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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 February 2017 (16.02.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/026887 A1

(51) International Patent Classification:
G06Q 20/32 (2012.01) *G06Q 20/40* (2012.01)

(21) International Application Number:
PCT/MY2015/050084

(22) International Filing Date:
12 August 2015 (12.08.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **VIGILANTECH PTE. LTD.** [—/SG]; 368 Thomson Road, #10-04, 368 Thomson, Singapore 298127 (SG).

(72) Inventor: **WEI, Meng Tan**; No. 30, Jalan Tengku Ampuan, Taman Duta, Kuala Lumpur 50480 (MY).

(74) Agent: **LOK, Choon Hong**; Pintas IP Group Sdn Bhd, No. 19, Jalan SS 1/36, Petaling Jaya, Selangor 47300 (MY).

(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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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))*

(54) Title: FRAUD PREVENTION SYSTEMS AND METHODS

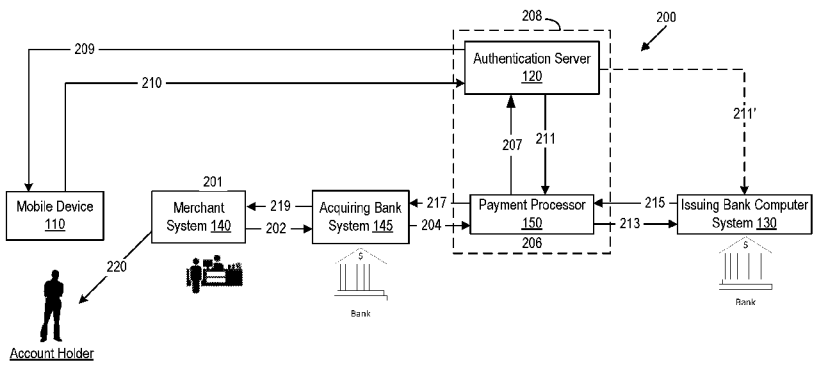

FIG. 2A

(57) Abstract: Systems or methods for authenticating transactions may include a server having a computer processor in communication with a non-transitory storage means, the authentication server configured to send an authentication notification to a mobile device, the server configured to preauthorize the mobile device to approve transactions related to at least one card of a card holder. The system may further include the server configured to approve the transaction after receiving an approval message from the mobile device and the server configured to reject the transaction upon receiving a rejection message from the mobile device or after failing to receive any message from the mobile device.

WO 2017/026887 A1

FRAUD PREVENTION SYSTEMS AND METHODS

BACKGROUND

[0001] Credit card payment methodologies are evolving to create a balance between security and convenience.Despite significant evolution, fraud is a major concern in the financial industry. Online credit card fraud continues to rise at a rapid pace. Despite significant investment and advances in the industry by all participants, fraud is still an increasing concern, driven by online transactions. Methods and systems thatare capable of further enhancing security, verify cardholder identification and deter fraud may be considered advantageous.

SUMMARY

[0002] Embodiments relate to a specifically programmed mobile device that links credit/debit cards with an account on an authorized phone that is used as a physical token. The credit/debit card is linked exclusively to the user's mobile device and/or a limited number of pre-authorized devices (2-3 devices). Every time a card transaction occurs, be it using a swipe and signature, contactless, chip and PIN, online or otherwise, a user must first authorize the transaction on the mobile device prior to thetransaction being successful. Accordingly, no unauthorized card transactions will be approved since no transaction would be processed without prior authorization from the respective user.Embodiments request transactions to be authorized by the user to mitigate fraud with virtually no friction.

[0003] In various embodiments, all transaction receipts and information will automatically be updated and stored in a transaction log on the mobile application servers or the mobile device for future reference. Embodiments may use the highest standard of cyber security and physical security as used in the financial industry (e.g. 128-bit SSL, SQL, etc.) on its mobile device, web servers and authentication servers.

[0004] Systems or methods for authenticating transactions may include an authentication server having a computer processor in communication with a non-transitory storage means, the authentication server configured to send an authentication notification to a mobile device, the authentication server configured to preauthorize the mobile device to approve transactions related to at least one card of a card holder. The system may further include the authentication

server configured to approve the transaction after receiving an approval message from the mobile device and the authentication server configured to reject the transaction upon receiving a rejection message from the mobile device or after failing to receive any message from the mobile device.

[0005] In various embodiments, a method for authenticating a transaction, the method may include sending, by an authentication server, an authentication notification to a mobile device, the mobile device configured to be preauthorized to approve transactions related to at least one card of a card holder. The method may include approving the transaction for at least one card, upon receiving an approval message from the mobile device. The method may further include rejecting the transaction for at least one card, upon receiving a rejection message from the mobile device.

[0006] Various embodiments include an apparatus for authenticating transactions, the apparatus includesa sending means for sending an authentication notification to a mobile device, and a preauthorizing means for preauthorizing the mobile device to approve transactions related to at least one card of a cardholder. The apparatus may include an approving means for approving the transaction forat least one card, upon receiving an approval message from the mobile device anda rejecting means for rejecting the transaction forat least one card, upon receiving a rejection message from the mobile device.

BRIEF DESCRIPTION OF THE FIGURES

[0007] The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features, aspects, and advantages of the disclosure will become apparent from the combination of the description, the drawings, and the claims in which:

[0008] Fig. 1is a schematic diagram of a computer-implemented transaction authentication system according to an embodiment;

[0009] Fig. 2A is an example authentication process implemented by the transaction authentication system of Fig. 1;

[0010] Fig. 2B is an example authentication process implemented by the transaction authentication system of Fig. 1; Fig. 3A is another authentication process implemented by the transaction authentication system of Fig. 1;

[0011] Fig. 3B is an example authentication process implemented by the transaction authentication system of Fig. 1;

[0012] Fig. 4A is another authentication process implemented by the transaction authentication system of Fig. 1;

[0013] Fig. 4B is another authentication process implemented by the transaction authentication system of Fig. 1;

[0014] Fig. 5 is another authentication process implemented by the transaction authentication system of Fig. 1;Fig. 6 is another authentication process implemented by the transaction authentication system of Fig. 1 to authenticate a transaction;

[0015] Fig. 7 is a screen shot prompting a user to provide an e-mail address and PIN to reset the password on an authentication mobile application implemented using the system of Fig. 1;

[0016] Fig. 8 is a screen shot of a device verification screen with a confirmation code that will be sent by the authentication server on an authentication application implemented using the system of Fig. 1;

[0017] Fig. 9 is a screen shot of a new password creation process as part of the registration display for an authentication application implemented using the system of Fig. 1;

[0018] Fig. 10 is a screen shot of a new PIN creation process as part of the registration display for an authentication application implemented using the system of Fig. 1;

[0019] Fig. 11 is a screen shot of a PIN confirmation display for an authentication application implemented using the system of Fig. 1;

[0020] Fig. 12 is a screen shot of a security question and answer as part of the registration display for an authentication application implemented using the system of Fig. 1;

[0021] Fig. 13 is a screen shot of a request for a confirmation code display that will be sent by the authentication server for an authentication application implemented using the system of Fig. 1;

[0022] Fig. 14 is a screen shot of a list of cards that are linked to the authentication account for an authentication application implemented using the system of Fig. 1;

[0023] Fig. 15 is a screen shot of a user editing or deleting the list of cards from Fig. 14 using the system of Fig. 1;

[0024] Fig. 16 is a screen shot of a user adding a new card to the authentication application using the system of Fig. 1;

[0025] Fig. 17 is a screen shot of a user entering a confirmation code received by a user from the authentication server of the authentication application using the system of Fig. 1;

[0026] Fig. 18 is a screen shot displaying transactions that may be cleared as shown in the display;

[0027] Fig. 19 is a screen shot of an authentication notification that may be displayed when the mobile device is locked in an example embodiment;

[0028] Fig. 20 is a screen shot of an authentication notification waiting for authorizationthat may be displayed when the mobile device is locked in another example embodiment;

[0029] Fig. 21 is a screen shot of an authentication notification that may be displayed when the mobile device is unlocked in an example embodiment;

[0030] Fig. 22 is a screen shot of an authentication notification waiting for authorizationthat may be displayed when the mobile device is unlocked in another example embodiment;

[0031] Fig. 23 is a screen shot of an authentication notification that may be displayed when the user of the mobile device fails to respond to the notification and subsequently opens the application or when the user has already opened the application according to an example embodiment;

[0032] Fig. 24 is a screen shot of an authentication notification when the user has selected “Accept” in Figs. 20, 22 or 23,according to an example embodiment;

[0033] Fig. 25 is a screen shot of an authentication notification when the user enters the correct PIN in Fig. 24; and

[0034] Fig. 26 is a screen shot of an authentication notification when the user has selected "Decline" and declines the transaction in Figs. 20, 22 or 23 according to an example embodiment.

DETAILED DESCRIPTION

[0035] The following business case shows an example of how the systems and methods described herein may be used. The systems that may be used for the applications described herein may include a central processor with multiple cores, RAM memory, non-transitory storage media, and/or remotely located non-transitory storage media.

[0036] Referring to Fig. 1, Fig. 1 is a schematic diagram of a computer-implemented transaction authentication system 100 according to an embodiment. The transaction authentication system 100 may include, among other systems, a mobile device 110, an authentication server 120, an issuing bank computer system 130, a merchant computer system 140, an acquiring bank computer system 145 and a payment processor 150. Each of the above systems may communicate with each other via a network 160. In various embodiments, the network 160 may include one or more of the Internet, Ethernet, cellular network, Wi-Fi, LTE, 4G, 3G, Wi-Max, a proprietary authentication network, a proprietary banking network, and so on. The authentication server 120, the issuing bank computer system 130, the merchant computer system 140, the acquiring bank computer system 145 and the payment processor 150 may each comprise a computer system (e.g., one or more servers each with one or more processors) configured to execute instructions, send and receive data, store in one or more non-transitory storage media or memory, and perform other operations to implement the operations described herein associated with processes and screenshots shown in Figs. 2 through 27.

[0037] The mobile device 110 may, for example be, a cellular phone, mobile handheld wireless device, smart phone, personal digital assistance, tablet computers, laptop computer, portable gaming device or other suitable devices. The mobile device 110 may include a processor in communication with one or more memory systems. The mobile device 110 may also include a wired or wireless transmitter and receiver. In various embodiments, an account holder may be in

possession of the mobile device 110 when conducting an in-person or card not present transaction (online, over the phone, etc.). In various embodiments, the mobile device 110 may be specifically configured to receive and sendone or more authentication messages from the authentication server 120 prior to the completion of a transaction via network interface logic 112.

[0038] The mobile device 110 may include a network interface logic 112, display device 113, input device 114 and card authenticator 115. The network interface logic 112 may include, for example, a wireless modem or a circuit that is configured to communicate acceptance or denial of a transaction by authentication messages. The display device 113 may be configured to display various output screens to the user and prompt the user for various input. In some embodiments, the display device 113 may also be an input device, such as a touch screen interface that allows a user to use a finger or a stylus to provide acceptance or denial for various card related transactions.In various embodiments, one account may include one or more cards associated with family member, for example, a card for the husband and another card for the wife. In such embodiments, more than one mobile device may be authorized to approve transactions for both cards. Accordingly, one or more mobile devices may be used in parallel to approve transactions.

[0039] In other embodiments, the mobile device 110 may be connected to another mobile device that cooperates with the mobile device 110 to provide the functionality described herein. For example, the other mobile device may be a watch or a small object with a small screen that the account holder can wear. In various embodiments, the other mobile device may be configured to communicate acceptance and rejection messages to the mobile device 110 and in turn the mobile device 110 may communicate the messages to the authentication server 120.

[0040] The card authenticator 115 may configure the mobile device 110 to be linked to one or more credit or debit cards that belong to the account holder. In various embodiments, linking may comprise the card authenticator sending mobile device identification information to the authentication server and linking the mobile device identification information to one or more credit cards that are input into the card authenticator 115 by the account holder or user of the mobile device 110. In various embodiments, the mobile device 110 may download one or more applications that may perform the card authenticator 115 functions. In other embodiments, the

card authenticator 115 may be a circuit that is integrated into the mobile device 110 by the manufacturer of the mobile device 110. The card authenticator 115 may be configured to receive and send authentication messages from the issuing bank computer system 130, the authentication server 120 or payment processor 150.

[0041] The authentication server 120 may be a computer system that includes one or more processors that is configured to store data on one or more non-transitory storage media. The authentication server 120 may be in communication with the payment processor 150 or issuing bank computer system 130 or various other computers in system 100 by using the network interface logic 123. The authentication server 120 may include, a mobile device registration system 122, a network interface logic 123, an account directory 124, an authentication sending means 125, a rejecting means 126, and an approving means 127. In various embodiments, the authentication server 120 may be the gateway between the funds being transferred from the account holder to the recipient/merchant when there are sufficient funds and the card is valid. In other embodiments, the authentication server 120 is required to send an approval signal for the transaction to be completed. Such functionality provides the account holder with further security that even when the account holders credit card, debit card, PIN is compromised, the fraudster is unable to complete the transaction without the authentication server 120 sending an approval for the transaction.

[0042] The account directory 124 may be configured to store one or more card numbers (credit, debit or otherwise) in correlation with one or more mobile devices 110. In some embodiments, upon receiving card information from a payment processor 150 or an acquiring bank computer system 145, the account directory 124 may identify mobile phone number or mobile phone identification information (UDID or IMEI or ECID) to request approval for the transaction from the account holder. Each of the above mobile phone identification information may be stored in the account information directory 124 and accessed to verify that correct mobile device 110 is responding to the authentication request.

[0043] The authentication sending means 125 may be a computer system with a processor that is configuredto send and receive an authentication message to or fromthe mobile device 110 that is linked to the card that is used for the transaction. The authentication sending means 125 may

receive the mobile device from the account directory 124. The rejection means and the accepting means may be computer systemsthat have a processor and a storage media.

[0044] The issuing bank computer system 130 may include a network interface logic 136, account processor 132 and an account database 134. The network interface logic 136 may be configured topermit the issuing bank computer system 130 to communicate with various other systems in the transaction authentication system 100. The acquiring bank computer system 145 may include similar systems as issuing bank computer system 130. For example, the acquiring bank computer system 145 may have a network interface logic, account processor and account database. In various embodiments, the issuing bank computer system 130 may only release funds after receiving approval from the user, the authentication system 120 or the payment processor 150, or any or a combination of any one or some of the above systems.

[0045] The merchant computer system 140 may include a card scanner 142 and a network interface logic 144. The card scanner 142 may be a physical card scanner located at a brick and mortar store or in other embodiments the card scanner may be an online store that receives the card number and card identification number. Upon receiving the card information from an account holder, the merchant computer system 140 may use the network interface logic 144 to communicate the card information to the acquiring bank computer system 145. Next, the acquiring bank computer system 145 may contact the payment processor 150 for payment. In some embodiments, the payment processor 150 may contact the authentication server 120 for approval of the transaction.

[0046] The payment processor 150 may include a network interface logic, account processor and account database. Examples of payment processor 150 may include Visa®, Mastercard ®, or American Express ®. In various embodiments, the payment processor 150 may seek approval of the authentication server 120 prior to approving the transaction.

[0047] Referring to Fig. 2A, Fig. 2A is an example authentication process 200 implemented by the transaction authentication system of Fig. 1.At step 201, the account holder may use his/her card at the POS (or online transaction, over the phone or any card not present transaction) at the merchant system 140.Next at step 201, the merchant system 140 then processes the card and at step 202 the transaction information is sent to the merchant's acquiring bank 145, which then

uses a payment processor 150 to contact the issuing bank 130 for authorization, at step 204. However, before the issuing bank is contacted, the transaction authorization maybe sent to the authentication server 120, at step 207, which will then contact the respective card user's mobile device 110 at step 209 for authorization via an authorization notification. At step 206, the payment processor 150 may identify the issuing bank computer system 130 that should be contacted and the identity of the authentication server 120 to be contacted. At the time of registration of the mobile device 110 and the linking of the card with the authentication server 120, the authentication server 120 may inform the payment processor 150 that each transaction related to the card requires an authentication request to be sent to the authentication server 120. Once authorized on the user's mobile device 110, the information will be relayed back to the authentication server 120 at step 210 and back to the payment processor 150 at step 211. In some embodiments, the authentication message may also be sent to the issuing bank computer system at step 211'. In various embodiments, steps 211 and 211' may occur in parallel to step 213. In other embodiments, either step 211 occurs or step 211' occurs. After the payment processor 150 determines that the mobile device 110 has approved (or sent a signal to approve) the transaction the payment processor 150 informs the issuing bank computer system 130 at step 213. After the issuing bank computer system 130 receives the approval the issuing bank verifies the card information. The issuing bank computer system 130 then internally evaluates the request and sends an approval to the payment processor at step 215. Next, at step 217 the payment processor 150 may inform the acquiring bank that the transaction has been approved and the acquiring bank may inform the POS merchant system 140 to finish the transaction with the account holder by generating a receipt for the account holder at step 220. As shown in Fig. 2A by integrated system 208, the authentication system 120 may be integrated into the payment processor 150. In other embodiments, the authentication system 120 and the payment processor 150 may be owned by the same entity or may be implemented in a single server.

[0048] In various embodiments, the transaction will not be processed if the mobile device 110 does not provide an approval. Accordingly, in various embodiments, the transaction is processed only after receiving approval from the account holder.Various exceptions discussed in greater detail below may be included, such as but not limited to, when the mobile device fails to respond or the mobile device does not have a connection to a network. Other exceptions to requiring

approval may include when the authentication server 120 fails to receive a read receipt from the mobile device. In various embodiments, these exceptions may have limits on the total transactions amounts that are approved, value of each single transaction or the total number of transactions that are permitted.

[0049] Referring to Fig. 2B, Fig. 2B illustrates a process 250 that is similar to the process shown in Fig. 2A with some changes. The steps of Fig. 2B are similar to the steps in Fig. 2A. However, as shown in the process 250, the issuing bank computer system 130 may incorporate the functionality of the authentication server 120. In various embodiments, the issuing bank computer system 130 and authentication system 120 may be owned by the same entity.Accordingly, the authentication request 207 and the permission for approval 215 will be sent to the issuing bank computer system 130 that incorporates the authentication server 120.

[0050] Fig. 3A is another authentication process 300 implemented by the transaction authentication system of Fig. 1. The embodiments shown in Fig. 3Aare similar to Fig. 2Aexcept that the payment processor 150 will first contact the issuing bank computer system 130 for approval of the transaction at step 307. In particular, various steps from Fig. 3A are similar to the steps described in Fig. 2A the steps that differ are described in greater detail below. For example, in various embodiments, step 201 from Fig. 2A is similar to step 301 of Fig. 2A, step 202 is similar to step 302, step 204 is similar to step 304, step 306 is similar to step 206, step 307 is similar to step 207, step 309 is similar to step 207 except it is generated from the issuing bank computer system 130, step 313 is similar to step 211, step 313' is similar to step 211', step 311 is similar to step 209, step 312 is similar to step 210, step 308 is similar to step 215, step 315 is similar step 217, step 317 is similar step 219 and step 319 is similar step 220.

[0051] At step 308 the issuing bank computer system 130 may transmit an approval message to the payment processor 150 based on the approval criteria related to the sufficiency of funds, and the validity of the cards. Once the issuing bank computer system 130 has approved the transaction the information will be sent to the authentication server 120 at step 309. The authentication server 120 will send an authorization notification to the mobile device 110 at step 311. Once the account holder has authorized the transaction on his/her mobile device 110, that information will be sent back to the authentication server 120 at step 312. Next at step 313 the

authentication server 120 may use the payment processor 150 to inform the acquiring bank at step 315 that the transaction has been approved by the issuing bank and the authentication server 120 bythe account holder. In an alternative embodiment, at step 313' the authentication server 120 may send the approval directly to the issuing bank computer system 130. In yet another embodiment, the system 310 may include the functionality of both the authentication server 120 and the issuing bank computer system 130. In yet another embodiment, the issuing bank computer system 130 may implement the functionality described herein from authentication server 120. The acquiring bank 145 will send a message to the merchant system 140 that the transaction has beenapproved at step 317. This is an alternative to the process shown in Fig. 2A.Receiving authorization for card transaction via a mobile device 110 prior to approval of the transaction is similar to both Figs. 2A and 3A.

[0052] In an alternative embodiment, the issuing bank computer system 130 may request the user authorization directly through the cardholder's mobile device 110. In other embodiments, the issuing bank computer system 130 may incorporate the full functionalities described herein of the authentication server 120 and directly contact the mobile device 110 for authentication prior to approving a transaction. This embodiment may be implemented for each of the processes described in Figs. 2-6.

[0053] Referring to Fig. 3B, Fig. 3B illustrates a process 350 that is similar to the process shown in Fig. 3A with some changes. The steps of Fig. 3B are similar to the steps in Fig. 3A. However, as shown in the process 350, the payment processor 150 may incorporate the functionality of the authentication server 120. In various embodiments, the payment processor 150 and authentication system 120 may be owned by the same entity as shown by system 310.

