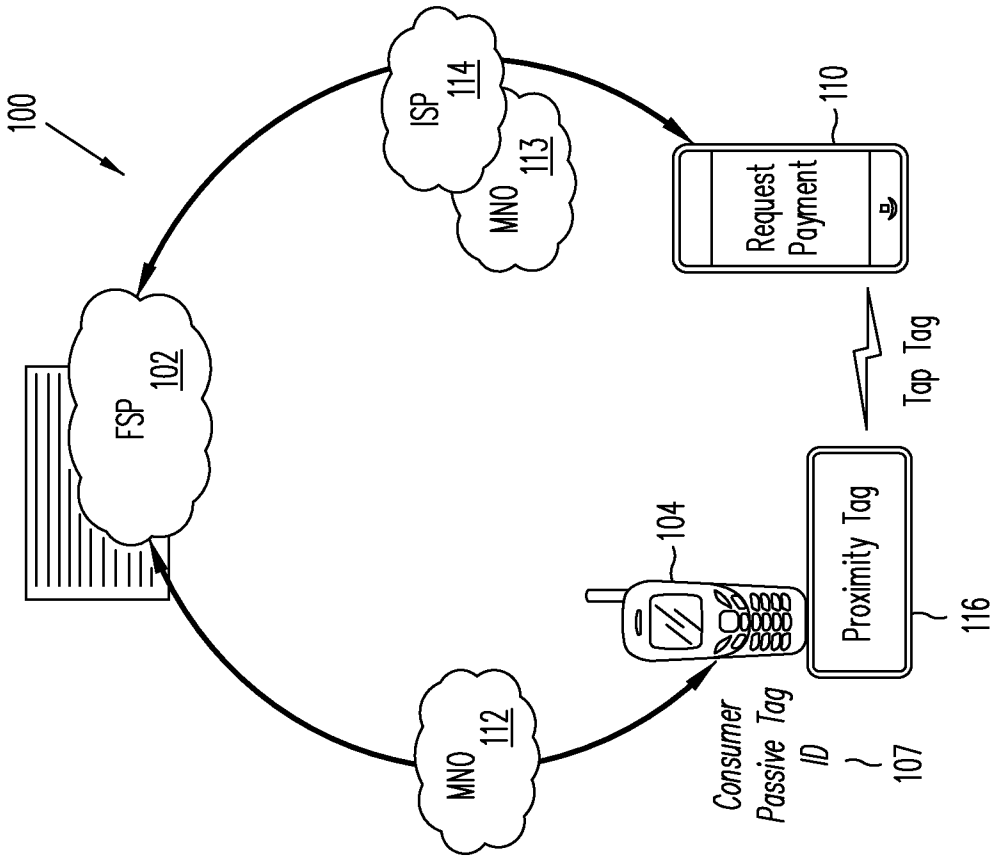

100
FSP 102
ISP 114
MNO 113
MNO 112
110
Request Payment
Tap Tag
104
Proximity Tag
116
Consumer Passive Tag ID
107

FIG. 2A

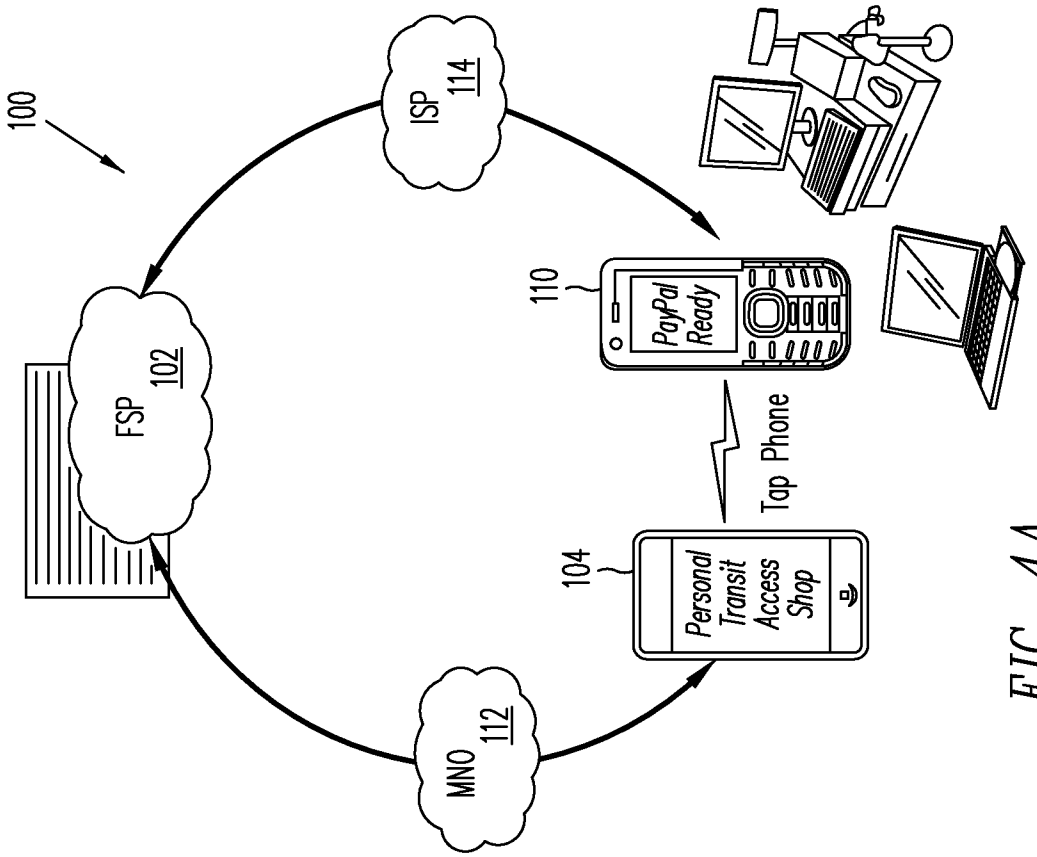

100
ISP 114
FSP 102
MNO 112
110
PayPal Ready
Tap Phone
104
Personal Transit Access Shop

FIG. 4A

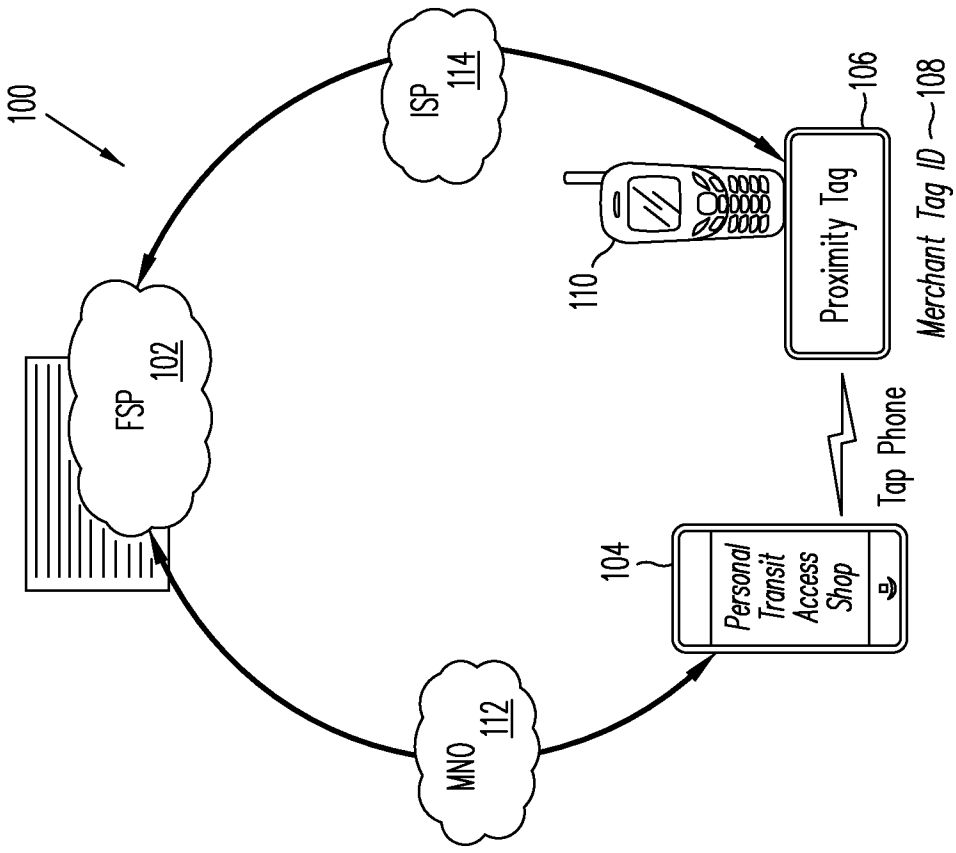

100
ISP 114
FSP 102
MNO 112
110
106
Proximity Tag
Merchant Tag ID 108
Tap Phone
104
Personal Transit Access Shop

FIG. 3A

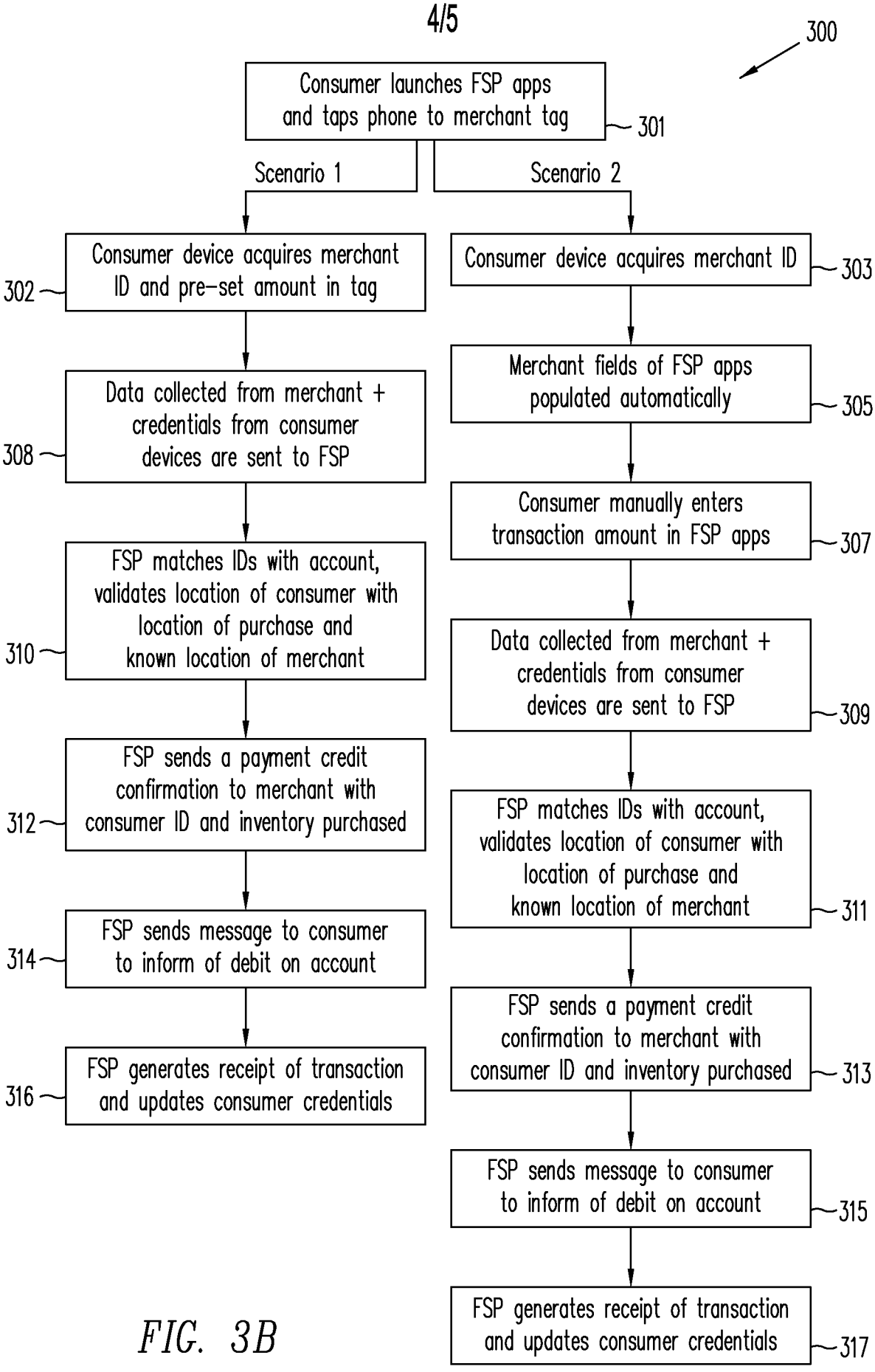

300
Consumer launches FSP apps and taps phone to merchant tag
301
Scenario 1
Scenario 2
Consumer device acquires merchant ID and pre-set amount in tag
302
Data collected from merchant + credentials from consumer devices are sent to FSP
308
FSP matches IDs with account, validates location of consumer with location of purchase and known location of merchant
310
FSP sends a payment credit confirmation to merchant with consumer ID and inventory purchased
312
FSP sends message to consumer to inform of debit on account
314
FSP generates receipt of transaction and updates consumer credentials
316
Consumer device acquires merchant ID
303
Merchant fields of FSP apps populated automatically
305
Consumer manually enters transaction amount in FSP apps
307
Data collected from merchant + credentials from consumer devices are sent to FSP
309
FSP matches IDs with account, validates location of consumer with location of purchase and known location of merchant
311
FSP sends a payment credit confirmation to merchant with consumer ID and inventory purchased
313
FSP sends message to consumer to inform of debit on account
315
FSP generates receipt of transaction and updates consumer credentials
317

