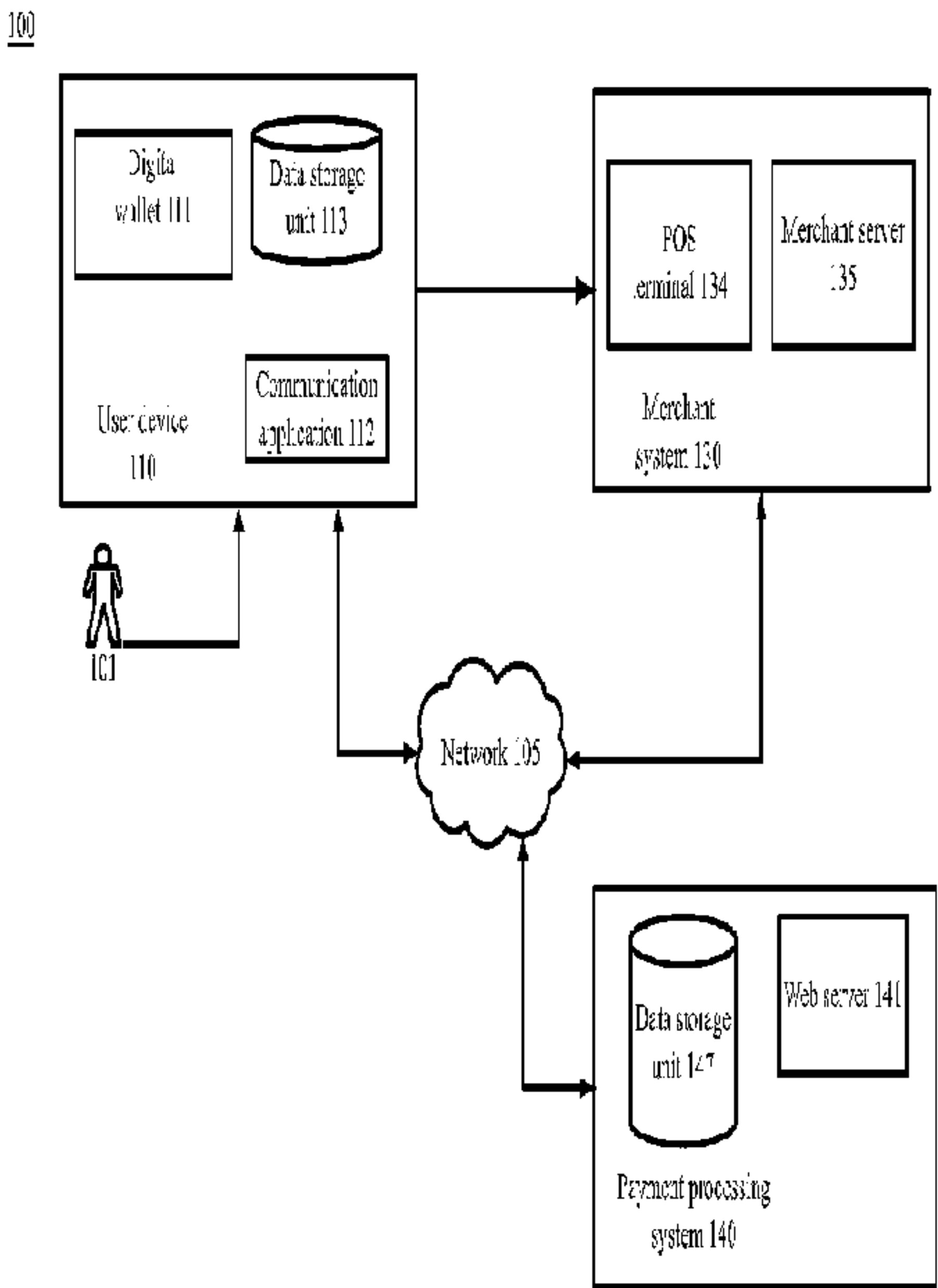




(86) Date de dépôt PCT/PCT Filing Date: 2015/01/23
(87) Date publication PCT/PCT Publication Date: 2015/08/13
(45) Date de délivrance/Issue Date: 2019/10/08
(85) Entrée phase nationale/National Entry: 2016/08/05
(86) N° demande PCT/PCT Application No.: US 2015/012784
(87) N° publication PCT/PCT Publication No.: 2015/119796
(30) Priorité/Priority: 2014/02/06 (US14/174,828)