[0054] Referring to Fig. 4A, Fig. 4A is another authentication process 400 implemented by the transaction authentication system 100 of Fig. 1. Other embodiments may include multiple issuing banks 130, 130', 130'' configured to communicate directly with the authentication server 120 so that user interface for the user is exactly the same for approving or rejecting the transaction. The process in Fig. 4A is similar to the process in Fig. 2A except, steps 409 and 412 are being performed by the issuing bank computer system 130 instead of the payment processor 150. Other steps 402-407 and 411, 413-420 are similar to the steps 202-207 and 211, 213-220

from Fig. 2A. As shown in Fig. 4A in block 410, the authentication server 120 and the payment processor 150 may be owned by a single entity or may operate on the same server system. In other embodiments, the payment processor 150 incorporates the functionality of the authentication server 120.

[0055] Referring to Fig. 4B, Fig. 4B is another authentication process 450 implemented by the transaction authentication system 100 of Fig. 1. The steps of Fig. 4B are similar to the steps in Fig. 4A. However, as shown in the process 450, the issuing bank computer system 130 may incorporate the functionality of the authentication server 120. In various embodiments, the issuing bank computer system 130 and authentication system 120 may be owned by the same entity as shown by system 410'. As shown in Fig. 4B, system 410' may be distributedly implemented or singularly implemented. For example, each issuing bank computer system 130, 130' and 130" may include an authentication server 120 within their own bank computer system. Additionally or alternatively, each issuing bank computer system 130, 130', or 130" may access a third party provided authentication server 120.

[0056] Payment processor 150 and/or issuing banks flow may also include additional steps described below. An account holder may register himself/herself on the respective issuing bank's application on the smartphone, tablet, etc. The authentication application could be issued by the payment processor 150 or the issuing bank 130. Additionally the issuing bank can integrate the authentication software, methodology and platform into their existing banking application that could be already linked to their cards.

[0057] Account holder may register and links his/her credit/debit card on the issuing bank's application under their respective account – this is accomplished by entering the card information and going through the issuing bank 130 security protocols such as answering security questions, unique IDs, physical one time codes sent by post or SMS codes sent by the issuing bank. Additionally or alternatively, the debit/credit cards will be linked to the mobile device or the application and recognize the device (mobile/tablet/etc.) as an authorized device.

[0058] In other embodiments, the issuing bank's application can also authorize other devices as an authorized device for the authorization process on the application up to a certain fixed number of devices.Only devices that have been recognized and authorized will be able to approve or

deny a transaction authorization process. Once the credit/debit card has been linked to the issuing bank's mobile application, the user can begin the authorization process when they use their cards or a card present or card not present transaction.

[0059] When a transaction is processed using the user's credit/debit card, the merchant/vendor will process the card through a POS (Point of Sale) terminal (either online, physical, over the phone, etc.).

[0060] The POS or merchant system 140 may transfer the card information to the merchant's acquiring bank 145 at step 402, which will in turn use a payment processor's network 150 (MasterCard, Visa, Amex, Union Pay, JCB, etc.) to connect to the issuing bank at step 407.

[0061] In some embodiments, once the request for authorization reaches the issuing bank computer system 130, the issuing bank computer system 130 will submit a notification to the respective card owner's application account to request for authorization either through their own bank application platform or through the authentication server 120. Note that the request for authorization is completed before a transaction can occur. If the authorization on the application is rejected by the user, the payment will not be processed and the vendor will need to request an alternative mode of payment from the account holder.The authorization process on the application should be similar or exactly the same as what the authentication server is proposing to its users (see wire frames below).

[0062] In some embodiments, once the authorization has been approved on the application by the user, the information will be sent back to the issuing bank which will then use the network processor to let the acquiring bank know that the transaction has been approved. Once the acquiring bank has the confirmation, the vendor/merchant can process the transaction and a receipt will be provided to the user. In other embodiments, the application will save the list of historical transactions on the application and/or the linked device.

[0063] Referring to Fig. 5, Fig. 5 is another authentication process implemented by the transaction authentication system of Fig. 1. The authentication process shown in Fig. 5 is one where the issuing bank computer system 130 and the payment processor 150 are the same entity. An example of this type of entity is American Express ® or Discover Card ®. At step 501, the account holder presents a card to a merchant system 140. Next at step 502 the merchant system

140 transmits the card information to the acquiring bank system 145. The acquiring bank determines that the issuing bank computer system 130 and the payment processor 150 are the same entity and at step 503 sends the transaction amount, merchant information, and card number to the issuing bank system 130 and payment processor 150. Next at step 504, the issuing bank 130 and the payment processor 150 requests the authentication server 120 to get an approval from the mobile device 110. The authentication server 120 determines, at step 505, based on the card information received in step 504, the identity of the mobile device 110 that is tied or linked to the card that the account holder presented. At step 507, the authentication notification is sent to the mobile device 110 and by receiving user input the transaction is approved or denied at step 509. After receiving an approval the authentication server 120 sends the approval to the issuing bank computer system 130 and the payment processor 150. Next the message of approval is transmitted at step 512 and 513 such that the merchant system 140 generates a receipt for the account holder 515 and the transaction is completed after the account holder has independently approved the transaction with their mobile device 110.

[0064] In some embodiments, as shown in block 508 the acquiring bank system 145, issuing bank computer 130 and payment processor 150 may each be owned by a single entity or be part of the same computer system. In other embodiments, if the acquiring bank system 145 is combined with the payment processor 150 and the issuing bank computer system 130, the authentication server 120 could be reached after attempting the transaction by the acquiring bank system 145. Next, the mobile device 110 may be asked for an approval. The authentication server 120 may be configured to receive the approval and send the approval back to the acquiring bank 145 or the issuing bank computer system 130 and payment processor 150. In various embodiments, similar messages may be transmitted among systems.

[0065] Fig. 6 is another authentication process implemented by the transaction authentication system of Fig. 1 to authenticate a transaction. At step 601 the process begins by the account holder providing card information (magstrip or online vendor or any card not present situations) to a merchant. At step 603, the merchant computer system 140 may receive the card information via the card reader or via the user entering it in online (or any card not present situation). At step 603 the acquiring bank computer system 145may receive the transaction information from the merchant computer system 140. Next at step 607 the payment processor receives transaction

information from the acquiring bank. After receiving the transaction information, the payment processor computer may send the authorization request to the authentication server 120, at step 609. At step 611, the authentication server may send an authentication notification to the preauthorized one or more mobile devices. The process ends at step 613 when the user of the mobile device 110 rejects the transaction.

[0066] If the user approves the transaction at step 611 the mobile application opens with a request for a PIN for the device or other options to approve certain transactions below a certain threshold amount such as swiping a notification or clicking "Accept" on the notification. At step 615 the user enters a PIN. Next at step 617, the application on the mobile device 110 stores the information regarding the transaction. Next at step 619, an authorization is sent to the issuing bank via the payment processor by the authentication server. In yet another embodiment, the authorization notification may be sent to the issuing bank directly without using the payment processor. At step 621, the issuing bank computer system may approve the transaction and transmit the approval to the payment processor. In other embodiments, the issuing bank computer system 130 will receive request for the transaction first and approve it before sending it to the authentication server to send the approval to the mobile phone for approval. Next at step 623, the acquiring bank computer system 100 may receive an approval from the payment processor. At step 625 the merchant may receive an approval and at step 627 the receipt for the transaction may be printed.Various options for approval may include, swiping without a PIN, biometrics, voice recognition, facial recognition, etc.

[0067] Fig. 7 is a screen shot prompting a user to provide e-mail address and PIN to reset the password on an authentication mobile application implemented using the system of Fig. 1. Display 700 may be shown to a user attempting to reset their password when the user forgot their password. Display 700 includes a text field 702, a PIN field 704 and create new password button 706. If the e-mail in the text field and the PIN in the PIN field 704 do not match then the display 700 may display a message informing the user that the e-mail and PIN do not match and the user should please try again. After entering the e-mail and PIN correctly the user may select the create a new password button to create a new password or reset their password.

[0068] Fig. 8 is a screen shot of a device verification screen on an authentication application implemented using the system of Fig. 1. Fig. 8 illustrates the device verification screen 800. The device verification screen 800 may be displayed when the user is attempting to register their device or link their mobile device 110 with a card or register their application. In some embodiments, the device verification screen 800 includes a confirmation code entry field 804. The user may enter the confirmation code that they received from the payment processor or the issuing bank either in the form of an email, physical mail, SMS or any other form of communication in order to link or verify that the device is the account holder's device. The screen 800 also provides a checkbox 806 to allow the account holder to inform the application to remember this device and a verify device button 808.

[0069] Fig. 9 is a screen shot of a registration display 900 for an authentication application implemented using the system of Fig. 1. The registration display 900 has an e-mail field 902, password 904, confirm password 906 and continue button 908.

[0070] Fig. 10 is a screen shot of a registration display 1000 for an authentication application implemented using the system of Fig. 1. The registration display 1000 provides the user with the option to enter a PIN (1002) at the time of registration.

[0071] Fig. 11 is a screen shot of a PIN confirmation display 1100 for an authentication application implemented using the system of Fig. 1.The registration display 1100 provides the user with the option to confirm their PIN (1102) at the time of registration. The registration process links the registered one or more mobile devices to the authentication server for one or more cards.

[0072] Fig. 12 is a screen shot of a security question display 1200 for an authentication application implemented using the system of Fig. 1. The security question display 1200 may include a pull down menu 1202 that includes a plurality of security questions that the user may select. The security question display 1200 also includes an answer text field 1204 where the user may enter an answer and upon receiving the answer the answer is stored on the authentication server. The security question display 1200 includes a phone number text field 1206. Upon the user selecting the verify phone number button 1208. The mobile device 110 may send a message

to the authentication server 120 and in response the authentication server may send a confirmation code via a text, or e-mail to the mobile device 110.

[0073] Fig. 13 is a screen shot of a request for a confirmation code display 1300 for an authentication application implemented using the system of Fig. 1. For display 1300 the mobile device 110 is sent a confirmation code by the authentication server 120 to enter into field 1302. Item 1304 informs the user that this mobile device 110 will be saved as a verified device. In some embodiments, when the mobile device 110 is verified after the user hits the verify button 1308. Once the mobile device 110 has been verified it is linked to the authentication server 120.In various embodiments, the mobile device 110 may be linked to one or more cards and to one or more authentication servers. When the user first registers the account on the mobile device, the user will enter their phone number. Once the verified phone number button is clicked the next slide appears requesting for the confirmation code which will be sent to the phone number via SMS. Once the right confirmation code has been entered and the verify button has been clicked, the application should automatically remember the device and the application will say "This device will be saved as a verified device".

[0074] More specifically once the confirmation code has been verified, only the remembered device can authorize transactions. This is the case where the account, phone, cards linked and PIN are all in sync.

[0075] In an alternative embodiment, the application will allow the user to remember 2-3 devices and will provide a separate option page to add devices to the user's account in the app. As a result, if the user tries to log into the application on his/her account on another phone, it will not be allowed to log in unless it is a remembered device. Additionally, the authorization notifications will not be sent to a new device that has not been verified or remembered. The authenticated smartphone with the account will act as a physical token for authorization purposes. If the user loses his or her phone, the user may log into the authentication server 120 website online and remove the lost device as a remembered device for the account. This will open up a vacancy in the application to allow a new smartphone or device to be a remembered device that is linked to the account.

[0076] The authentication application will be inherently linked to the smartphone through either a web thumbprint from the phone if it is using web technology or native iOS, Android, Windows or Blackberry code or any other native OS. Every smartphone has a unique UDID or IMEI number that the application can use to identify the phone. The application will pull the information from the phone and detect the UDID or IMEI number to authorize and remember the phone. If the user tries to log on into his/her account on another unauthorized device/smartphone, the application will detect this and raise a flag and not grant access to the account. Additionally, the user will be able to authorize other devices to access the account and receive authorization notifications. This can be done by receiving a confirmation code notification on the main device which the user will use to enter into the application on the new device when prompted to do so. Basically, the user must have the main device present and log in before he/she can authorize another device. The application should recognize the phone by its unique ID rather than its phone number that the phone currently has. This means that if another SIM is used on the same phone the application should not know the difference and should work with that phone regardless.

[0077] Alternatively, if another SIM is used a further authentication process may take place based on the user's profiled settings. For example, the user may let the application know that the user intends to travel overseas and will be using a different SIM.In terms of security the industry standards will be used such as,but not limited to, SSL Certificates for the app, SSH for remote server access and SQL injections using Laravel query builder with PDO parameter binding throughout to protect the application against SQL injection attacks.

[0078] Fig. 14 is a screen shot of a list of cards that are linked to the authentication server for an authentication application implemented using the system of Fig. 1. Fig. 14 shows a display of cards 1400 that are linked to the mobile device displaying the list of cards. For example, display 1400 shows visa card 1402, master card 1404 and discover 1406. To generate the display shown in 1400 a user may select the"My Cards" button 1408.

[0079] Fig. 15 is a screen shot of a user editing the list of cards 1500 from Fig. 14 using the system of Fig. 1. Editing list of card screen 1500 may be generated when the user selects the edit button from Fig. 14. As shown in display 1500 the user may select the delete button to remove

cards from being linked to mobile device 110. When the user selects the delete button 1508, the discover card 1506 may be unlinked from the mobile device 110.

[0080] Fig. 16 is a screen shot of a user adding a new card to the authentication application using the system of Fig. 1. Adding a new card screen 1600 may display a card nickname text field 1602, a card number text field 1604 and a add button 1606. Fig. 17 is a screen shot of a user entering a confirmation code received by a user of the authentication application using the system of Fig. 1. Fig. 17 allows the user to enter a add card security code in field 1702. User may select the verify button 1706 to verify the confirmation code. The confirmation code may be sent to the user via SMS,e-mail or physical mail.

[0081] Fig. 18 is a screen shot displaying transactions that may be cleared as shown in the display. The transaction display 1800 may show various historical transactions. The transaction display 1800 also displays transactions that were declined as shown in line 1808. In various embodiments, the declined transactions may be shown in different colors. The user can select specific transactions and choose to press the clear button and the mobile device 110 may ask the user whether the user is sure that the transactions selectedshould be deleted. Alternatively, the user can select to clear all the transactions.

[0082] Fig. 19 is a screen shot of an authentication notification that may be displayed when the mobile device is locked in an example embodiment. The display 1900 in Fig. 19 shows a notification alert 1902 regarding a transaction that needs to be authenticated. The authentication message 1902 may include the name of the store and the amount of the transaction.

[0083] In various embodiments, the user may provide input by slide to the right 1906 to open the authentication application. In other embodiment, sliding to the left may open a blue to approve or red to decline button while the mobile device 110 remains in a locked state. Accordingly, in various embodiments, transactions may be approved without the user having to unlock the mobile device 110.

[0084] Fig. 20 is a screen shot of an authentication notification that may be displayed when the mobile device 110 is in a locked state.Display 2000 may be generated in response to a user selecting 1904 in Fig. 19. If the user selects the accept button 2002, then the transaction is either authenticated by the mobile device 110 or will open the application in the mobile device to enter

a PIN or alternatives(See. Fig. 24). The actions followed by selecting the accept button 2002 will depend on a set transaction amount. Once the authorization from the user is completed,the mobile device 110 sends an approval message to the authentication server. If the user selects the decline button 2006, then the decline message is sent to the authentication server or/and a declined page (See. Fig. 26) can be opened in the mobile application. The choice is regarding transaction 2004.

[0085] Fig. 21 is a screen shot of an authentication notification that may be displayed when the mobile device is unlocked in an example embodiment.Fig. 21 shows a display 2100 where the authentication message 2102 is displayed at the top of the mobile device screen. The authentication message 2102 may include the name of the store and the amount of the transaction.

[0086] Fig. 22 is a screen shot of an authentication notification that may be displayed when the mobile device is unlocked in another example embodiment. In the embodiment shown in screen 2200, the user pulled down on the notification that was received in Fig. 21. The authentication application displays the message 2202, the accept button 2204 and decline button 2206. By clicking on the "Accept" button the application may display the PIN entry page Fig. 24 (other forms of user authentication may be used as well) and by clicking the "Decline" button it will bring the user to the decline page (See. Fig. 26).

[0087] Fig. 23 is a screen shot 2300 of an authentication notification that may be displayed when the user of the mobile device fails to respond to the notification according to an example embodiment. If the user fails to respond to any of the above notifications, the authentication application may be initiated and the application may display the accept button 2302, decline button 2304, the details regarding the transaction 2306 and request a PIN 2308 from the user. By clicking on the "Accept" button the application may display the PIN entry page Fig. 24 (other forms of user authentication may be used as well) and by clicking the "Decline" button it will bring the user to the decline page (See. Fig. 26).

[0088] Fig. 24 is a screen shot of an authentication notification when the user has selected accept in Fig. 23 according to an example embodiment. As shown in Fig. 24, after the user selects the accept button 2404, the user has the opportunity to enter the PIN 2408. By clicking on the

"Accept" button the application may display the PIN entry page Fig. 24 (other forms of user authentication may be used as well) and by clicking the "Decline" button it will bring the user to the decline page (See. Fig. 26).

[0089] Fig. 25 is a screen shot of an authentication notification when the user enters the correct PIN in Fig. 24. Upon receiving the correct PIN the screen display 2500 may be generated. Screen display 2500 shows a charge accepted button 2504 to inform the user that the charge has been accepted and the transaction should be completed.Once this happens, the transaction log in Fig. 18 is updated with the transaction information. In some embodiments, by clicking on the "Accept" button the application may display the PIN entry page Fig. 24 (other forms of user authentication may be used as well) and by clicking the "Decline" button it will bring the user to the decline page (See. Fig. 26).

[0090] Fig. 26 is a screen shot of an authentication notification when the user declines the transaction according to an example embodiment. In the embodiments where the charge is declined, screen 2600 is displayed. For example, a charged declined message 2604 is shown. Also shown the report fraud button 2608 and the call the issuing bank button 2605. Selecting any of 2605 and 2608 may allow the user to reach the issuing bank to cancel the compromised card.The transaction log from Fig. 18 is also updated with the declined transaction information.

[0091] In other embodiments, for card present transactions if the mobile phone is unavailable or there is no data connection, the authentication server 120 will attempt to contact the respective account holder preauthorized mobile phone 110 for authorization and fail. The authentication server's 120 realization of the failed receipt of the authorization notification is acknowledge by a received confirmation.Upon failure the authentication server 120 will allow the transaction to be approved but the authentication server 120 is configured to request for the transaction or transactions be approved by the user when the mobile device 110 regains connection to the authentication server 120 on the user's phone. If the transactions are not approved by the user within a certain period of time (e.g., 4 hours, 10 hours, 12 hours, or 24 hours), the card will be frozen and the user will have to contact the bank via a telephone to verify the situation with their card. If the user's authentication account on his or her phone is reachable and a fraudulent attempt is made, he/she will know in advance before the transaction occurs as a notification

authorization will be sent to the phone. Moreover, if a notification authorization is sent to the user's phone and received, the transaction will not be processed unless the transaction is approved by the user. For Online transactions, the mobile device is usually reachable or similar temporarily approvals may be granted and will always need an authorization from the user in order to process a transaction.

[0092] In regards to the idea for the authorization for physical transactions when there is no mobile coverageor no phone battery (basically when the mobile device 110 cannot be reached), the authentication server may include a read receipt function in the patent. This highlights that if the authentication server 120 does not receive a read receipt from the user for the authorization, the authentication server 120 will notify the issuing bank or payment network processor (in a closed loop network) that an authorization from the user has not been received and to process the transaction regardless. The user will then need to authorize the transaction within a certain period of time (e.g., 4 hours, 10 hours, 12 hours, or 24 hours) or their card will be blocked. Various exceptions to requiring an approval from the mobile device 110 may include when the mobile device fails to respond or the mobile device does not have a connection to a network. Other exceptions to requiring approval may include when the authentication server 120 fails to receive a read receipt from the mobile device. In various embodiments, these exceptions may have limits on the total transactions amounts that are approved, value of each single transaction or the total number of transactions that are permitted.

[0093] In various embodiments, the authentication server 120 may be configured to request the battery levels of each mobile device 110. Additionally or alternatively, the card authenticator115may be configured to track the battery levels of the mobile device 110 and upon reaching a threshold amount of battery level (e.g., 3, 4, 5, 10, or 15 percent remaining) may alert the authentication server 120 that the mobile device 110 is about to lose power. In other embodiments, the card authenticator 115 may determine that the power is about to be depleted and present the user with various options for when the power is lost. Accordingly, while the user has power and is aware of their activities for the next few hours, the user may decide what type of transactions may be processed in the next few hours while the battery runs out. For example, if the user knows that they are not going to conduct a transaction over $100, then the user may set that as a threshold amount for automatically rejecting all purchases over the threshold

amount, until the mobile device 110 regains power. Accordingly, after receiving the user's input the mobile device 110 may send a message to the card authentication sever 120 to automatically reject transactions over the threshold amount until the card authentication 115 goes above a certain threshold power level. Upon receiving a low battery setting from the mobile device the card authenticator 120 may update its setting regarding all cards (or transactions) associated with mobile device 110.

[0094] Other examples of choices may include, but are not limited to, offer the user the option to approve transactions totaling a threshold amount, or approving all transactions for a particular period of time after the loss of power. Each option that is chosen by the mobile device 110 may be transmitted to the authentication server 120 and stored and executed by the authentication server 120.

[0095] Internet transaction authorization will be updated through the application and all other transactions will be updated in the transaction log.A unique code provided by the issuing bank through physical mail will be used to add new cards rather than a SMS.