*FIG. 3B*

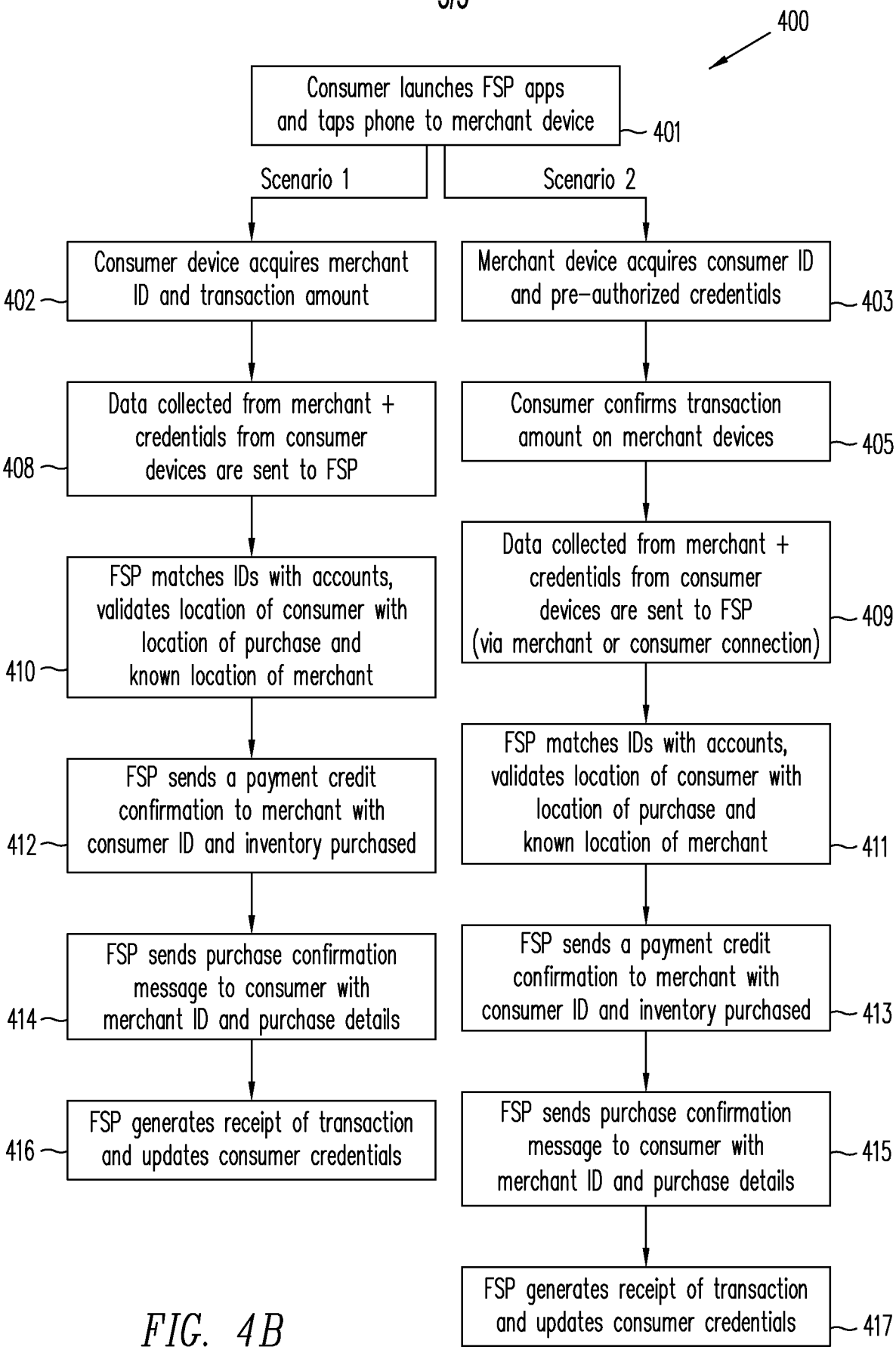

400
Consumer launches FSP apps and taps phone to merchant device
401
Scenario 1
Scenario 2
Consumer device acquires merchant ID and transaction amount
402
Merchant device acquires consumer ID and pre-authorized credentials
403
Data collected from merchant + credentials from consumer devices are sent to FSP
408
Consumer confirms transaction amount on merchant devices
405
FSP matches IDs with accounts, validates location of consumer with location of purchase and known location of merchant
410
Data collected from merchant + credentials from consumer devices are sent to FSP (via merchant or consumer connection)
409
FSP sends a payment credit confirmation to merchant with consumer ID and inventory purchased
412
FSP matches IDs with accounts, validates location of consumer with location of purchase and known location of merchant
411
FSP sends purchase confirmation message to consumer with merchant ID and purchase details
414
FSP sends a payment credit confirmation to merchant with consumer ID and inventory purchased
413
FSP generates receipt of transaction and updates consumer credentials
416
FSP sends purchase confirmation message to consumer with merchant ID and purchase details
415
FSP generates receipt of transaction and updates consumer credentials
417

*FIG. 4B*