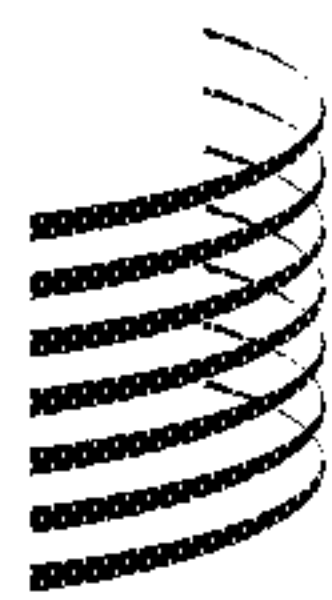
(51) Cl.Int./Int.Cl. *G06Q 20/36* (2012.01),
G06Q 20/38 (2012.01), *G06Q 20/40* (2012.01)
(72) Inventeurs/Inventors:
BRICKELL, JUSTIN LEE, US;
MAHADEVAN, SWAMINATHAN, US;
BUTLER, HARRY LEE, IV, US;
WIELER, BOBBY, US;
BLANCO, IGNACIO CARLOS, US
(73) Propriétaire/Owner:
GOOGLE LLC, US
(74) Agent: GOWLING WLG (CANADA) LLP

(54) Titre : ALTERATION DYNAMIQUE DE DONNEES DE SUIVI
(54) Title: DYNAMIC ALTERATION OF TRACK DATA



(57) **Abrégé/Abstract:**
Using discretionary data fields to secure transactions comprises a payment system employing a server configured to associate a payment account of a user with a user computing device, the payment account comprising a payment account identifier that identifies the payment account, and establish a authentication challenge and an corresponding challenge response. The payment system receives a first payment authorization request originating from a merchant computing system comprising the payment account identifier, data associated with the payment account identifier, and a request to fund a transaction using the payment account, wherein the data associated with the payment account identifier comprises a challenge response provided by the user computing device located in a discretionary data field. The payment system compares the provided challenge response with the corresponding challenge response, and approves the transaction based on whether the provided challenge response and the corresponding challenge response match.

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

(19) World Intellectual Property
Organization
International Bureau

WIPO | PCT

(10) International Publication Number
WO 2015/119796 A1(43) International Publication Date
13 August 2015 (13.08.2015)

(51) International Patent Classification:

G06Q 20/36 (2012.01) *G06Q 20/38* (2012.01)
G06Q 20/40 (2012.01)

(21) International Application Number:

PCT/US2015/012784

(22) International Filing Date:

23 January 2015 (23.01.2015)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

14/174,828 6 February 2014 (06.02.2014) US

(71) Applicant: **GOOGLE INC.** [US/US]; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).(72) Inventors: **BRICKELL, Justin, Lee**; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US). **MAHADEVAN, Swaminathan**; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US). **BUTLER, Harry, Lee, IV**; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US). **WIELER, Bobby**; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US). **BLANCO, Ignacio, Carlos**; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).(74) Agent: **ISAACS, William, O., II**; Johnson, Marcou & Isaacs, LLC, 317A E. Liberty Street, Savannah, GA 31401 (US).(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, 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).