[0096] Various embodiments may include a method for authenticating a transaction, the method comprising: sending, by an authentication server, an authentication notification to a mobile device, the mobile device configured to be preauthorized to approve transactions related to at least one card of a card holder; approving the transaction forthe at least one card, upon receiving an approval message from the mobile device; and rejecting the transaction forthe at least one card, upon receiving a rejection message from the mobile device.

[0097] The method of the above embodiments, wherein the mobile device has been preauthorized to approve the transaction by the authentication server for the at least one card further comprises the authentication server being configured to determine the identity of the mobile device using the card information.

[0098] The method of the above embodiments, wherein the mobile device being configured to be preauthorized further comprising receiving from the mobile device transaction information, at least one of card information, and mobile device identification information.

[0099] The method of the above embodiments, wherein only a single mobile device is configured to be preauthorized to approve transaction for the at least one card.

[00100] The method of the above embodiments, wherein approving the transaction further comprises generating a message to a network processor to approve the transaction.

[00101] The method of the above embodiments, wherein approving the transaction further comprises generating a message to an issuing bank computer system that issued the at least one card to approve the transaction.

[00102] The method of the above embodiments, wherein the message to the issuing bank computer system includes mobile device identification information.

[00103] A system for authenticating transactions, the system comprising:an authentication server having a computer processor in communication with a non-transitory storage means, the authentication server configured to send an authentication notification to a mobile device, the authentication server configured to preauthorize the mobile device to approve transactions related to the at least one card of a card holder;the authentication server configured to approve the transaction after receiving an approval message from the mobile device; andthe authentication server configured to reject the transaction upon receiving a rejection message from the mobile device or after failing to receive any message from the mobile device.

[00104] The system as described above, wherein the authentication server is configured to authorize the mobile device to approve the transaction by the authentication server for the at least one card further comprises the authentication server being configured to determine the identity of the mobile device using the card information.

[00105] The system as described above, wherein the mobile device being configured to be preauthorized further comprising: the authentication server configured to receive from the mobile device the at least one of card information, mobile device identification information.

[00106] The system as described above, wherein only a single mobile device is configured to be preauthorized to approve transaction for the at least one card.

[00107] The system as described above, further comprising the authentication server configured to generate a message to a network processor to approve the transaction.

[00108] The system as described above, further comprising the authentication server configured to generate a message to an issuing bank computer system after receiving an approval from the at least one card to approve the transaction.

[00109] The system as described above, wherein the message to the issuing bank computer system includes mobile device identification information.

[00110] An apparatus for authenticating transactions, the system comprising:a sending means for sending an authentication notification to a mobile device;a preauthorizing means for preauthorizing the mobile device to approve transactions related to at least one card of a card holder;an approving means for approving the transaction forthe at least one card, upon receiving an approval message from the mobile device; anda rejecting means for rejecting the transaction forthe at least one card, upon receiving a rejection message from the mobile device.

[00111] The apparatus as described above, further comprising a determination means for determining an identity of the mobile device in response to receiving the card information.

[00112] The apparatus as described above, further comprising a receiving means for receiving from the mobile device mobile device identification information.

[00113] The apparatus as described above, wherein the approving means for approving responds to only a single mobile device that is preauthorized to approve transaction for the at least one card.

[00114] The apparatus as described above, wherein the approving means for approving is configured to generate a message to a network processor to approve the transaction and configured to generate a message to an issuing bank computer system that issued the at least one card to approve the transaction.

[00115] The apparatus as described above, wherein the message to the issuing bank computer system includes mobile device identification information.

[00116] The present disclosure contemplates methods, systems and program products on any machine-readable non-transitory storage media for accomplishing various operations. The embodiments of the present disclosure may be implemented using existing computer processors, or by a special purpose computer processor for an appropriate system, incorporated for this or

another purpose, or by a hardwired system. Embodiments within the scope of the present disclosure include program products comprising machine-readable media for carrying or having machine-executable instructions or data structures stored thereon. Such machine-readable media can be any available media that can be accessed by a general purpose or special purpose computer or other machine with a processor. By way of example, such machine-readable media can comprise RAM, ROM, EPROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code in the form of machine-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer or other machine with a processor. Combinations of the above are also included within the scope of machine-readable media. Machine-executable instructions include, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing machines to perform a certain function or group of functions. Software implementations could be accomplished with standard programming techniques with rule-based modules and other logic to accomplish the various connection steps, processing steps, comparison steps and decision steps.

[00117] While this specification contains many specific implementation details, these should not be construed as limitations on the scope of what may be claimed, but rather as descriptions of features specific to particular implementations. Certain features described in this specification in the context of separate implementations can also be implemented in combination in a single implementation. Conversely, various features described in the context of a single implementation can also be implemented in multiple implementations separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a subcombination or variation of a subcombination.

[00118] Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous.

Moreover, the separation of various system components in the implementations described above should not be understood as requiring such separation in all implementations, and it should be understood that the described program components and systems can generally be integrated in a single software product or packaged into multiple software products embodied on tangible media.

[00119] Thus, particular implementations of the subject matter have been described. Other implementations are within the scope of the following claims. In some cases, the actions recited in the claims can be performed in a different order and still achieve desirable results. In addition, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. In certain implementations, multitasking and parallel processing may be advantageous.

[00120] The claims should not be read as limited to the described order or elements unless stated to that effect. It should be understood that various changes in form and detail may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims. All implementations that come within the spirit and scope of the following claims and equivalents thereto are claimed.

CLAIMS

1. A method for authenticating a transaction, the method comprising:

sending, by aserver, anauthentication notificationto a mobile device, the mobile device configured to be preauthorized to approve transactions related to at least one card of a card holder;

approving the transaction for the at least one card, upon receiving an approval notificationfrom the mobile device; and

rejecting the transaction for the at least one card, upon receiving a rejection notification from the mobile device.

2. The method of claim 1, wherein the mobile device has been preauthorizedto approve the transaction by the server for the at least one card further comprises the server being configured to determine the identity of the mobile device using the card information.

3. The method of claim 2, wherein the mobile device being configured to be preauthorized further comprising receiving from the mobile device transaction information, at least one of card information, and mobile device identification information.

4. The method of claim 2, wherein only a single mobile device is configured to be preauthorized to approve transaction for the at least one card.

5. The method of claim 1, wherein approving the transaction further comprises generating a message to a network processor to approve the transaction.

6. The method of claim 1, wherein approving the transaction further comprises generating a message to an issuing bank computer system that issued the at least one card to approve the transaction.

7. The method of claim 6, wherein the message to the issuing bank computer system includes mobile device identification information.

8. A system for authenticating transactions, the system comprising:
a server having a computer processor in communication with a non-transitory storage means, the server configured to send anauthentication notification to a mobile device, the

server configured to preauthorize the mobile device to approve transactions related to at least one card of a card holder;

the server configured to approve the transaction after receiving an approval message from the mobile device; and

the server configured to reject the transaction upon receiving a rejection message from the mobile device or after failing to receive any message from the mobile device.

9. The system of claim 8, wherein the serveris configured to authorizethe mobile device to approve the transaction by the server for the at least one card further comprises the server being configured to determine the identity of the mobile device using the card information.

10. The system of claim 9, wherein the mobile device being configured to be preauthorized further comprising: the server configured to receive from the mobile device at least one of card information, mobile device identification information.

11. The system of claim 9, wherein only a single mobile device is configured to be preauthorized to approve transaction for the at least one card.

12. The system of claim 8, further comprising the server configured to generate a message to a network processor to approve the transaction.

13. The system of claim 8, further comprising the server configured to generate a message to an issuing bank computer system after receiving an approval from at least one card to approve the transaction.

14. The system of claim 13, wherein the message to the issuing bank computer system includes mobile device identification information.

15. An apparatus for authenticating transactions, the apparatus comprising:

a sending means for sending anauthentication notification to a mobile device;

a preauthorizing means for preauthorizing the mobile device to approve transactions related to at least one card of a card holder;

an approving means for approving the transaction for the at least one card, upon receiving an approval message from the mobile device with approval being achieved through one or more authorization means comprising swiping, PIN, or biometrics; and

a rejecting means for rejecting the transaction for the at least one card, upon receiving a rejection message from the mobile device.

16. The apparatus of claim 15, further comprising a determination means for determining an identity of the mobile device in response to receiving the card information.

17. The apparatus of claim 16, further comprising a receiving means for receiving from the mobile device mobile device identification information.

18. The apparatus of claim 16, wherein the approving means for approving responds to only a single mobile device that is preauthorized to approve transaction for the at least one card.

19. The apparatus of claim 15, wherein the approving means for approvingis configured to generate a message to a network processor to approve the transaction and configured to generate a message to an issuing bank computer system that issued the at least one card to approve the transaction.

20. The apparatus of claim 19, wherein the message to the issuing bank computer system includes mobile device identification information.

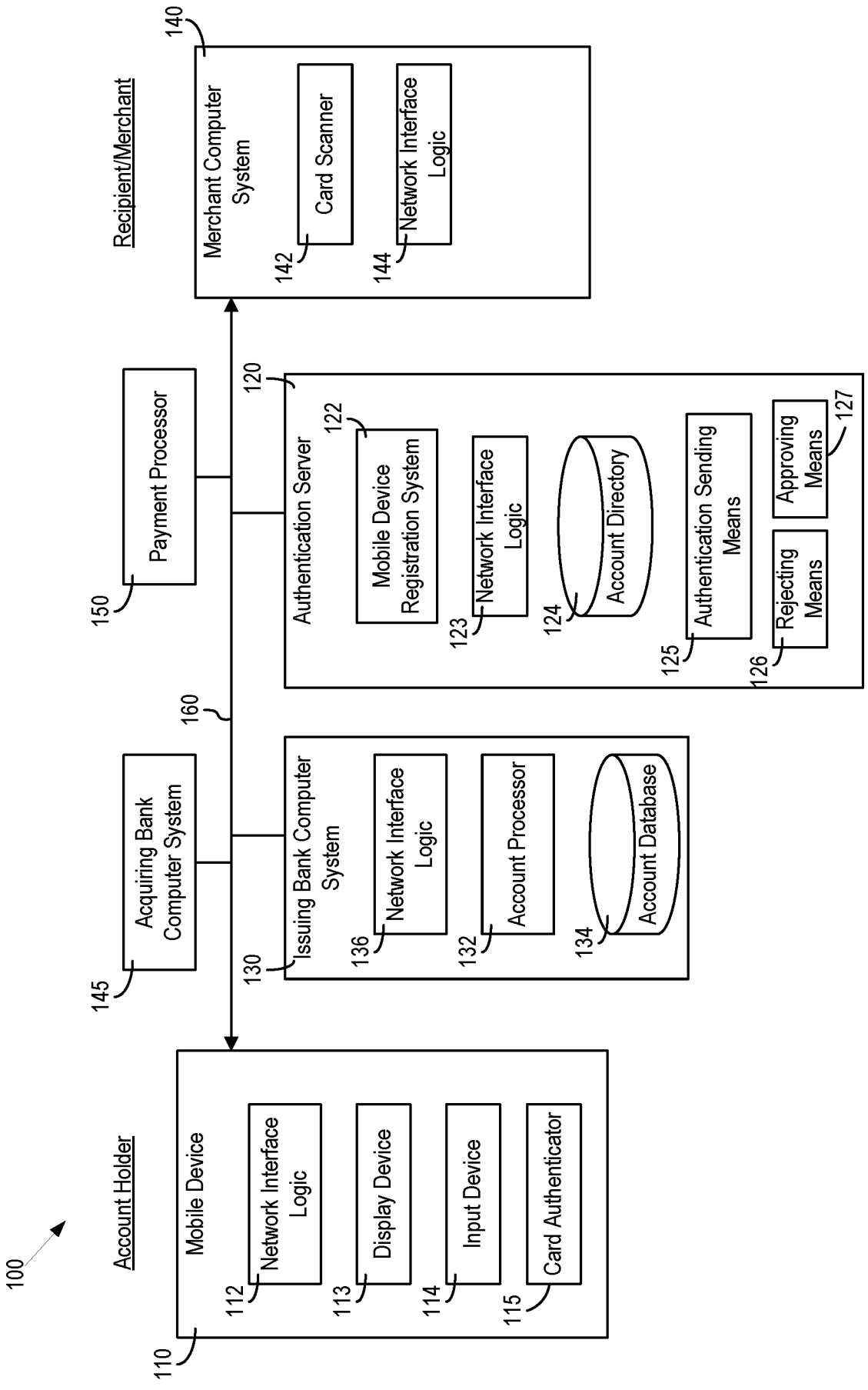
100
Account Holder
Mobile Device
110
Network Interface Logic
112
Display Device
113
Input Device
114
Card Authenticator
115
Acquiring Bank Computer System
145
Issuing Bank Computer System
130
Network Interface Logic
136
Account Processor
132
Account Database
134
160
Payment Processor
150
Recipient/Merchant
Merchant Computer System
140
Card Scanner
142
Network Interface Logic
144
Authentication Server
120
Mobile Device Registration System
122
Network Interface Logic
123
Account Directory
124
Authentication Sending Means
125
Rejecting Means
126
Approving Means
127

FIG. 1

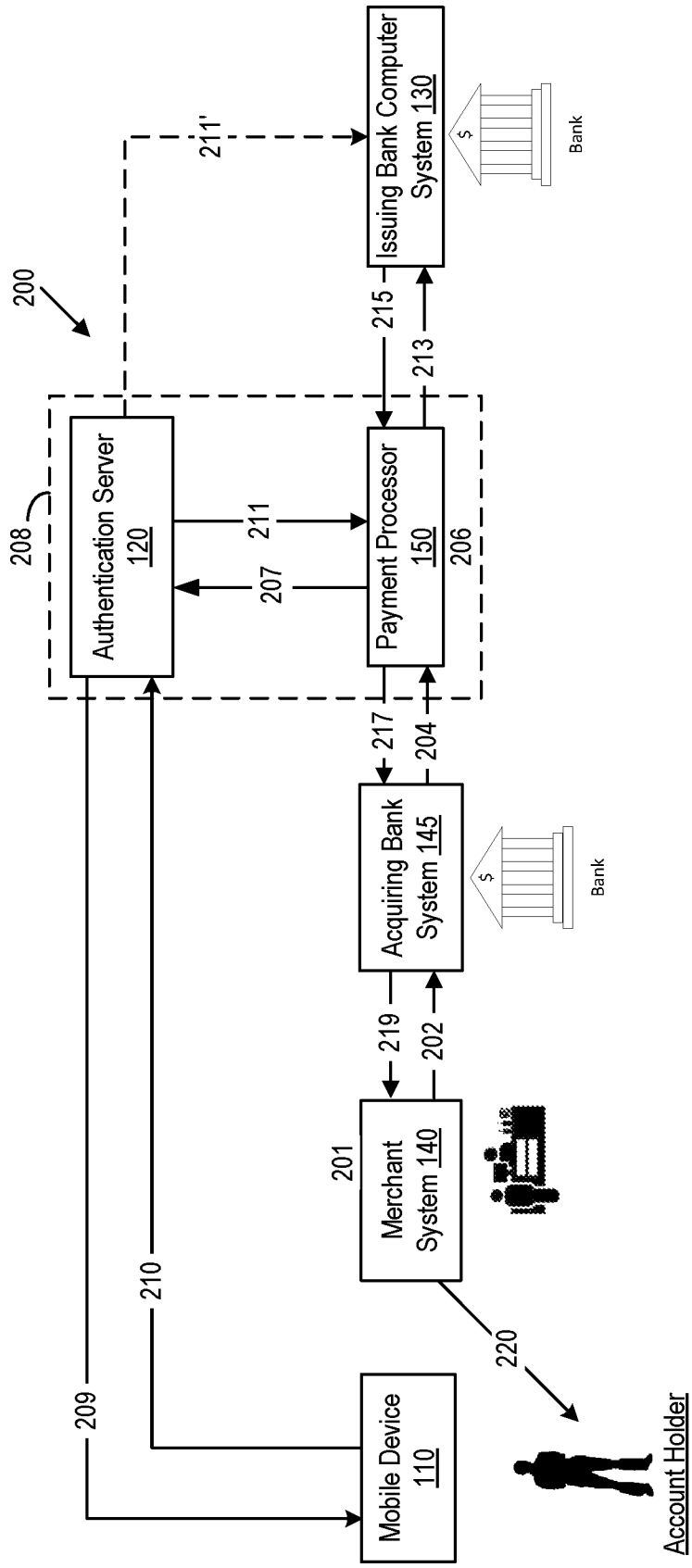
200
211'
Issuing Bank Computer System 130
Bank
215
213
208
Authentication Server 120
211
207
Payment Processor 150
206
217
204
Acquiring Bank System 145
Bank
219
202
201
Merchant System 140
210
209
220
Mobile Device 110
Account Holder

FIG. 2A

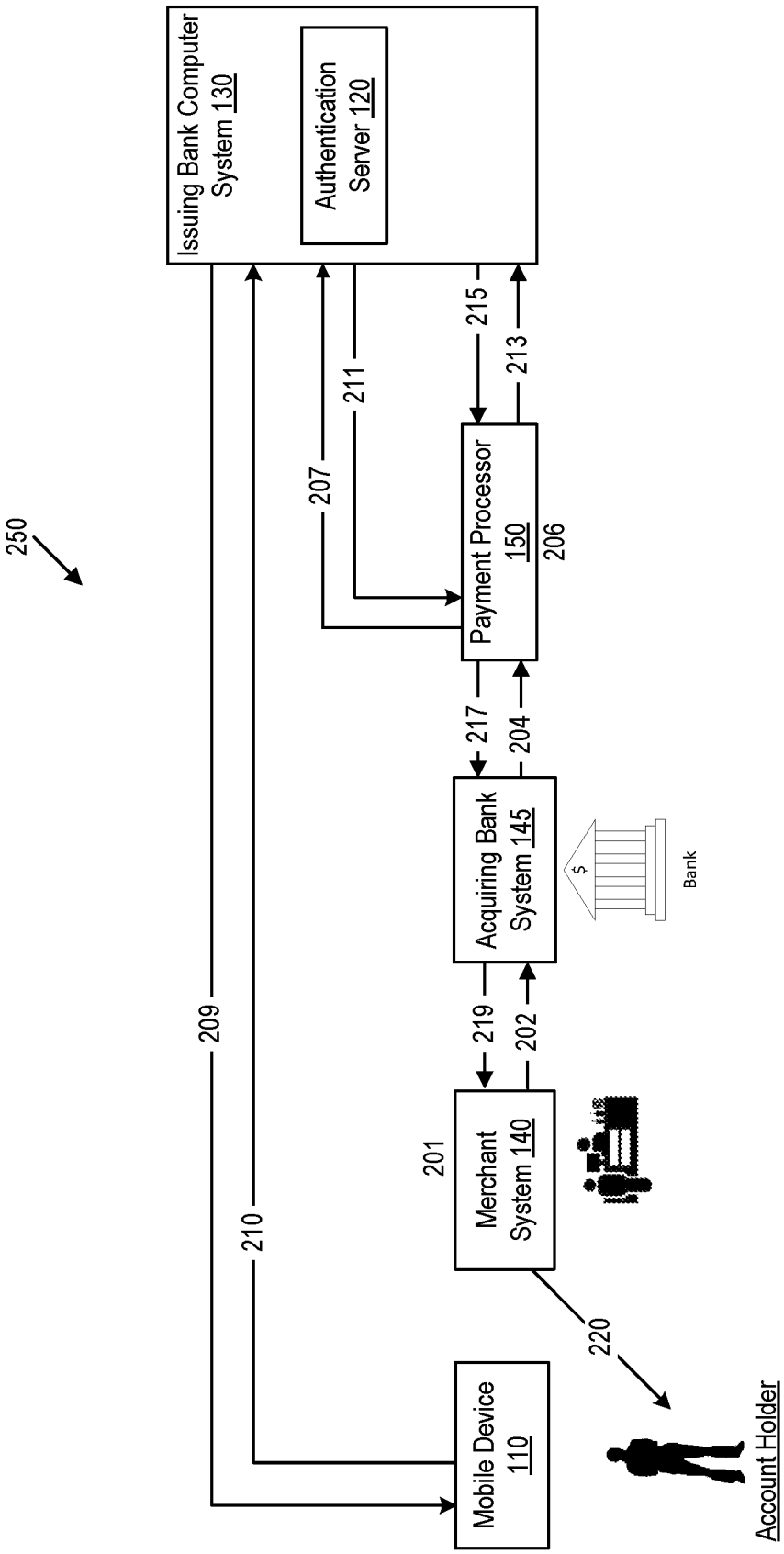
250
Issuing Bank Computer System 130
Authentication Server 120
Payment Processor 150
206
Acquiring Bank System 145
Bank
Merchant System 140
201
Mobile Device 110
Account Holder
207
211
215
213
217
204
219
202
209
210
220