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/033828

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/00 (2011.01)
USPC - 705/39
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 10/00, 40/00, 50/00 (2011.01)
USPC - 340/5.2, 5.7; 705/35, 39

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, Google Scholar

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2008/0238610 A1 (ROSENBERG) 02 October 2008 (02.10.2008) entire document | 1, 7-8 and 14-15 |
| Y | | 2-6, 9-13 and 16-20 |
| Y | US 2009/0228365 A1 (TOMCHEK et al) 10 September 2009 (10.09.2009) entire document | 2-6, 9-13 and 16-20 |
| A | WO 2009/097215 A1 (GRIFFIN et al) 06 August 2009 (06.08.2009) entire document | 1-20 |
| A | US 2007/0244811 A1 (TUMMINARO) 18 October 2007 (18.10.2007) entire document | 1-20 |

☐ Further documents are listed in the continuation of Box C. ☐

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

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 30 June 2011 | 12 JUL 2011 |

| Name and mailing address of the ISA/US | Authorized officer: |
|---|---|
| Mail Stop PCT, Attn: ISA/US, Commissioner for Patents<br>P.O. Box 1450, Alexandria, Virginia 22313-1450<br>Facsimile No. 571-273-3201 | Blaine R. Copenheaver<br>PCT Helpdesk: 571-272-4300<br>PCT OSP: 571-272-7774 |

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