[Continued on next page]

(54) Title: DYNAMIC ALTERATION OF TRACK DATA

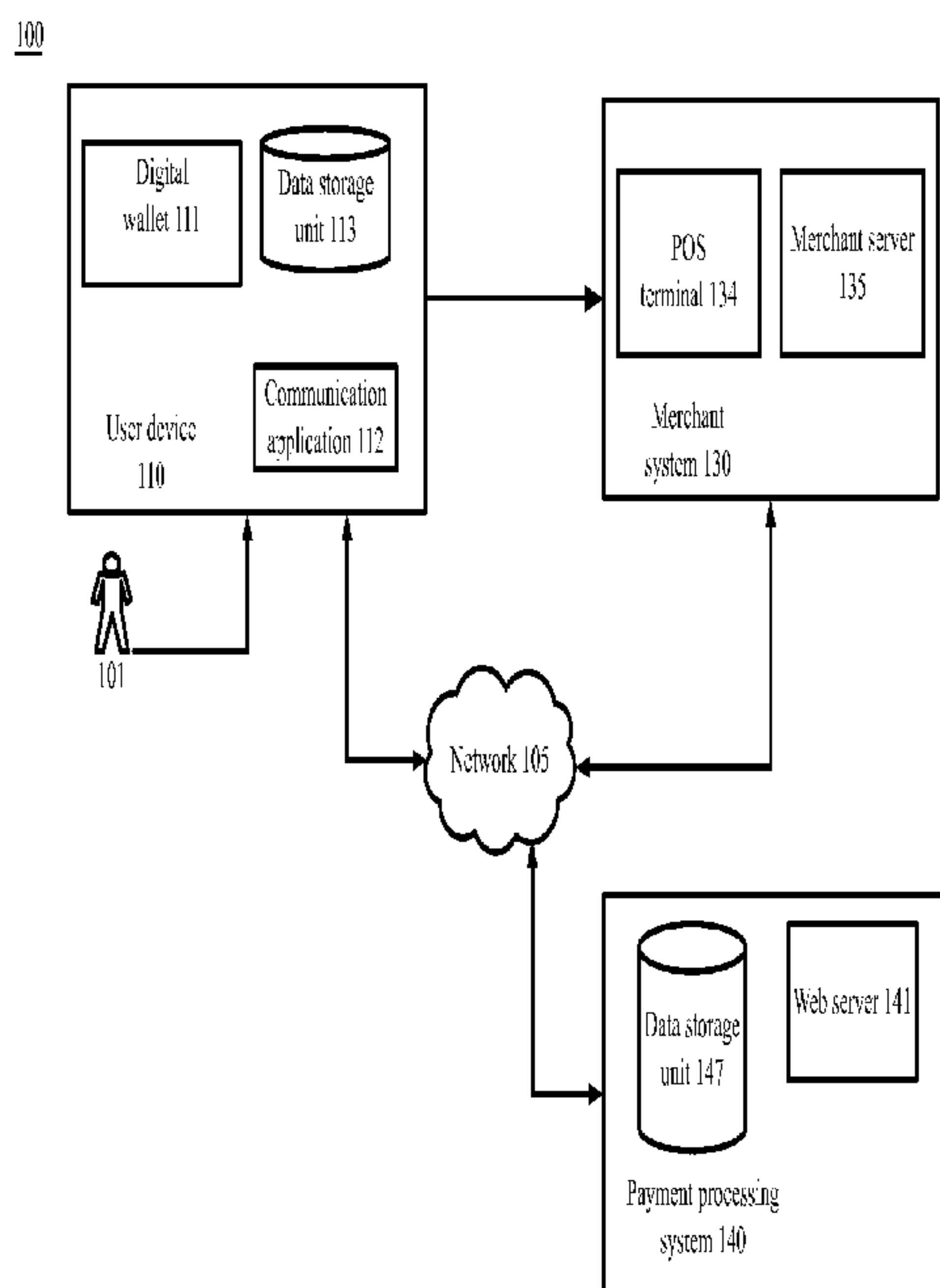


Fig. 1

(57) Abstract: Using discretionary data fields to secure transactions comprises a payment system employing a server configured to associate a payment account of a user with a user computing device, the payment account comprising a payment account identifier that identifies the payment account, and establish a authentication challenge and an corresponding challenge response. The payment system receives a first payment authorization request originating from a merchant computing system comprising the payment account identifier, data associated with the payment account identifier, and a request to fund a transaction using the payment account, wherein the data associated with the payment account identifier comprises a challenge response provided by the user computing device located in a discretionary data field. The payment system compares the provided challenge response with the corresponding challenge response, and approves the transaction based on whether the provided challenge response and the corresponding challenge response match.