FIG. 2B

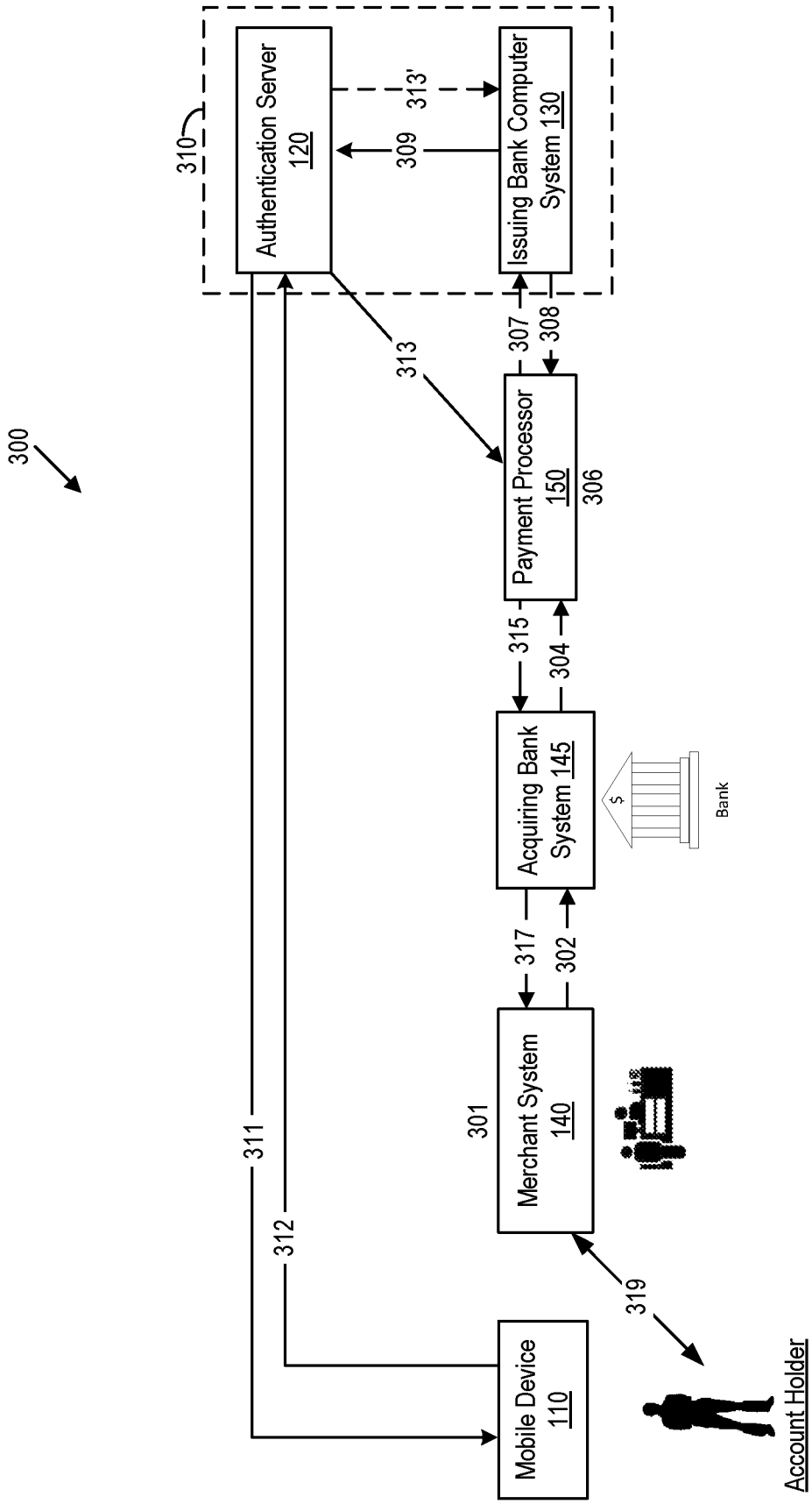
300
310
Authentication Server 120
Issuing Bank Computer System 130
313'
309
313
307
308
Payment Processor 150
306
315
304
Acquiring Bank System 145
$
Bank
317
302
301
Merchant System 140
311
312
319
Mobile Device 110
Account Holder

FIG. 3A

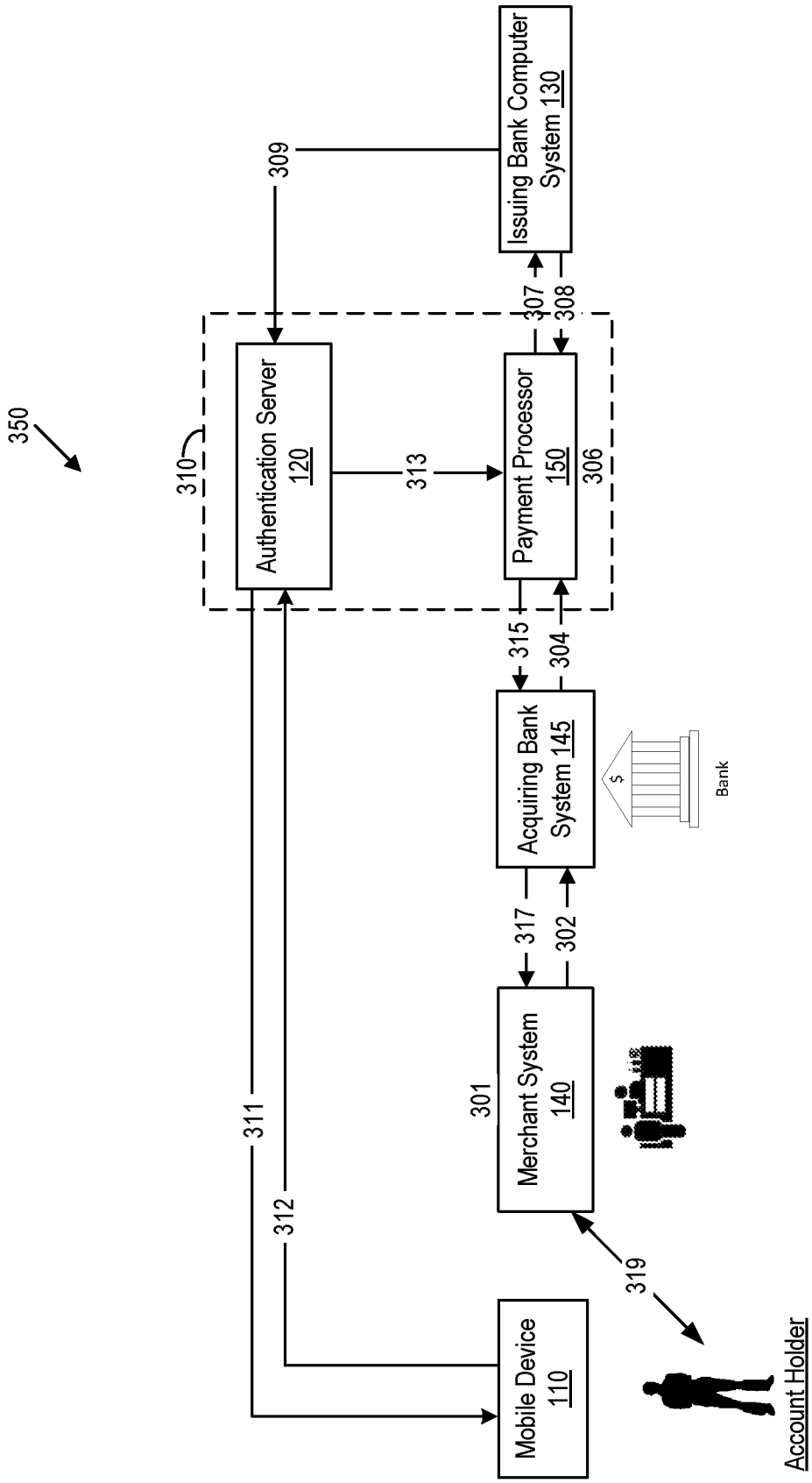
350
Issuing Bank Computer System 130
309
307
308
310
Authentication Server 120
313
Payment Processor 150
306
315
304
Acquiring Bank System 145
$
Bank
317
302
301
Merchant System 140
311
312
319
Mobile Device 110
Account Holder

FIG. 3B

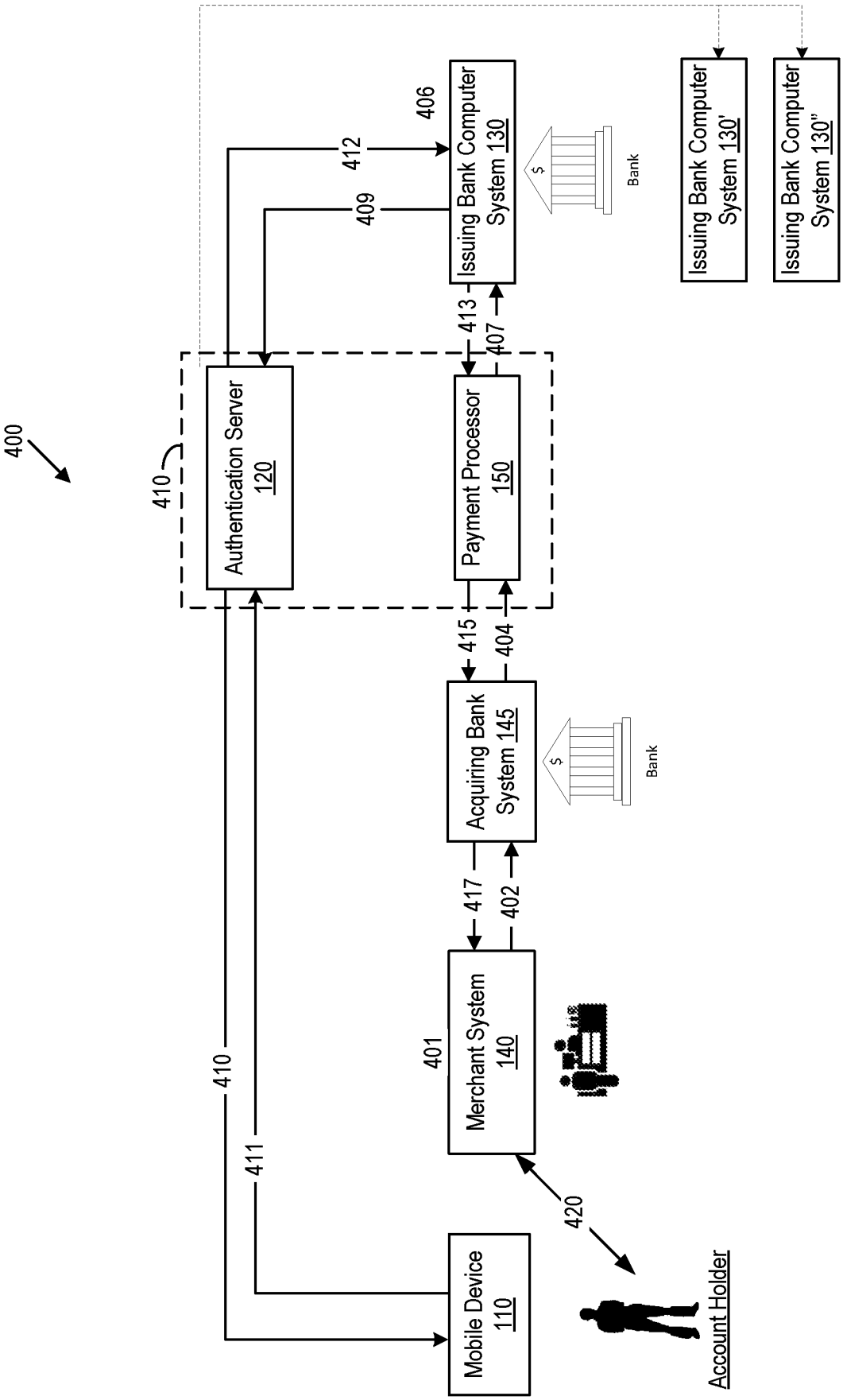
400
410
Authentication Server 120
Payment Processor 150
Issuing Bank Computer System 130
Issuing Bank Computer System 130'
Issuing Bank Computer System 130"
406
412
409
413
407
415
404
Acquiring Bank System 145
417
402
401
Merchant System 140
410
411
Mobile Device 110
420
Account Holder
Bank
Bank

FIG. 4A

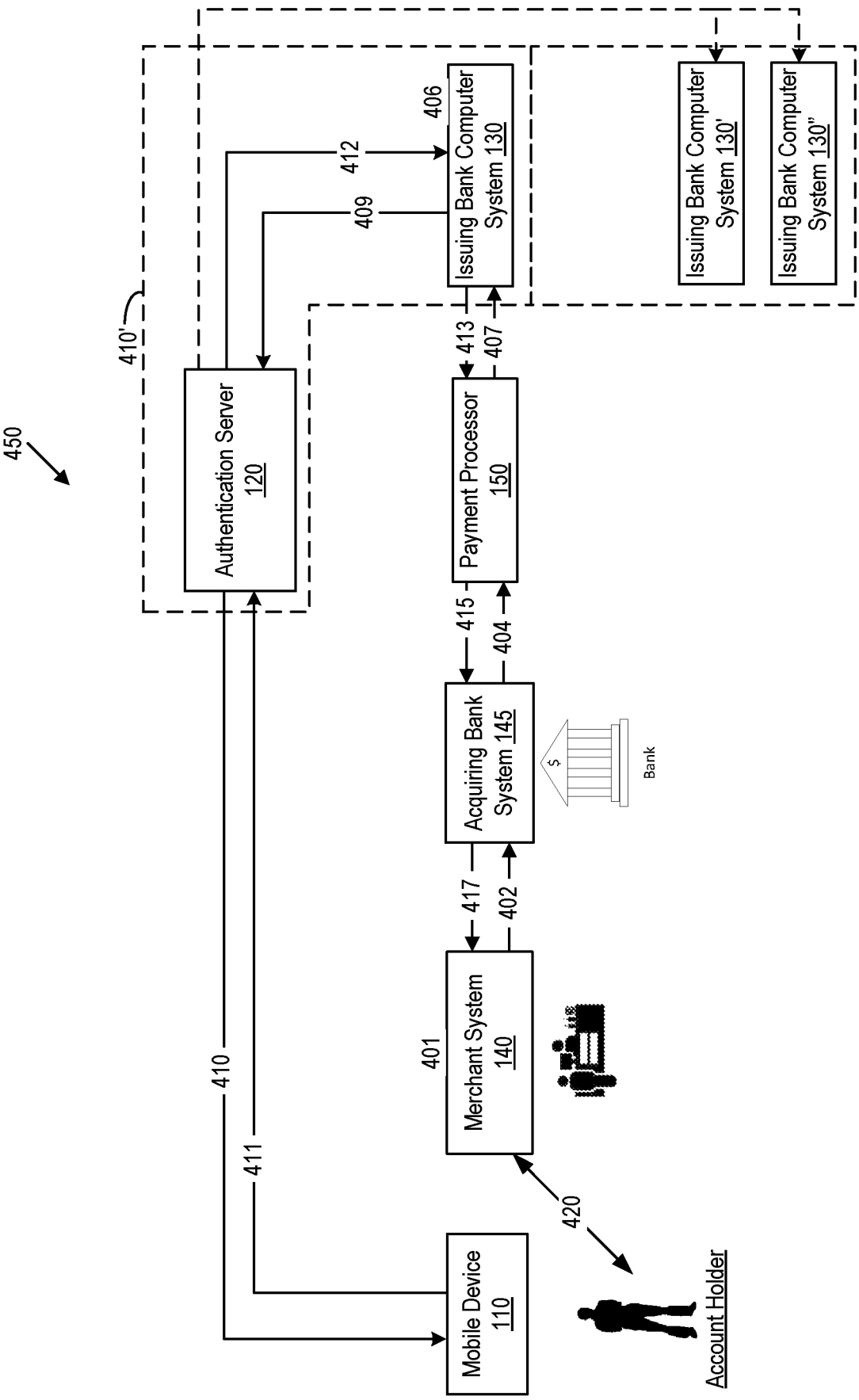
450
410'
Authentication Server 120
Payment Processor 150
Issuing Bank Computer System 130
Issuing Bank Computer System 130'
Issuing Bank Computer System 130"
Acquiring Bank System 145
Merchant System 140
Mobile Device 110
Account Holder
Bank
401
402
404
406
407
409
410
411
412
413
415
417
420

FIG. 4B

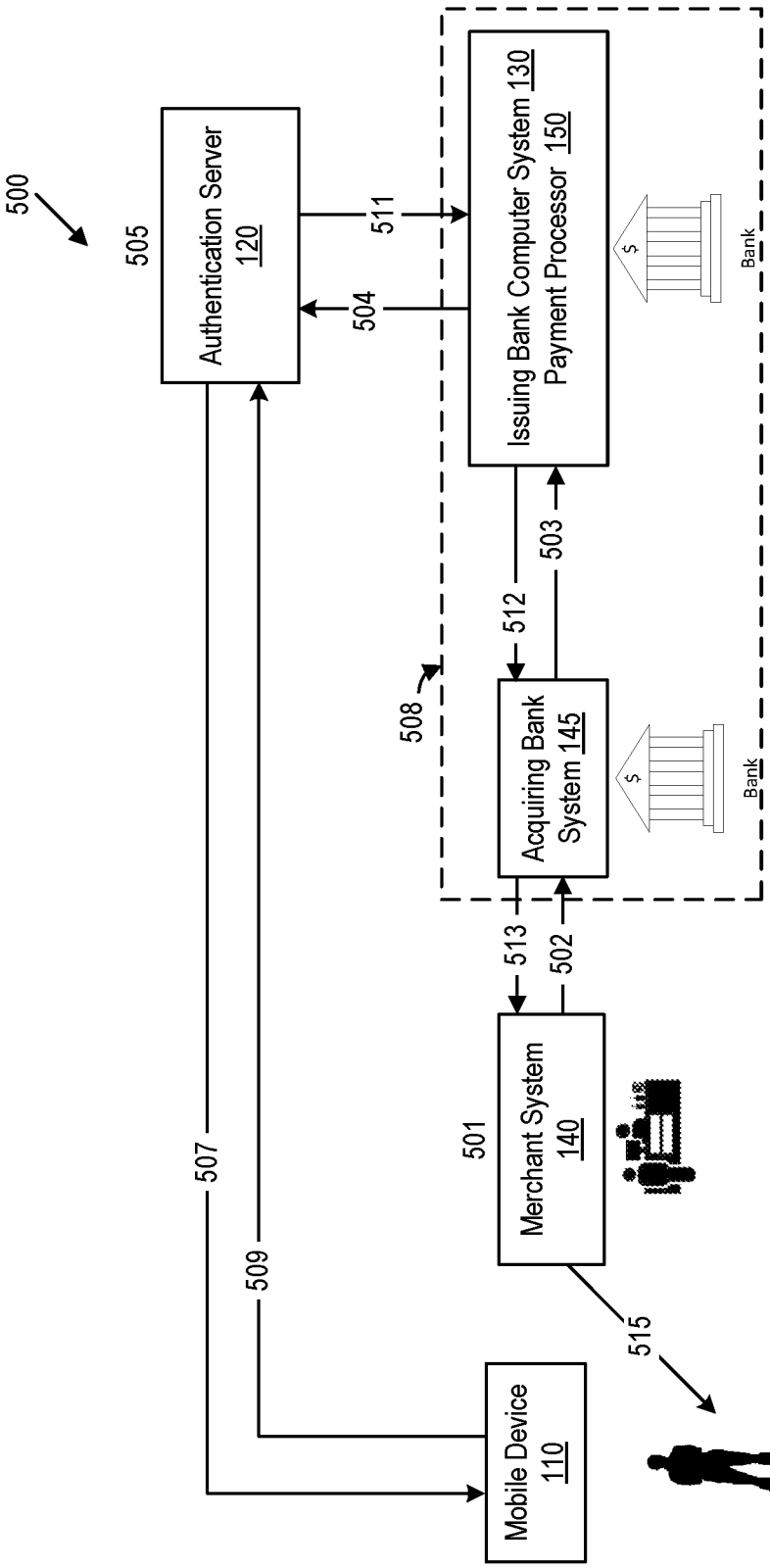
500
505
Authentication Server
120
511
504
Issuing Bank Computer System 130
Payment Processor 150
Bank
503
512
508
Acquiring Bank
System 145
Bank
513
502
501
Merchant System
140
507
509
515
Mobile Device
110
Account Holder