WO 2015/119796 A1

Published:

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

DYNAMIC ALTERATION OF TRACK DATA

TECHNICAL FIELD

[0001] The present disclosure relates generally to digital wallet account transactions, and more particularly to using discretionary data fields to secure transactions.

BACKGROUND

[0002] Digital wallet accounts on payment processing systems enable users to utilize a user computing device to conduct transactions. A user applies the wallet account to a transaction with the merchant's point-of-sale system via near field communication, WI-Fi, Bluetooth, infrared, or in any suitable manner. The payment processing system can utilize the provided financial account to conduct the transaction with the merchant.

[0003] Digital wallet accounts and user computing devices often have certain authorization and authentication procedures to reduce fraud. For example, a user computing device may require a password to access the digital wallet application module. However, conventional systems do not allow the user computing device to provide security information to a payment processing system via the discretionary data field on a payment instrument.

SUMMARY

[0004] Techniques herein provide a computer-implemented method to use discretionary data fields to secure transactions. A payment system employs a server configured to associate a payment account of a user with a user computing device, the payment account comprising a payment account identifier that identifies the payment account, and to establish an authentication challenge and a corresponding challenge response. The payment system receives a first payment authorization request originating from a merchant computing system, the first payment authorization request comprising the payment account identifier, data associated with the payment account identifier, and a request to fund a transaction using the payment account, wherein the data associated with the payment account identifier comprises a challenge response provided by the user computing device located in a discretionary data field. The payment system compares

the provided challenge response with the corresponding challenge response, and replies to the merchant computing system with a responsive authorization state, wherein the responsive authorization state is determined based on the determination whether the provided challenge response and the corresponding challenge response match.

[0005] In certain other example aspects described herein, a system and a computer program product to use discretionary data fields to secure transactions.

[0006] These and other aspects, objects, features, and advantages of the example embodiments will become apparent to those having ordinary skill in the art upon consideration of the following detailed description of illustrated example embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Figure 1 is a block diagram depicting a system for using discretionary data fields to secure transactions, in accordance with certain example embodiments.

[0008] Figure 2 is a block flow diagram depicting a method for using discretionary data fields to secure transactions, in accordance with certain example embodiments.

[0009] Figure 3 is a block flow diagram depicting a method for the user computing device to communicate payment account information to the merchant POS terminal in the discretionary data field of the payment account information, in accordance with certain example embodiments.

[0010] Figure 4 is an illustration of a user computing device requesting an authentication response, in accordance with certain example embodiments.

[0011] Figure 5 is a block diagram depicting a computing machine and a module, in accordance with certain example embodiments.

DETAILED DESCRIPTION OF THE EXAMPLE EMBODIMENTS

Overview

[0012] In one example embodiment, a user attempts a transaction with a merchant point of sale (“POS”) terminal. When the user selects a payment instrument, such as a credit card, to use, a digital wallet communicates with a payment processing system to obtain an authentication challenge. In certain embodiments, the authentication challenge resides in the user computing device, and the payment processing system does not need

to be contacted. The digital wallet populates a discretionary data field of the payment instrument being used with a challenge response. The payment instrument information, including the discretionary data field, is transmitted to a POS terminal to conduct the transaction. The POS terminal communicates the transaction request to the payment processing system. The payment processing system accesses the challenge response from the discretionary data field. If the challenge response is acceptable, then the transaction proceeds.

[0013] In one example embodiment of a wallet account, payment processing systems enable users to utilize a payment account to conduct transactions. The user associates one or more financial accounts with the wallet account. For example, the user can associate with the user's wallet account one or more debit/credit cards maintained by multiple issuers (including the payment processing system operating as an issuer), stored value cards (for example, gift cards, prepaid cards, re-loadable transaction cards, exchange cards, and other forms of non-credit based value cards), loyalty cards or other store rewards cards, value added service accounts (for example, coupons, vouchers for prepaid offers, redemption offers, and other forms of offers), peer-to-peer transaction accounts, bank accounts and/or other forms of financial accounts.

[0014] The wallet account can be represented on a digital wallet application module or other payment application on a user computing device, such as a mobile phone. For example, the user wallet account information, such as a wallet account identifier, can be stored on the user computing device for use in a payment transaction by the digital wallet application module or other application.

[0015] To conduct a transaction using a wallet account on a user computing device, the user can communicate the wallet account identifier and other transaction data to a merchant point of sale ("POS") terminal using the user computing device via near field communication ("NFC"), barcode, BLUETOOTH, Wi-Fi communication, infrared, or other suitable communication technology. Alternatively, the wallet account can have thereto associated a physical payment card comprising a magnetic stripe or other machine-readable portion comprising the user's wallet account identifier and other payment information. In this case, the user scans or swipes the wallet account at the merchant POS terminal to communicate the wallet account identifier and other

transaction data to the merchant POS terminal. Additionally or alternatively, the wallet account can be represented as any other suitable payment instrument, such as an RFID device or a smartcard. Additionally or alternatively, the payment account can be a digital wallet application module or other payment account on a user computing device for conducting online transactions, such as a mobile or desktop computer, laptop computer, or a television with one or more processors embedded therein and/or coupled thereto.

[0016] Continuing the example of a conventional transaction, the merchant system creates a payment request for the transaction using the wallet account information and forwards the payment request to an acquirer, which forwards the payment request to a card network. The card network forwards the payment request to the payment processing system, which may function as the issuer of the payment instrument for the payment request.

[0017] The payment processing system reads wallet account information from the payment request and accesses the user's account associated with the wallet account. If the payment processing system is the issuer of the particular financial account selected as the backing account for the wallet account transaction, the payment processing system will approve or decline the transaction.

[0018] If another issuer maintains the particular financial account to be used as the backing account for the transaction, the payment processing system will generate and send a new payment request for the transaction to the other issuer via the card network (or via a different card network). The payment processing system receives an authorization message from the other issuer via the card network if the transaction is approved.

[0019] The payment processing system forwards an authorization to the acquirer through the card network, which forwards the authorization to the merchant system. The authorization is based on the payment processing system's determination as the issuer to authorize the transaction or the authorization received from the other issuer.

[0020] The merchant system then approves the transaction, based on the authorization received from the payment processing system.

[0021] In certain example embodiments, the user and/or the payment processing system establish a security procedure for transactions. The security procedure may be a

particular challenge and response, an interrogation of the user computing device, a location verification, or any suitable procedure. The details of example security procedures will be described herein.

[0022] In an example embodiment, the user initiates a purchase at a merchant location. The user opens the digital wallet application module executing on the user computing device. The digital wallet application module represents any application or other user interface system the user employs to conduct wallet account and other transactions via the user computing device. The user accesses the wallet account of the user via the digital wallet application module.

[0023] The user can select a payment account associated with the wallet account to be the used for the subsequent transaction. In certain embodiments, at the time that a user indicates that a transaction is imminent, such as by opening the digital wallet application module, the user computing device accesses the authentication challenge that has been configured for the account. In one example embodiment, the authentication challenge is stored in the digital wallet application module, on the secure element, in other memory, or in any suitable location on the user computing device. In an alternate example embodiment, at the time that a user indicates that a transaction is imminent, the user computing device contacts the payment processing system to request an authentication challenge. The user computing device may contact the payment processing system over the Internet via a Wi-Fi signal, a cellular communication, an email, a text, or any suitable communication technology. When contacted, the payment processing system transmits the authentication challenge to the user computing device.