FIG. 5

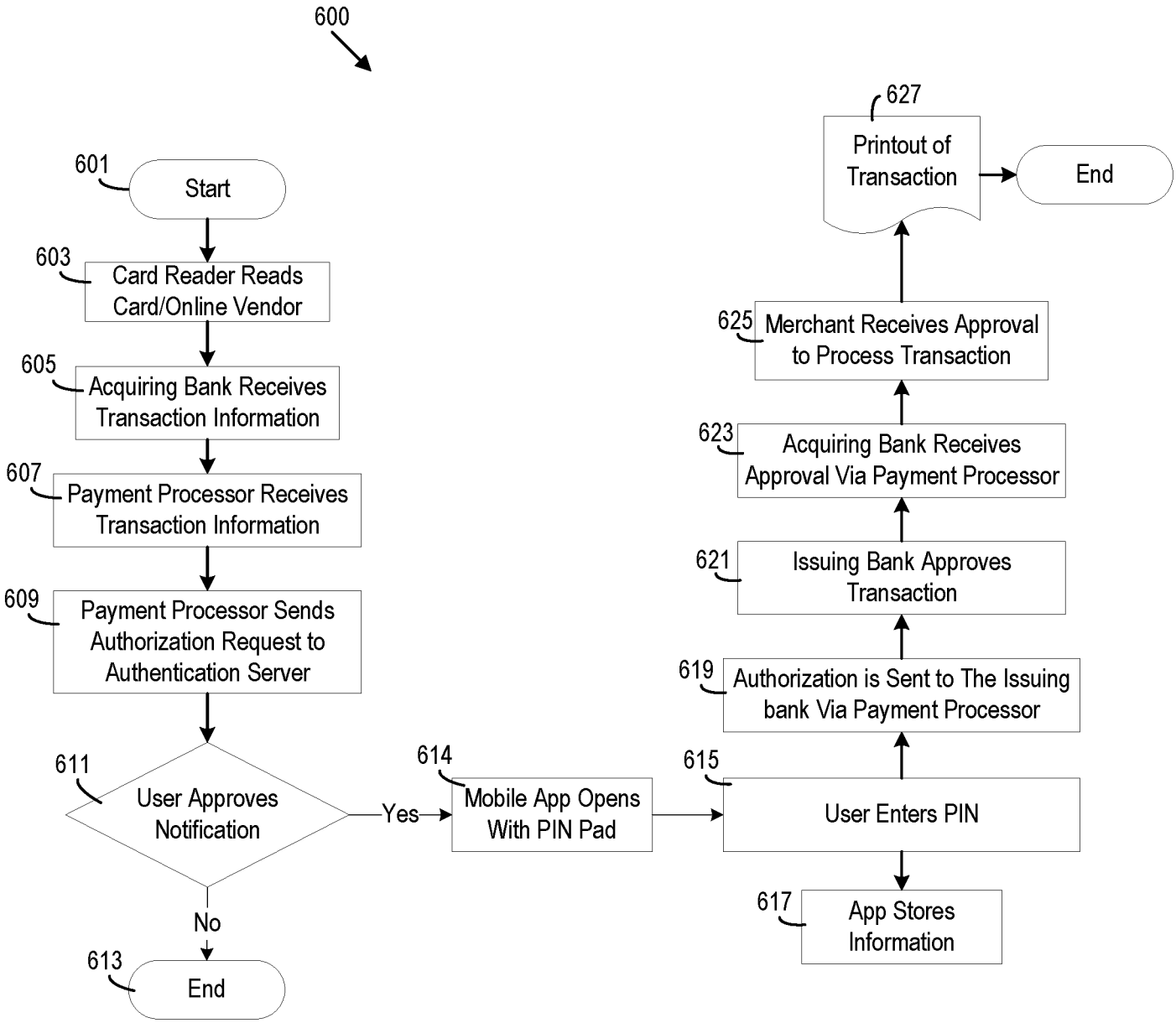
600
601
Start
603
Card Reader Reads Card/Online Vendor
605
Acquiring Bank Receives Transaction Information
607
Payment Processor Receives Transaction Information
609
Payment Processor Sends Authorization Request to Authentication Server
611
User Approves Notification
Yes
No
613
End
614
Mobile App Opens With PIN Pad
615
User Enters PIN
617
App Stores Information
619
Authorization is Sent to The Issuing bank Via Payment Processor
621
Issuing Bank Approves Transaction
623
Acquiring Bank Receives Approval Via Payment Processor
625
Merchant Receives Approval to Process Transaction
627
Printout of Transaction
End

FIG. 6

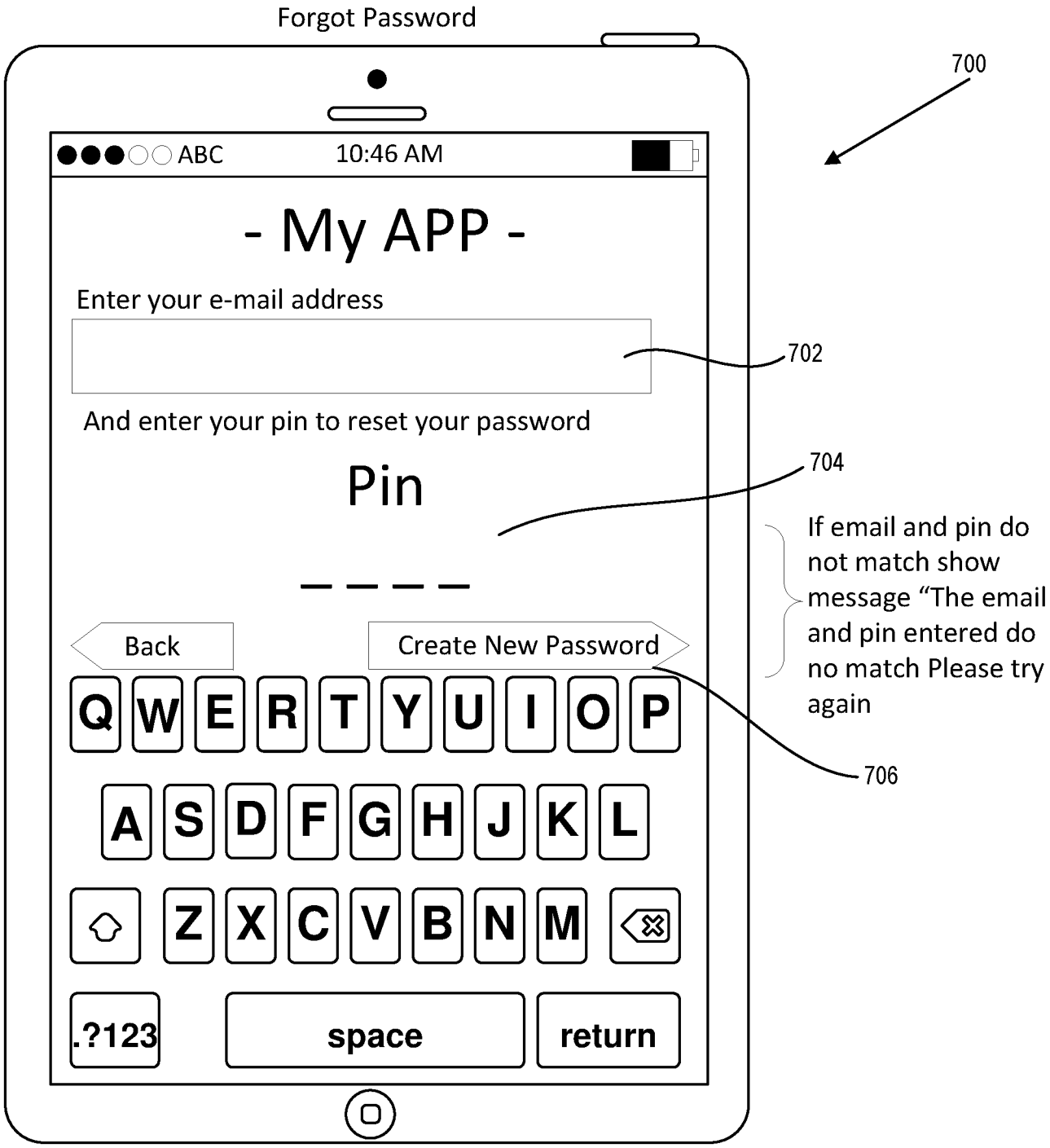
Forgot Password
700
ABC
10:46 AM
- My APP -
Enter your e-mail address
702
And enter your pin to reset your password
Pin
704
If email and pin do not match show message "The email and pin entered do no match Please try again
Back
Create New Password
706
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
.?123
space
return

FIG. 7

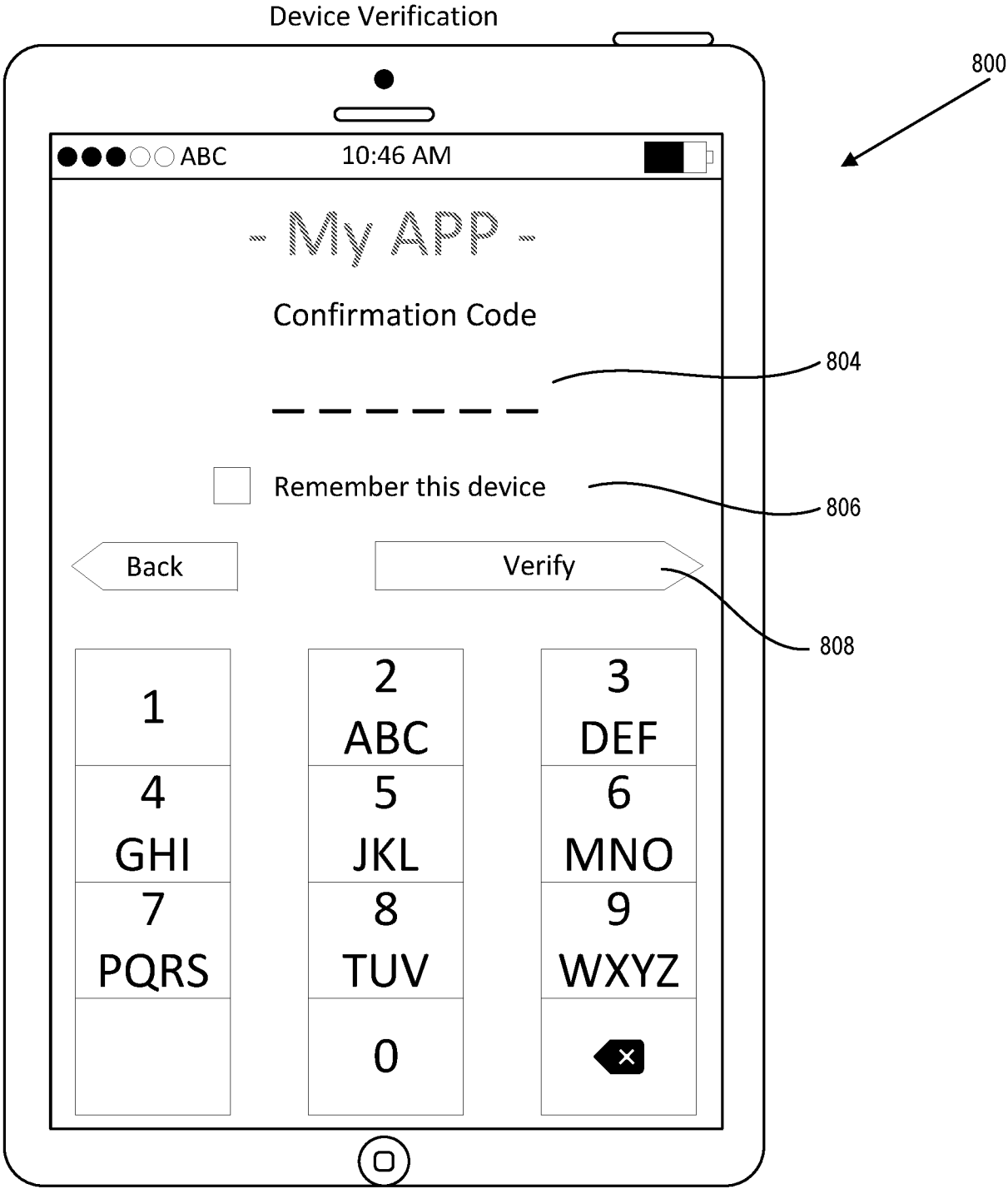
Device Verification
800
ABC
10:46 AM
My APP
Confirmation Code
804
Remember this device
806
Back
Verify
808
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

FIG. 8

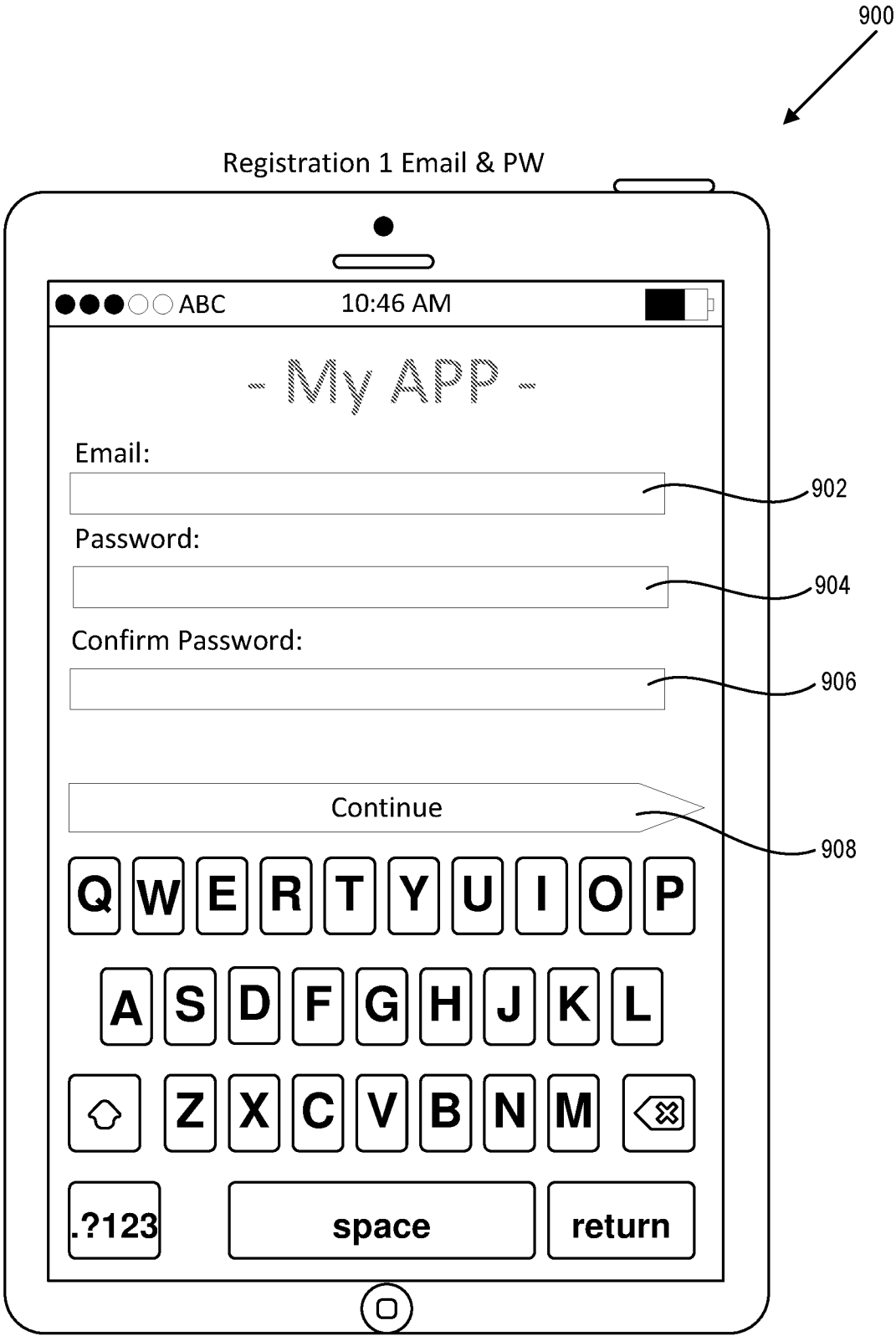
900
Registration 1 Email & PW
ABC
10:46 AM
- My APP -
Email:
902
Password:
904
Confirm Password:
906
Continue
908
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
.?123
space
return

FIG. 9

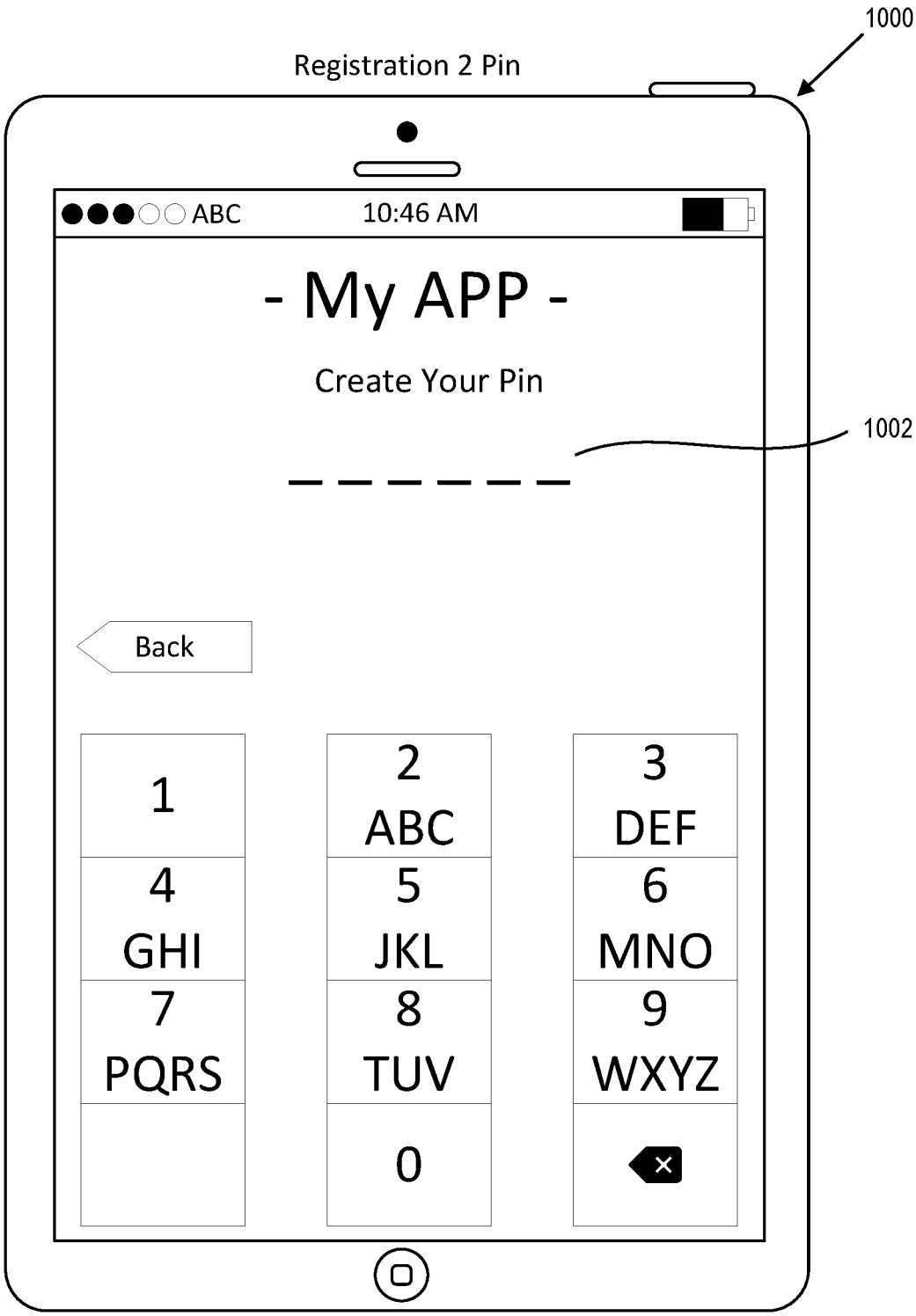
1000
Registration 2 Pin
ABC
10:46 AM
- My APP -
Create Your Pin
1002
Back
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

FIG. 10

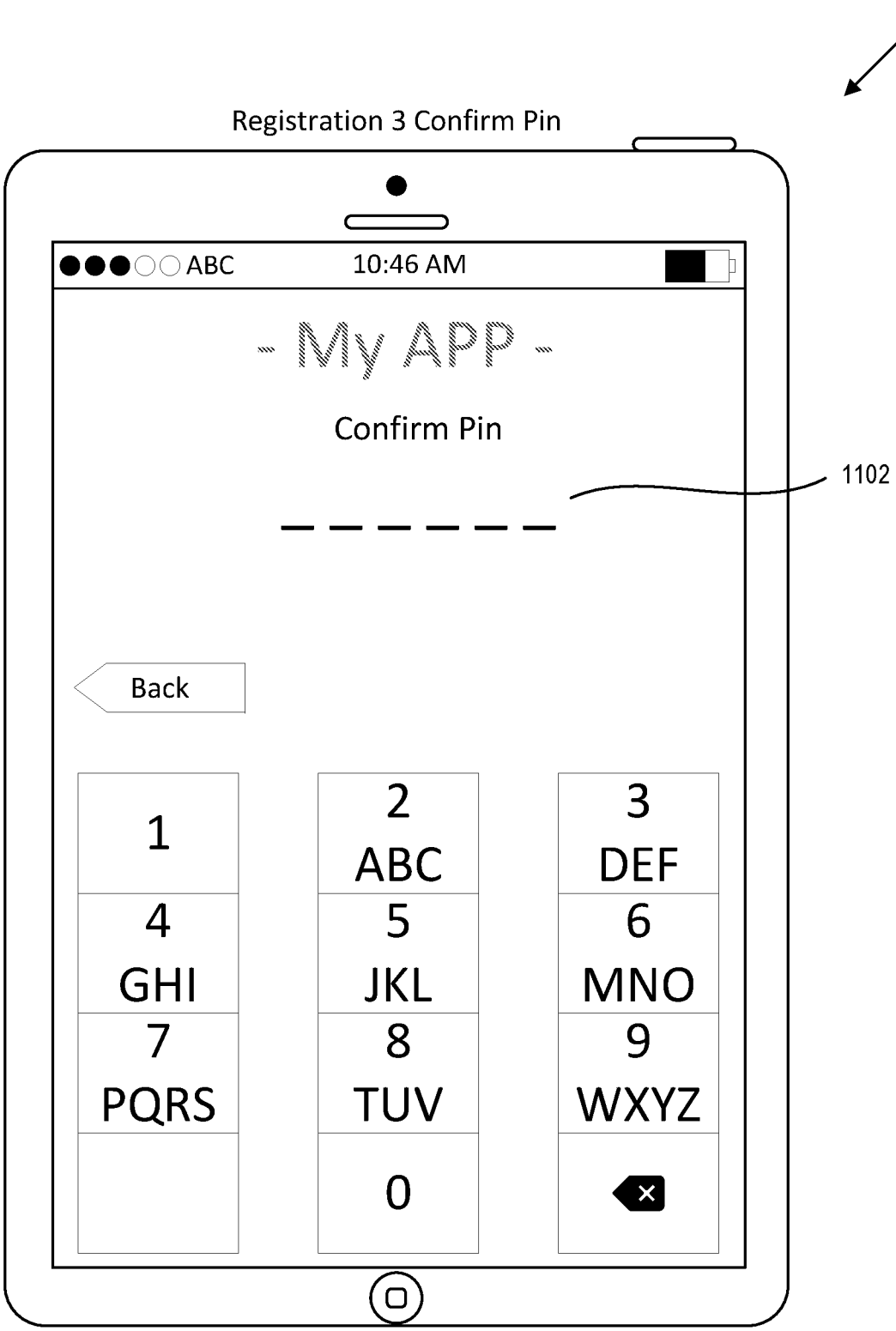
1100
Registration 3 Confirm Pin
ABC
10:46 AM
My APP
Confirm Pin
1102
Back
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