[0024] In alternate example embodiments, the user computing device accesses the authentication challenge after the merchant POS terminal provides a transaction request to the user computing device. For example, the POS terminal receives an initiation of a transaction and transmits a request to the user computing device to provide payment information. At the time of the request from the POS terminal, the user computing device may access the authentication challenge or request the authentication challenge from the payment processing system.

[0025] The authentication challenge may be a challenge/response question for the user. For example, the challenge may be a question for which an answer has been

previously configured with the payment processing system. One example question may be “what is your mother’s maiden name?” Another question may be “In what city were you born?” Any suitable question may be used. The challenge question may be displayed on the user interface of the user computing device. The user enters the appropriate response into the user interface of the user computing device. The response must be stored on the device and or at the payment processing system if configured prior to the transaction.

[0026] In another example, the authentication challenge may be directed to the user computing device. For example, the challenge may be a request for the identification number of the user computing device, the model number of the user computing device, or a similar request. In another example, the payment processing system may request the location of the user computing device. The location may be accessed from a global positioning system (“GPS”) technology on the user computing device, from a Wi-Fi location technology, or any suitable technology. In another example, data from the transaction history of the user computing device may be used. For example, the time or location of the last successful transaction may be requested.

[0027] The user computing device communicates payment account information to the merchant point of sale (“POS”) system, comprising the wallet account identification and challenge response. For example, the user can select a product for purchase at a merchant location and conduct the purchase transaction at a POS terminal of the merchant system.

[0028] The wallet account information that is stored in the digital wallet application module on the user computing device is used to make a payment to the merchant. The wallet account information is transmitted to the POS terminal via NFC, Bluetooth, barcode displayed via the user computing device, Wi-Fi, or other form of communication. The user can initiate the communication by performing a wireless “tap” of the user computing device with the POS terminal or any other suitable action, such as by actuating a real or virtual button on the user computing device or speaking a command into the user computing device. In an alternative example embodiment, a purchase is initiated by use of an RFID device, smartcard, barcode displayed on the user computing device, or other suitable medium that can be read by the POS terminal.

[0029] When a transaction is initiated, the digital wallet application module can access the wallet account information residing in the digital wallet application module or other secured or unsecured storage in the user computing device, including the challenge response. If a challenge response has been supplied by the user or by the user computing device, then the digital wallet application module includes the response in the transaction details being transmitted to the POS terminal. The response may be transmitted in a discretionary data field of the wallet account information. As the challenge response may be located in a discretionary data field, the challenge response is not utilized by the merchant system or the POS terminal; however, the challenge response information is still communicated to the payment processing system by the merchant system.

[0030] In an example embodiment, the challenge response is the answer provided by the user to a challenge question. In another example, the challenge response is a GPS location of the user computing device. In another example, the challenge response is an identification number of the user computing device. In another example, the challenge response is specific transaction related data that was requested from the user computing device, such as the time of the last transaction.

[0031] A payment authorization request is communicated to the payment processing system from the POS terminal. The request includes the wallet account identification and challenge response. The POS terminal communicates a payment authorization request to the payment processing system to obtain payment for the purchase transaction between the user and the merchant. The payment authorization request comprises transaction details, such as the product being purchased, the total price, the merchant system information, the wallet account information, and other suitable data.

[0032] The payment processing system receives the payment authorization request and determines if the challenge response is accepted. Along with the wallet account information, the payment processing system identifies the challenge response from the provided data. The payment processing system accesses the wallet account of the user based on the wallet account information provided in the request and determines if the challenge response is appropriate. For example, the payment processing system can determine if an answer provided by the user matches the configured expected answer. In an example, the expected answer to the question "What is your mother's maiden name?"

is “Jones.” If the user answered “Jones,” and the answer was transmitted to the payment processing system, then the payment processing system determines that the challenge response is accepted.