FIG. 11

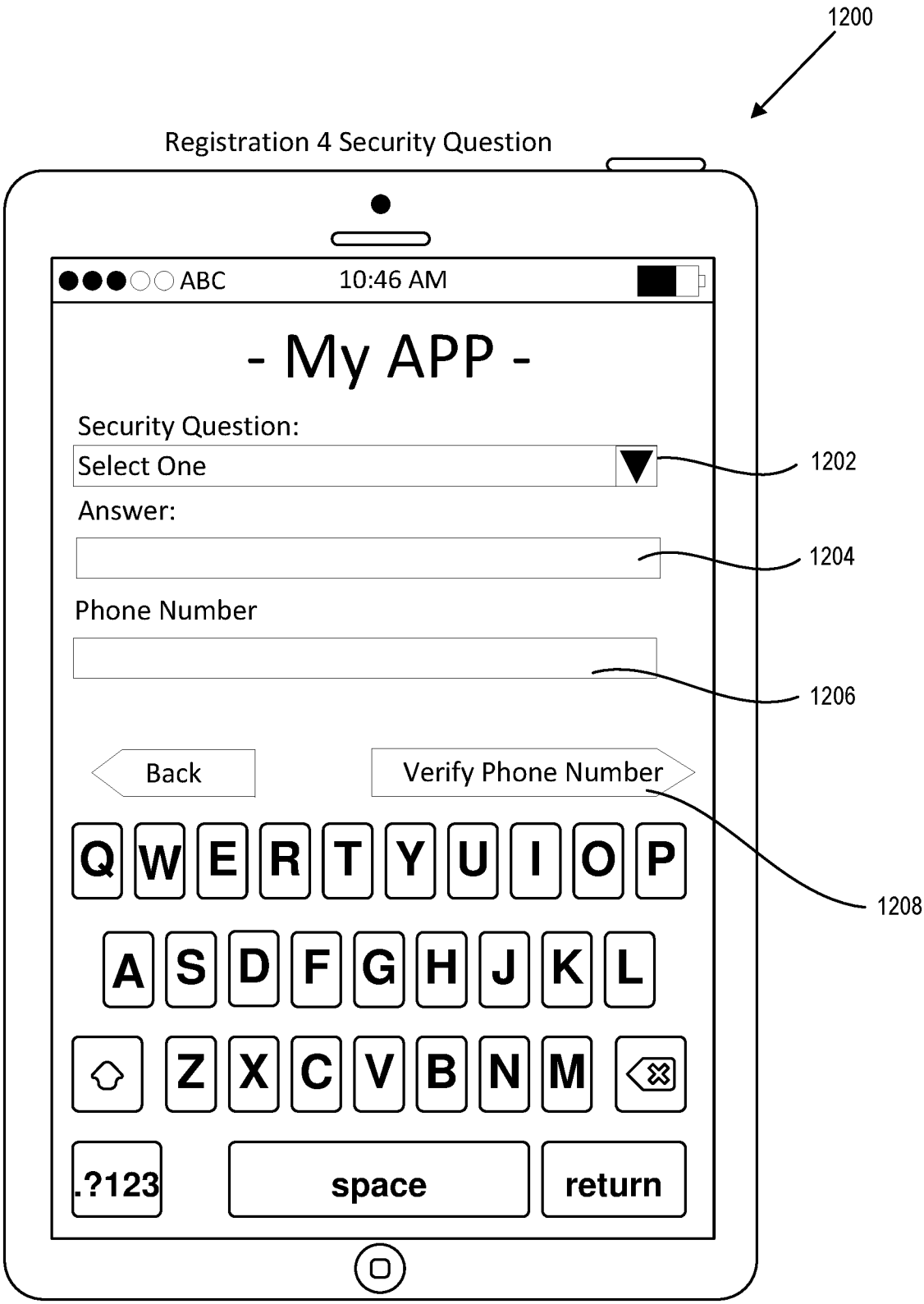
1200
Registration 4 Security Question
ABC
10:46 AM
- My APP -
Security Question:
Select One
1202
Answer:
1204
Phone Number
1206
Back
Verify Phone Number
1208
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
.?123
space
return

FIG. 12

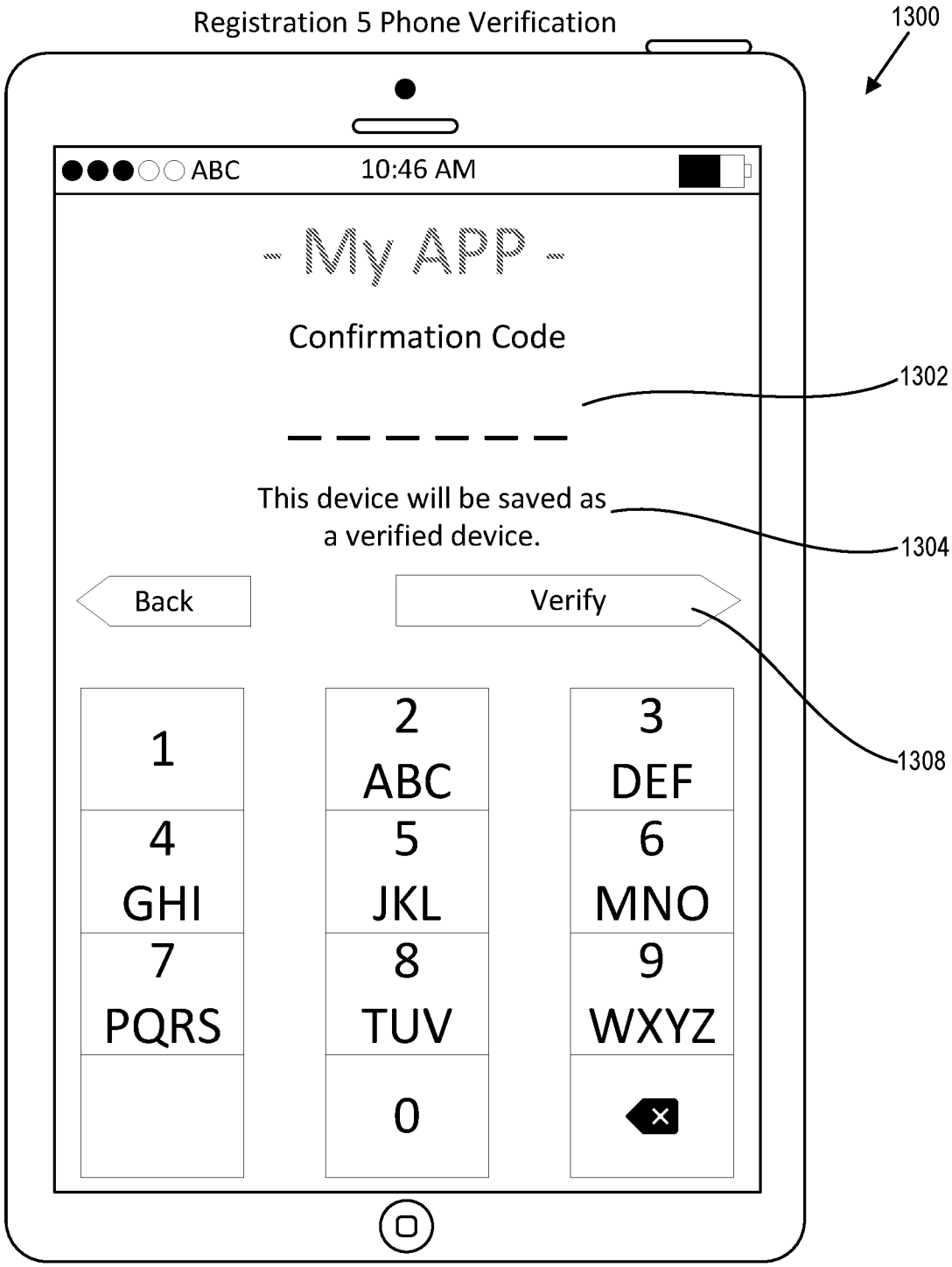
Registration 5 Phone Verification
1300
ABC
10:46 AM
My APP
Confirmation Code
1302
This device will be saved as
a verified device.
1304
Back
Verify
1308
1
2
ABC
3
DEF
4
GHI
5
JKL
6
MNO
7
PQRS
8
TUV
9
WXYZ
0

FIG. 13

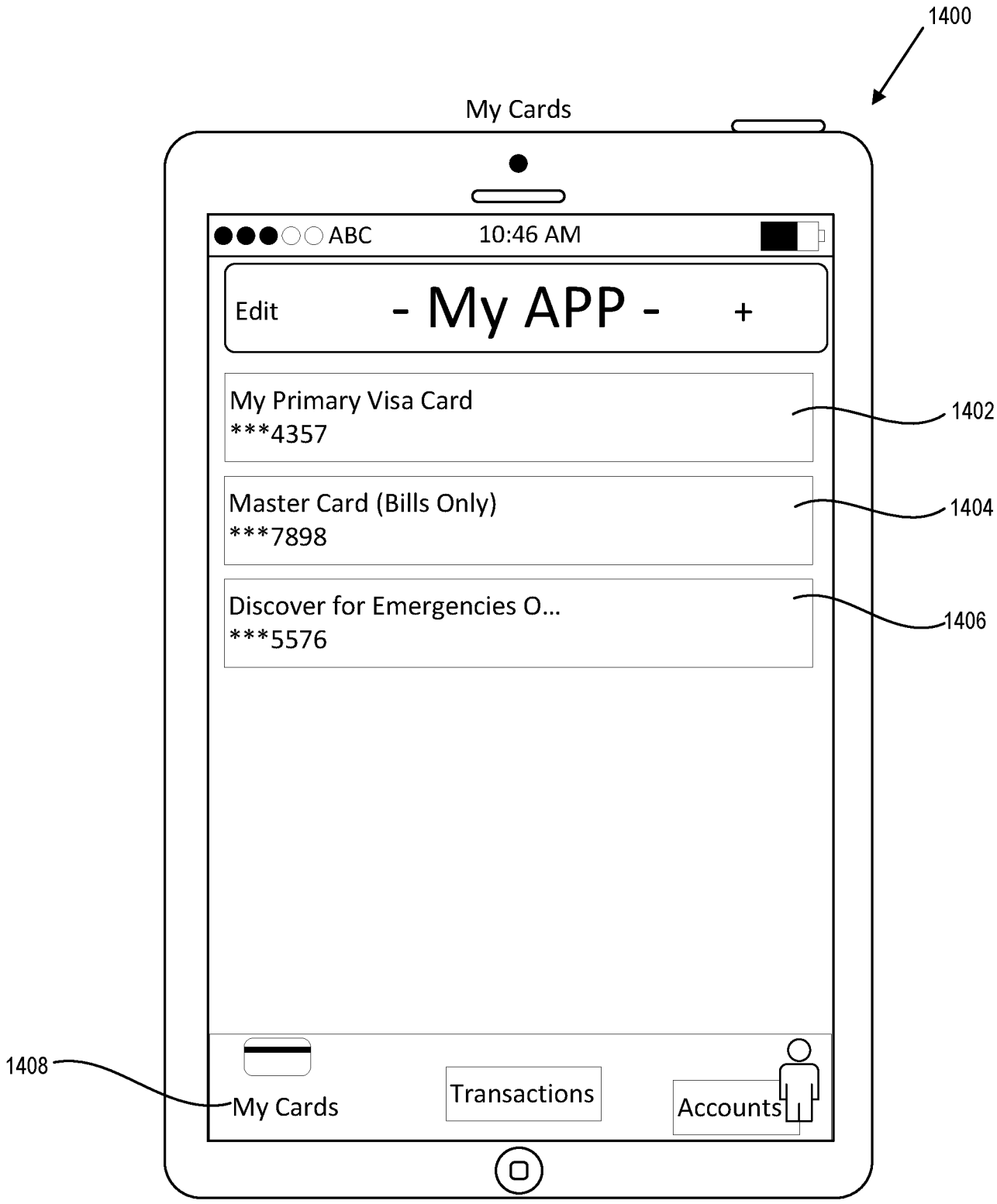
1400
My Cards
ABC
10:46 AM
Edit
- My APP -
+
My Primary Visa Card
***4357
1402
Master Card (Bills Only)
***7898
1404
Discover for Emergencies O...
***5576
1406
1408
My Cards
Transactions
Accounts

FIG. 14

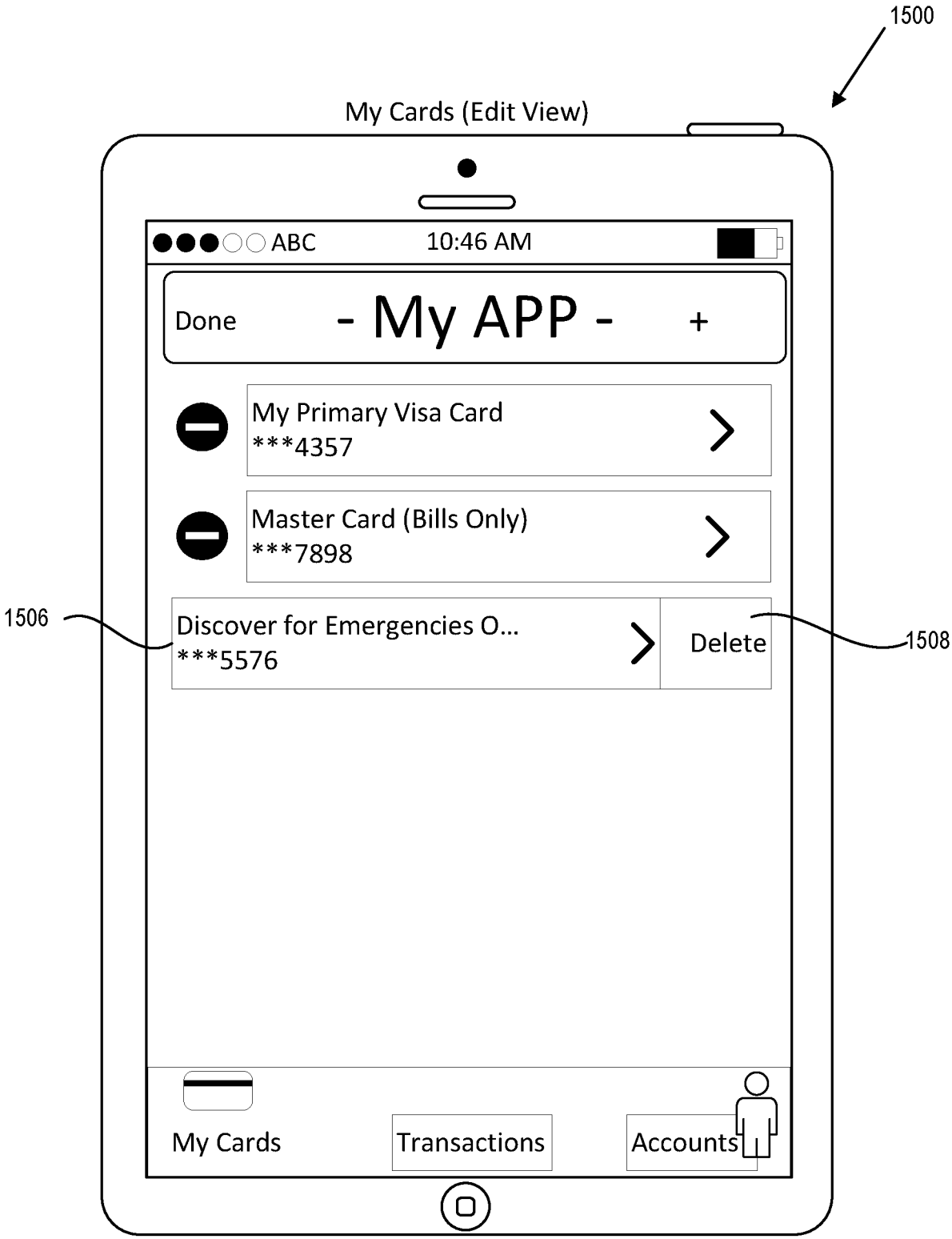
1500
My Cards (Edit View)
ABC
10:46 AM
Done
- My APP -
+
My Primary Visa Card
***4357
Master Card (Bills Only)
***7898
1506
Discover for Emergencies O...
***5576
Delete
1508
My Cards
Transactions
Accounts

FIG. 15

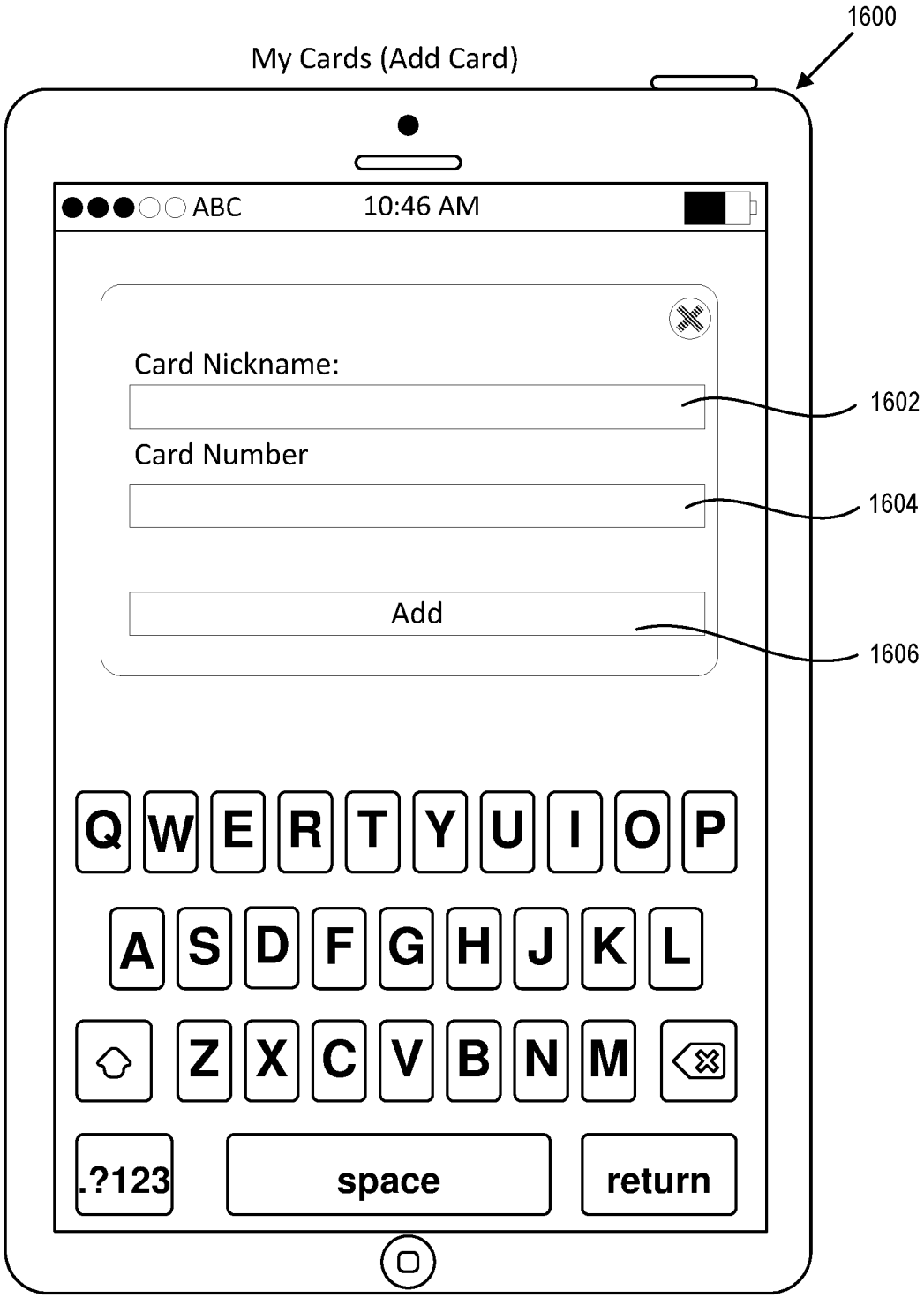
1600
My Cards (Add Card)
ABC
10:46 AM
Card Nickname:
1602
Card Number
1604
Add
1606
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
.?123
space
return

FIG. 16

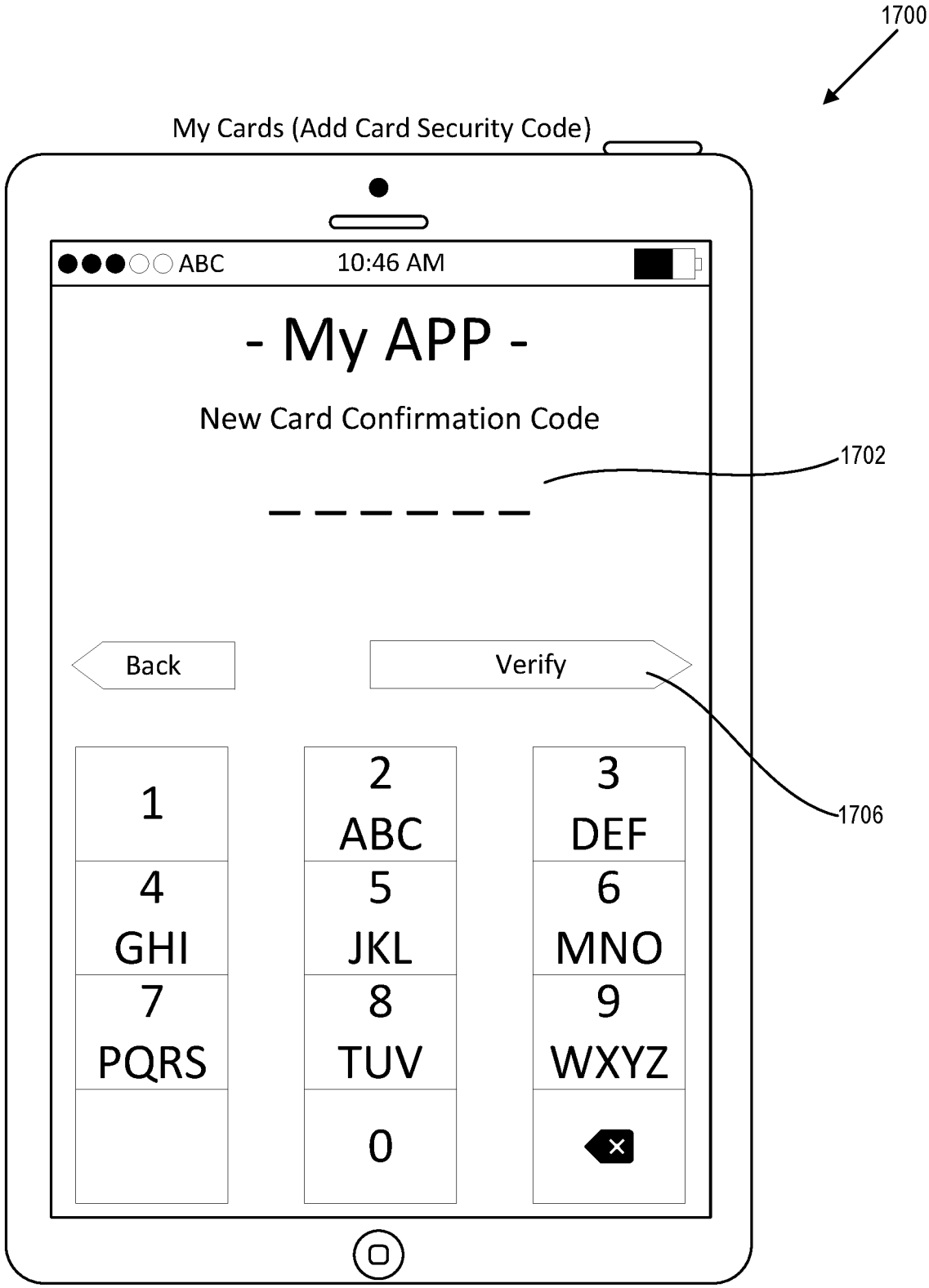
1700
My Cards (Add Card Security Code)
ABC
10:46 AM
- My APP -
New Card Confirmation Code
1702
Back
Verify
1706
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

FIG. 17

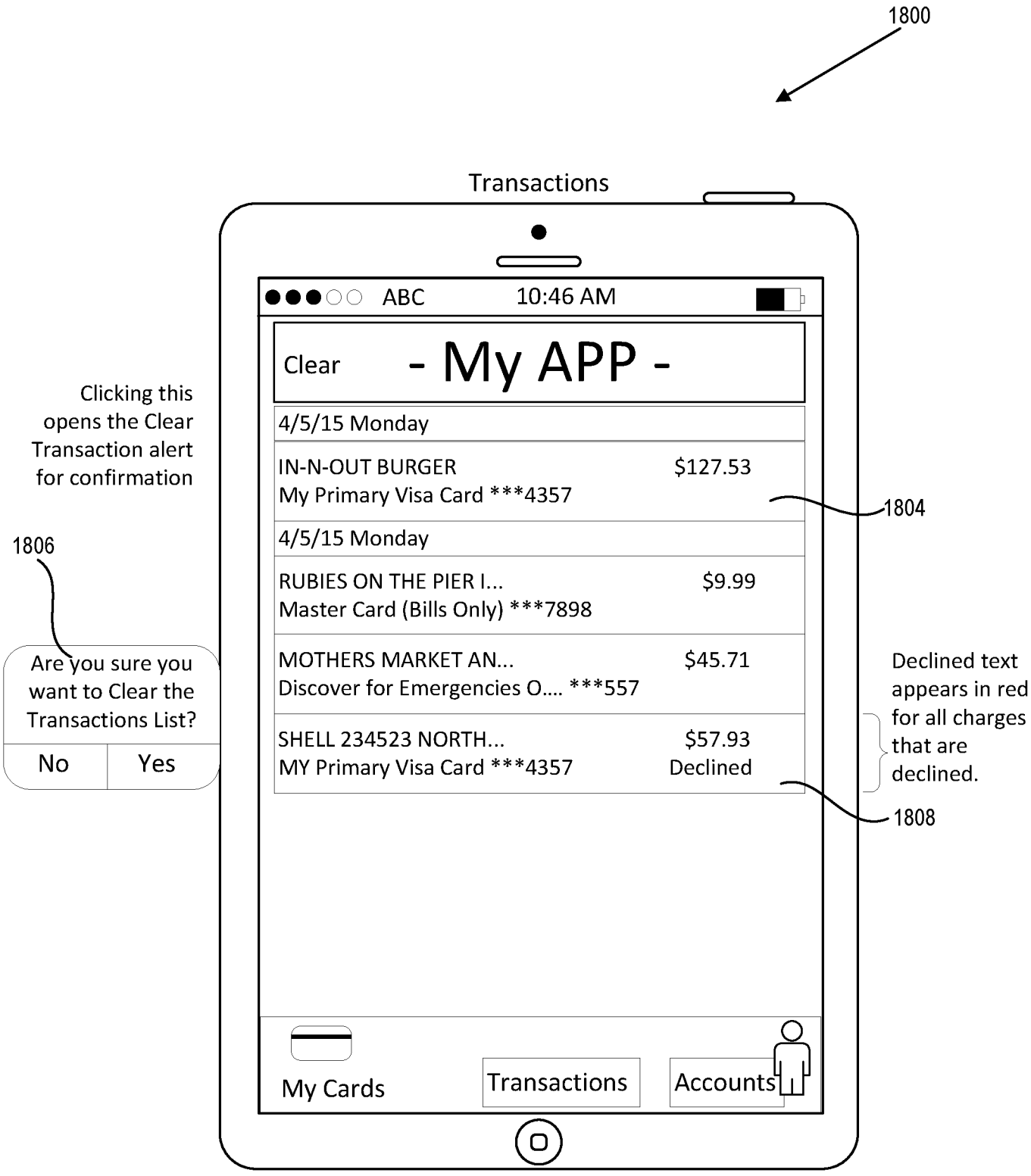
1800
Transactions
ABC
10:46 AM
Clear
- My APP -
4/5/15 Monday
IN-N-OUT BURGER
$127.53
My Primary Visa Card ***4357
1804
4/5/15 Monday
RUBIES ON THE PIER I...
$9.99
Master Card (Bills Only) ***7898
MOTHERS MARKET AN...
$45.71
Discover for Emergencies O.... ***557
SHELL 234523 NORTH...
$57.93
MY Primary Visa Card ***4357
Declined
1808
Declined text appears in red for all charges that are declined.
Clicking this opens the Clear Transaction alert for confirmation
1806
Are you sure you want to Clear the Transactions List?
No
Yes
My Cards
Transactions
Accounts

FIG. 18

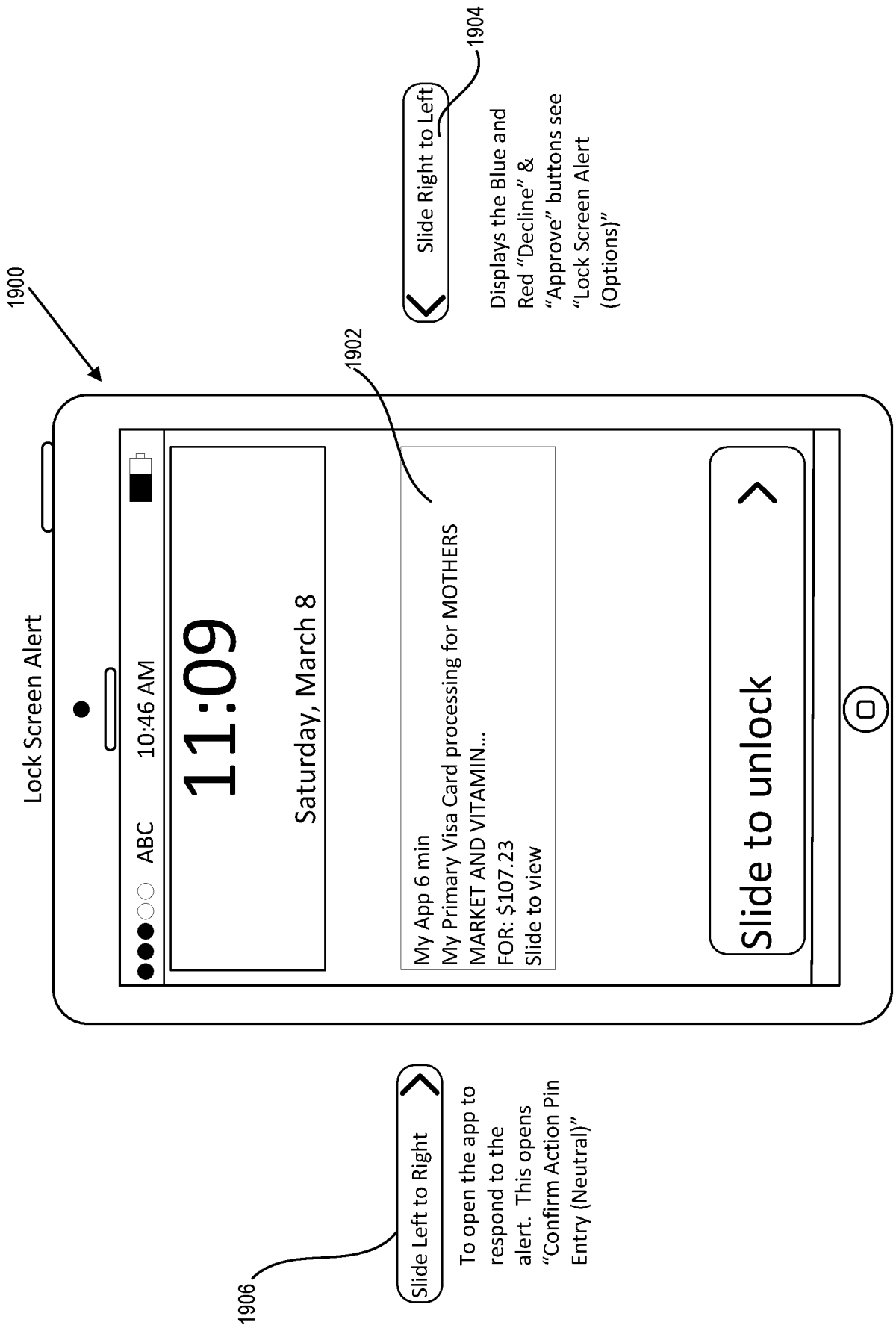
1900
Lock Screen Alert
ABC
10:46 AM
11:09
Saturday, March 8
1902
My App 6 min
My Primary Visa Card processing for MOTHERS MARKET AND VITAMIN...
FOR: $107.23
Slide to view
Slide to unlock
1904
Slide Right to Left
Displays the Blue and Red "Decline" & "Approve" buttons see "Lock Screen Alert (Options)"
1906
Slide Left to Right
To open the app to respond to the alert. This opens "Confirm Action Pin Entry (Neutral)"

FIG. 19

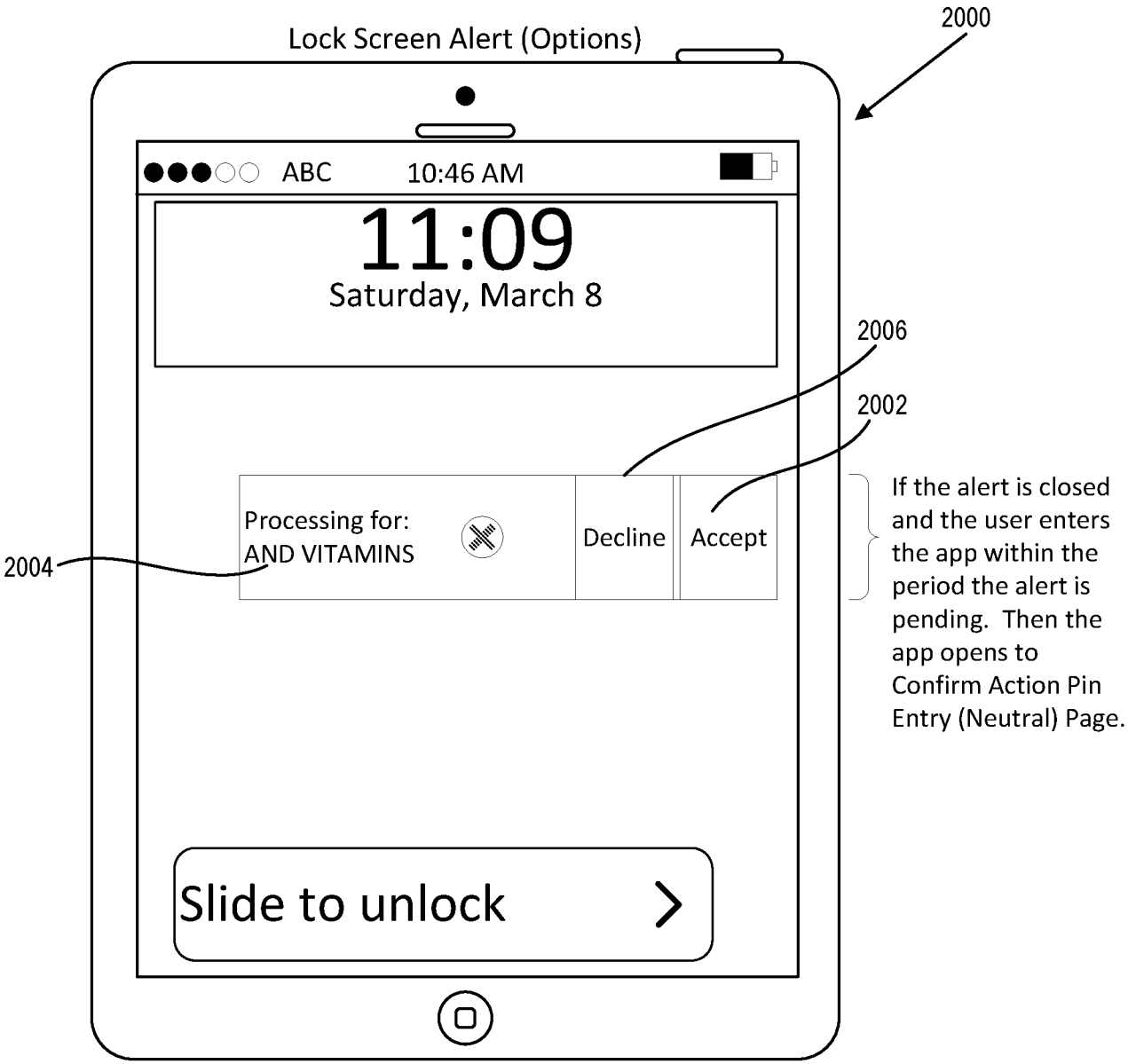
Lock Screen Alert (Options)
2000
ABC
10:46 AM
11:09
Saturday, March 8
2006
2002
Processing for:
AND VITAMINS
Decline
Accept
2004
If the alert is closed and the user enters the app within the period the alert is pending. Then the app opens to Confirm Action Pin Entry (Neutral) Page.
Slide to unlock

FIG. 20

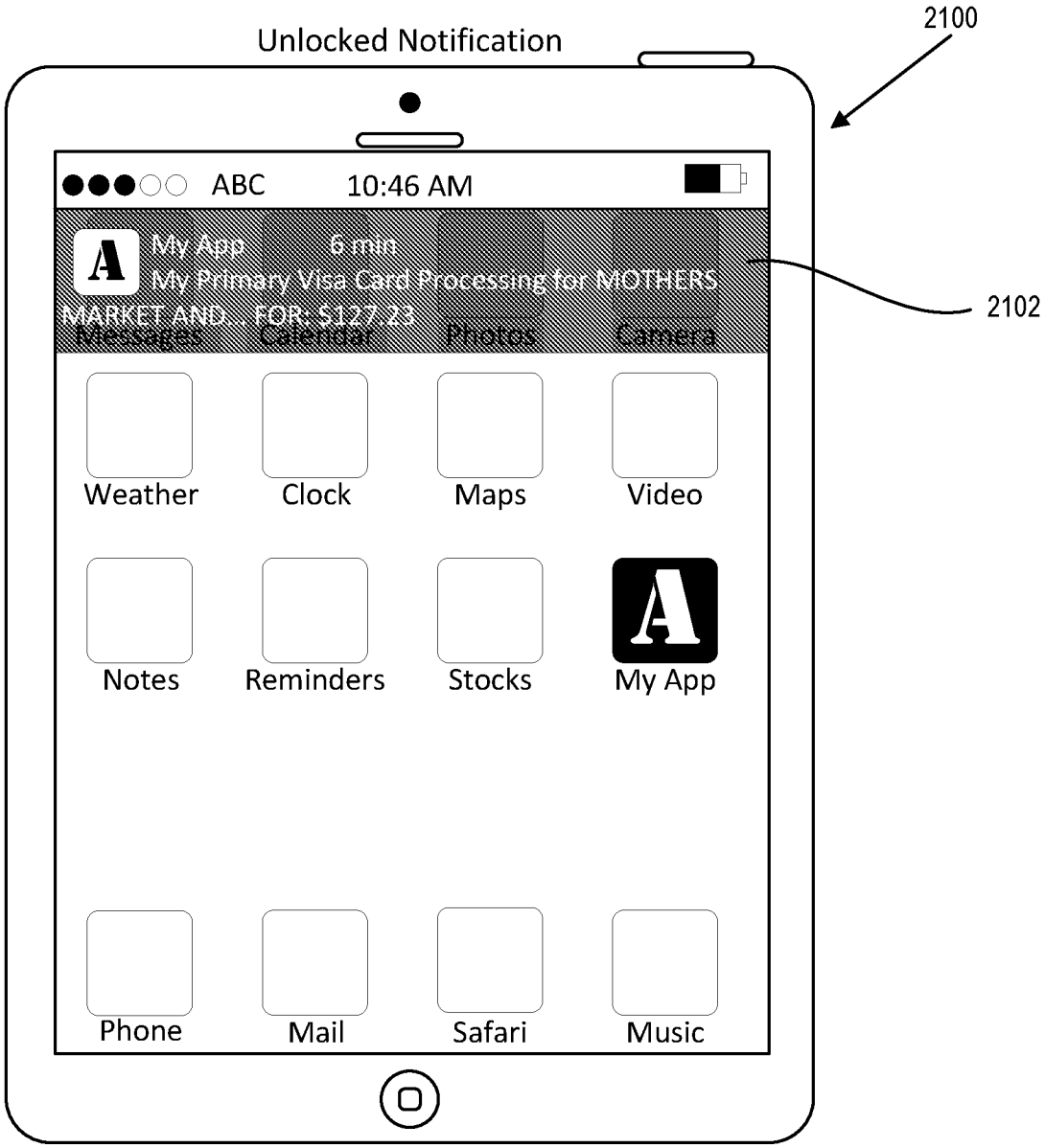
Unlocked Notification
2100
ABC
10:46 AM
My App
6 mins
My Primary Visa Card Processing for MOTHERS
MARKET AND FOR: 5127.23
2102
Messages
Calendar
Photos
Camera
Weather
Clock
Maps
Video
Notes
Reminders
Stocks
My App
Phone
Mail
Safari
Music

FIG. 21

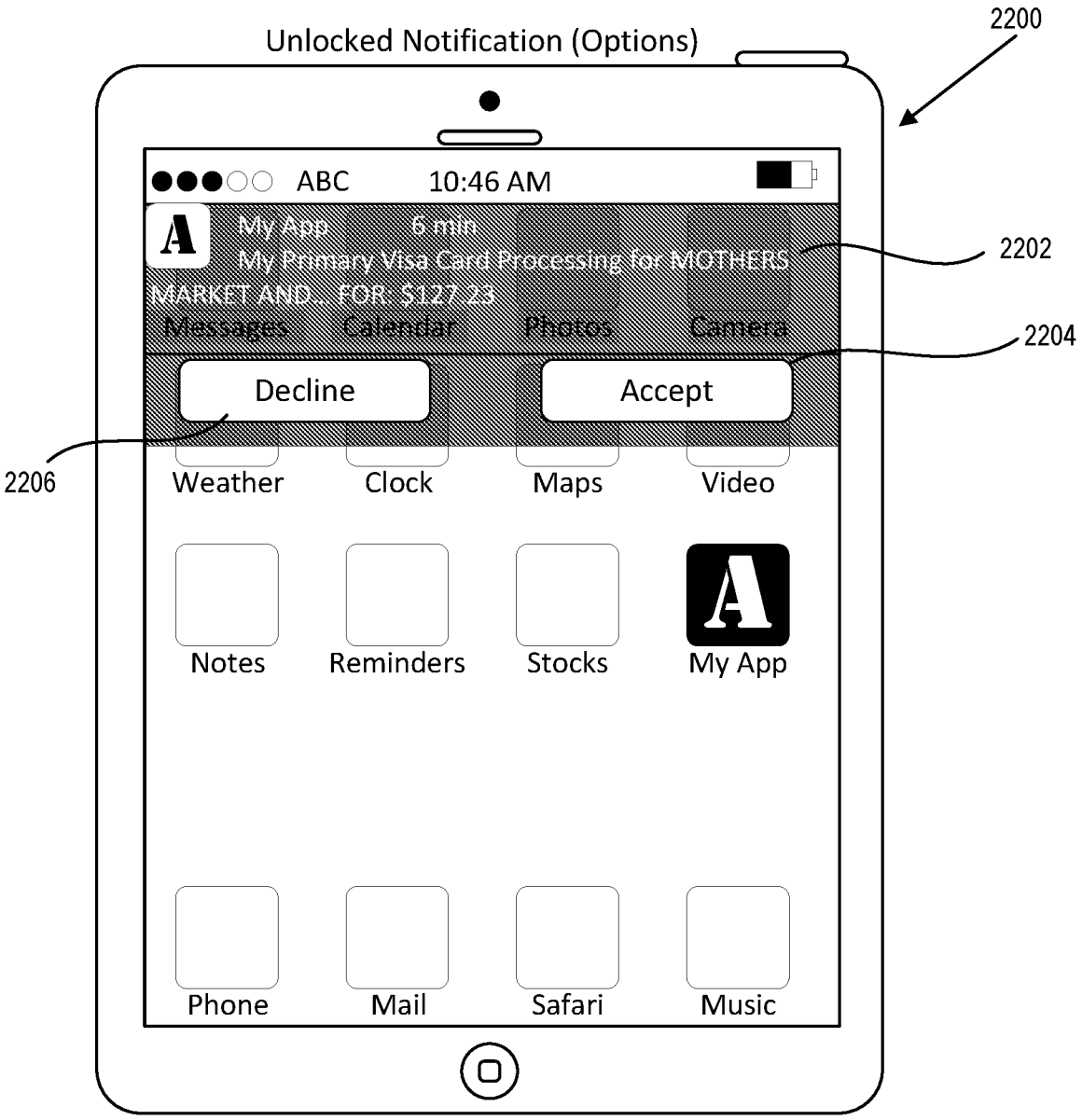
Unlocked Notification (Options)
2200
ABC
10:46 AM
My App
6 min
My Primary Visa Card Processing for MOTHERS
MARKET AND... FOR: $127.23
2202
Messages
Calendar
Photos
Camera
2204
Decline
Accept
2206
Weather
Clock
Maps
Video
Notes
Reminders
Stocks
My App
Phone
Mail
Safari
Music

FIG. 22

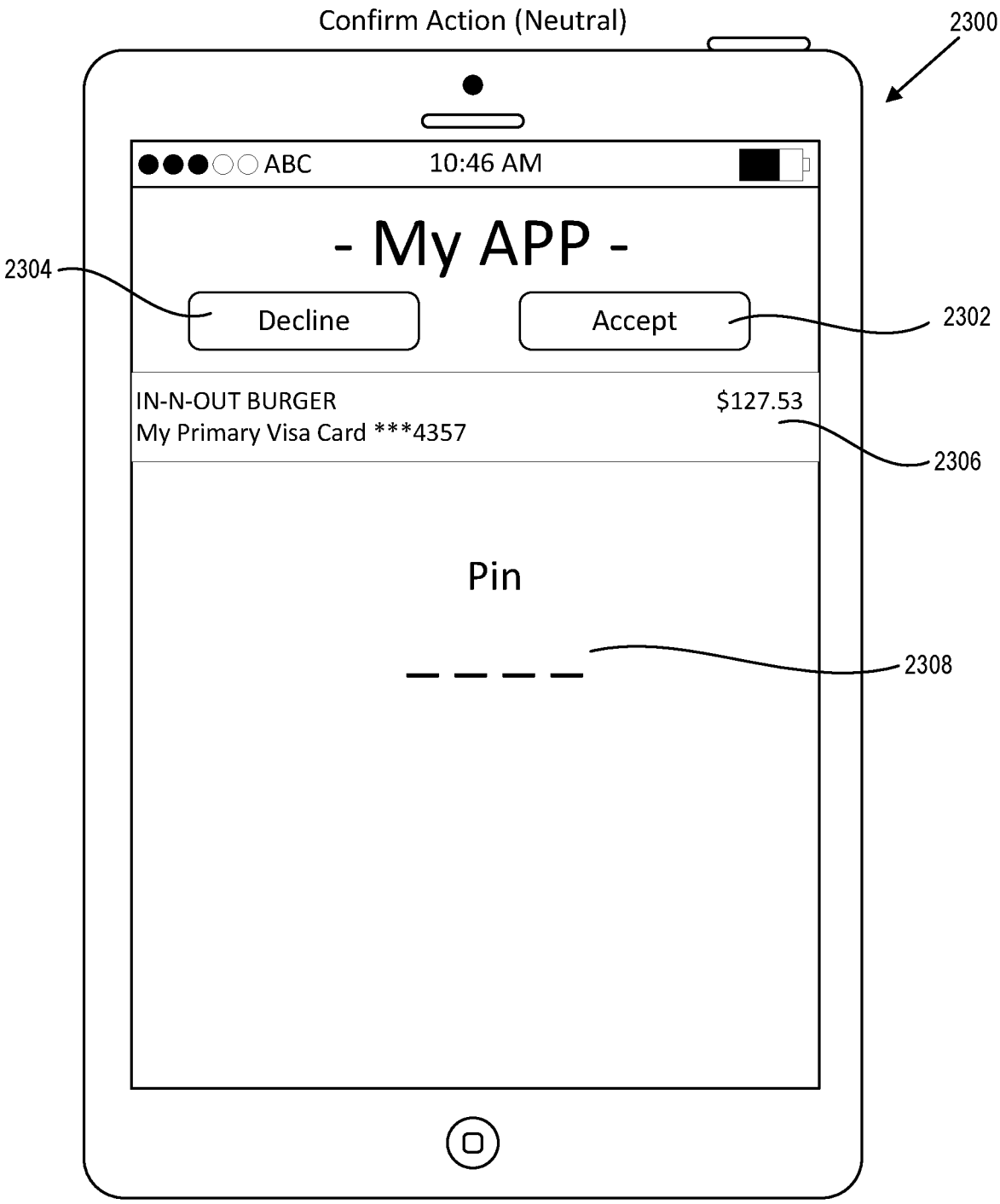
Confirm Action (Neutral)
2300
ABC
10:46 AM
- My APP -
2304
Decline
Accept
2302
IN-N-OUT BURGER
$127.53
My Primary Visa Card ***4357
2306
Pin
2308

FIG. 23

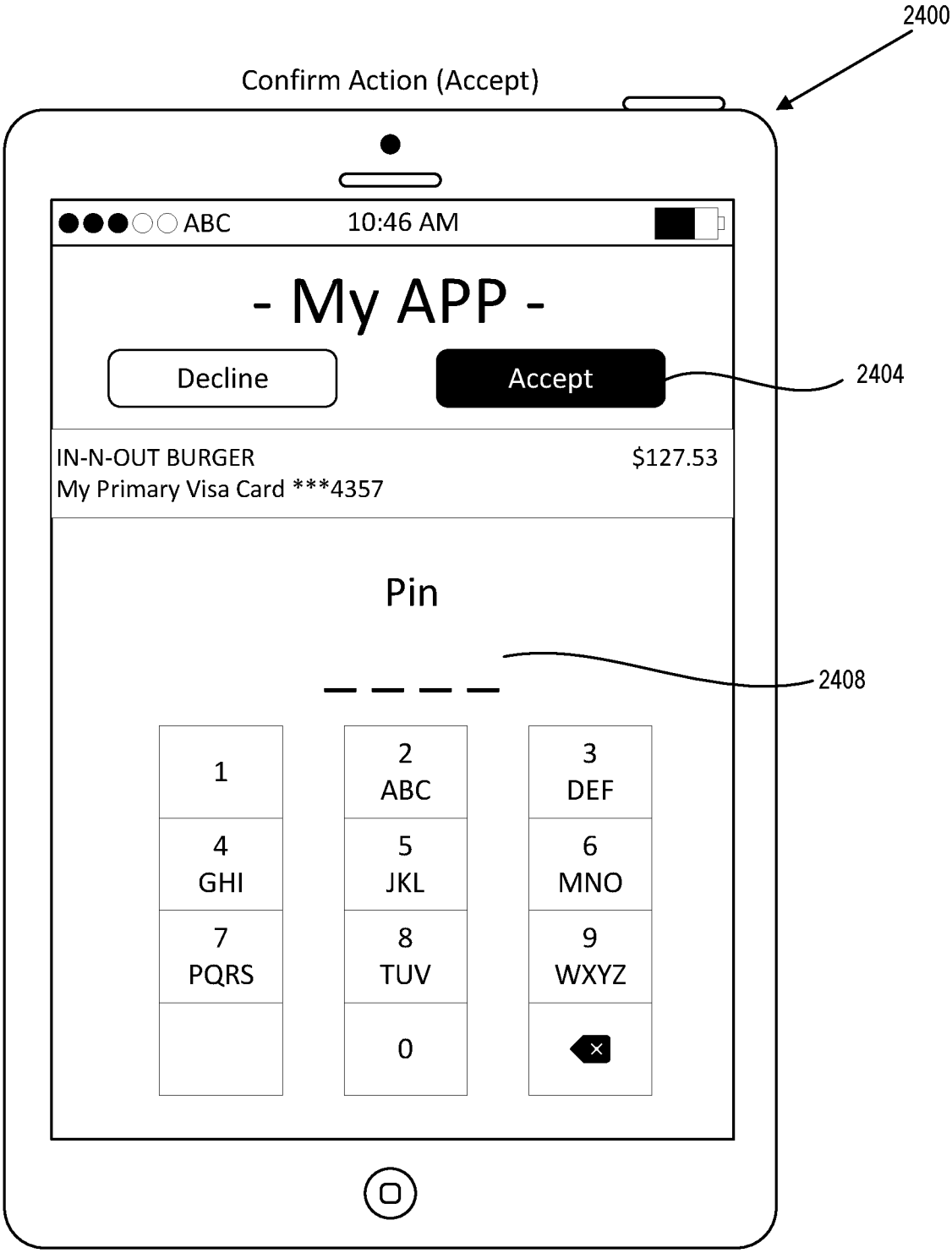
2400
Confirm Action (Accept)
ABC
10:46 AM
- My APP -
Decline
Accept
2404
IN-N-OUT BURGER
$127.53
My Primary Visa Card ***4357
Pin
2408
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

FIG. 24

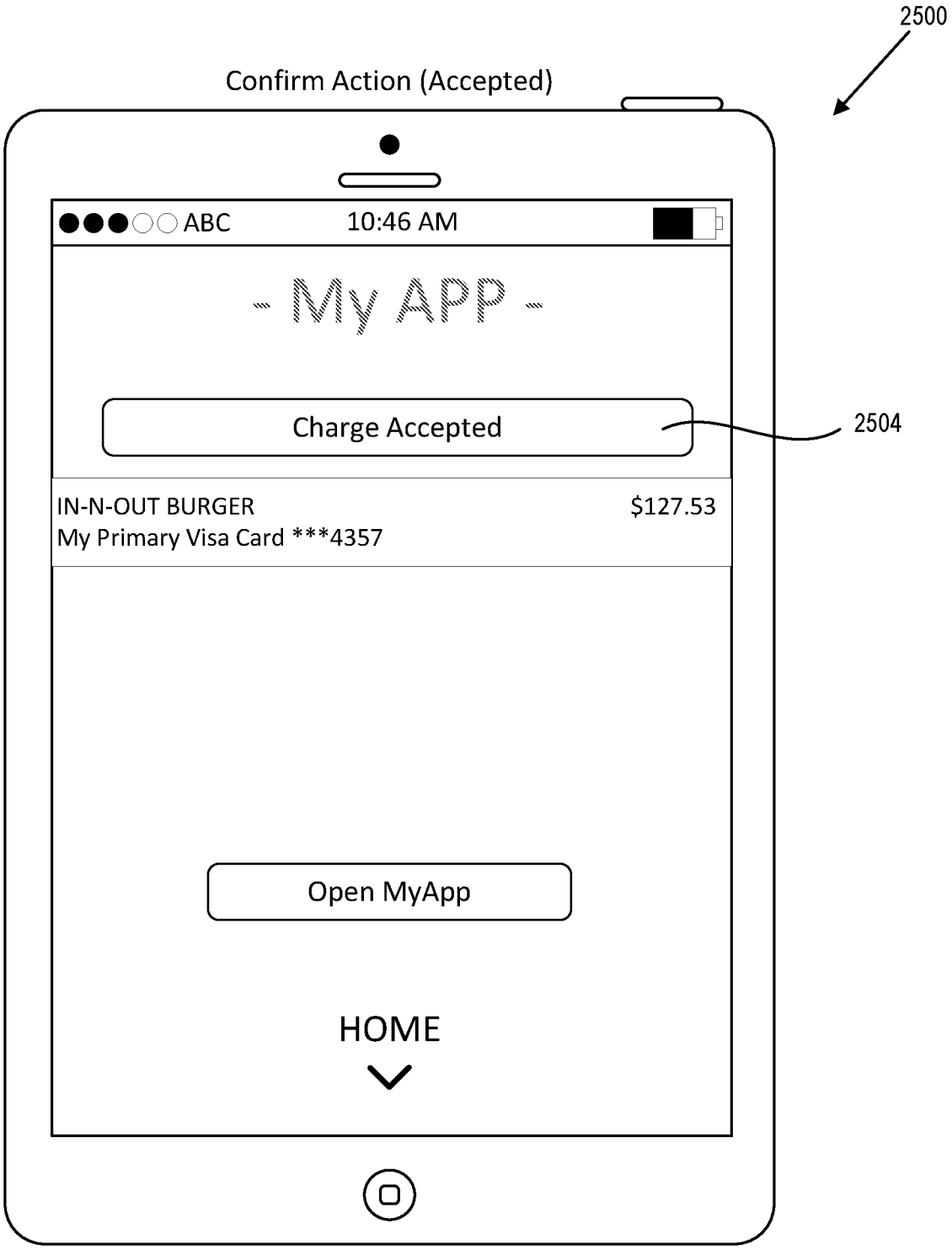
2500
Confirm Action (Accepted)
ABC
10:46 AM
- My APP -
Charge Accepted
2504
IN-N-OUT BURGER
$127.53
My Primary Visa Card ***4357
Open MyApp
HOME

FIG. 25

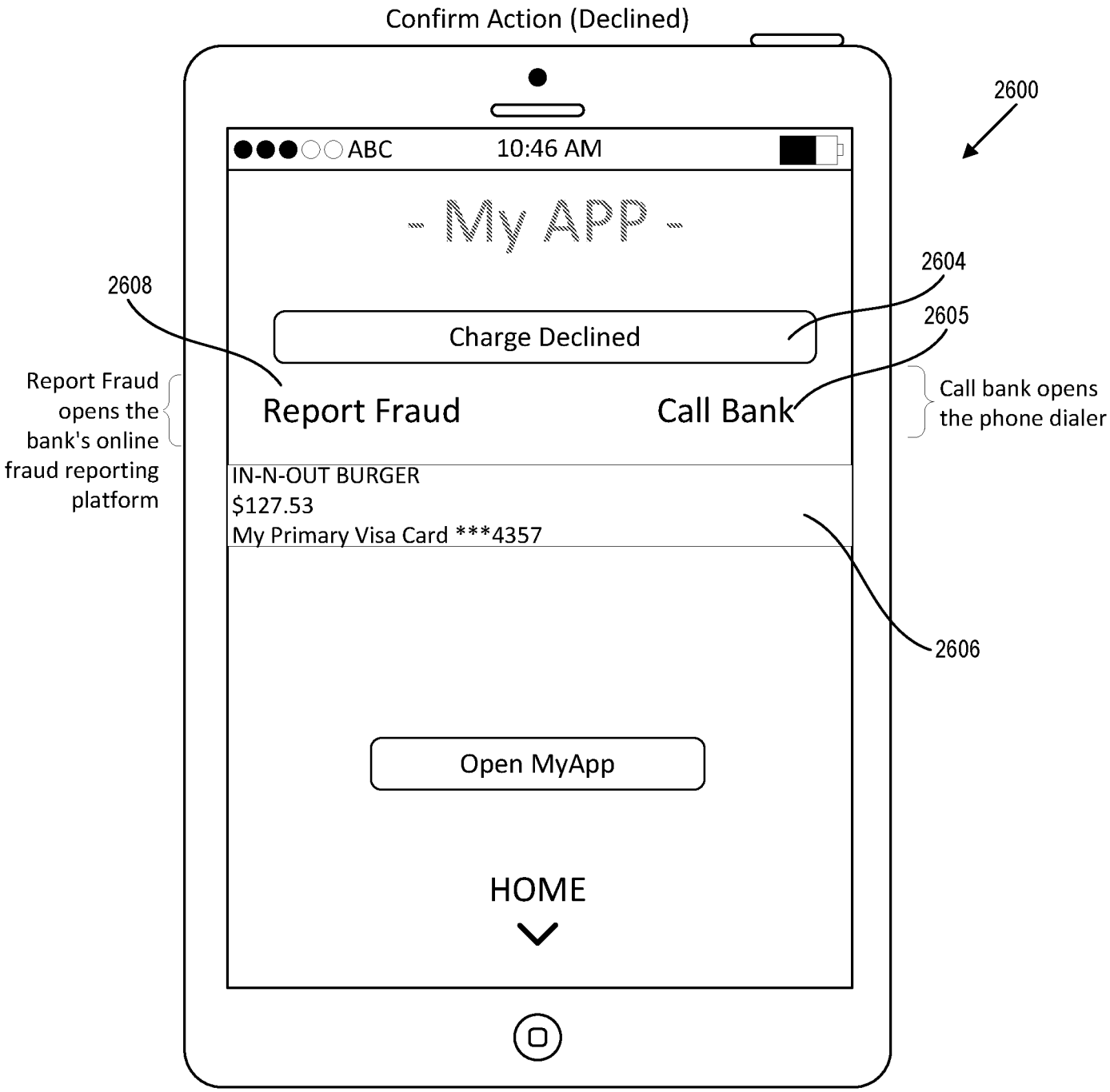
Confirm Action (Declined)
2600
ABC
10:46 AM
- My APP -
2604
2608
2605
Charge Declined
Report Fraud opens the bank's online fraud reporting platform
Report Fraud
Call Bank
Call bank opens the phone dialer
IN-N-OUT BURGER
$127.53
My Primary Visa Card ***4357
2606
Open MyApp
HOME

FIG. 26

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2015/050084

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/32 (2012.01) G06Q 20/40 (2012.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, IPC G06Q20, FREE PATENTS ONLINE:

MOBILE, CELLULAR, CARD, APPROVAL, CONSENT, ACCEPTANCE, REJECT, DECLINE, DISAPPROVAL, REFUSAL and the like terms with Applicant(s)/Inventor(s) name searched in internal databases provided by IP Australia.

.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [ ] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 October 2015	30 October 2015
Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	Boris Cetinich AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. 0399359619

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/MY2015/050084**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2014/073997 A1 (MASSPAY SP. Z.O.O.) 15 May 2014 abstract, pages 1-8 and claims 1-6	1-20
X	US 2014/0379504 A1 (GEORGE) 25 December 2014 abstract, paragraphs 31-34 and claim 5	1-20
X	US 2008/0189186 A1 (CHOI et al.) 07 August 2008 abstract, paragraphs 19-23 and 60-67	1-20
X	US 2014/0297435 A1 (WONG) 02 October 2014 abstract, paragraphs 4-5 and 33-34	1-20
X	EP 2 648 148 A2 (LG CNS CO LTD) 09 October 2013 abstract, claims 1-9 and figure 4	1-20
X	US 2002/0169713 A1 (CHANG et al.) 14 November 2002 abstract, claims 1-12 and figure 3	1-20
X	US 2001/0034707 A1 (SAKAGUCHI) 25 October 2001 abstract, claims 1-7 and figures 2-3	1-20