[0033] In another example, the challenge response is the GPS location of the user computing device. The payment processing system determines the expected GPS location of the user computing device based on the location of the merchant identified in the transaction details. For example, the user computing device identifies the merchant and accesses the location of the merchant from a database of merchant locations. The payment processing system compares the location of the merchant with the location of the user computing device. If the locations match, then the payment processing system determines that the user computing device is located at the merchant and the likelihood of a fraudulent transaction is reduced.

[0034] In another example, the challenge response is a detail from a recent transaction. The user computing device determines the last transaction conducted by the user with the user computing device and extracts a particular detail, such as the time of the last transaction. The payment processing system compares the time of the last transaction of the user computing device with the time of the last transaction stored in a memory of the payment processing system. If the times match, then the payment processing system determines that the user computing device is the same user computing device previously used and the likelihood of a fraudulent transaction is reduced.

[0035] Any suitable response to a suitable challenge may be provided. For example, an identification number of the user computing device or a personal identification number.

[0036] If the wallet account on the payment processing system functions as a proxy account, then the payment processing system can initiate a second transaction with an issuer of the selected backing account to fund the merchant transaction. The payment processing system can transmit an approval or refusal of the transaction to the merchant system, based on approval or refusal of the transaction with the selected backing account.

[0037] The payment processing system approves the transaction based on transaction details and challenge response. If the challenge response is accepted and the transaction is approved, then the payment processing system transmits the approval to the POS

terminal. The merchant system receives the approval, provides the purchased product or service to the user, and logs the transaction. The transaction funds are remitted to the merchant system.

Example System Architectures

[0038] Turning now to the drawings, in which like numerals represent like (but not necessarily identical) elements throughout the figures, example embodiments are described in detail.

[0039] Figure 1 is a block diagram depicting a system for using discretionary data fields to secure transactions, in accordance with certain example embodiments. In some embodiments, a user associated with a device must install an application and/or make a feature selection to obtain the benefits of the techniques described herein.

[0040] As depicted in Figure 1, the system 100 includes network computing devices 110, 130, and 140 that are configured to communicate with one another via one or more networks 105 or via any suitable communication technology.

[0041] Each network 105 includes a wired or wireless telecommunication means by which network devices (including devices 110, 130, and 140) can exchange data. For example, each network 105 can include a local area network (“LAN”), a wide area network (“WAN”), an intranet, an Internet, a mobile telephone network, storage area network (SAN), personal area network (PAN), a metropolitan area network (MAN), a wireless local area network (WLAN), a virtual private network (VPN), a cellular or other mobile communication network, Bluetooth, NFC, or any combination thereof or any other appropriate architecture or system that facilitates the communication of signals, data. Throughout the discussion of example embodiments, it should be understood that the terms “data” and “information” are used interchangeably herein to refer to text, images, audio, video, or any other form of information that can exist in a computer-based environment. The communication technology utilized by the devices 110, 130, and 140 may be similar networks to network 105 or an alternative communication technology.

[0042] Each network computing device 110, 130, and 140 includes a device having a communication module capable of transmitting and receiving data over the network 105 or a similar network. For example, each network device 110, 130, and 140 can include a

server, desktop computer, laptop computer, tablet computer, a television with one or more processors embedded therein and / or coupled thereto, smart phone, handheld computer, personal digital assistant (“PDA”), or any other wired or wireless, processor-driven device. In the example embodiment depicted in Figure 1, the network devices 110, 130, and 140 are operated by end-users or consumers, merchant system operators, and payment processing system operators, respectively.

[0043] The user 101 can use the communication application 112, which may be, for example, a web browser application or a stand-alone application, to view, download, upload, or otherwise access documents or web pages via a distributed network 105. The communication application 112 can interact with web servers or other computing devices connected to the network 105, including the point of sale terminal 134 of the merchant system 130, the merchant server 135 of the merchant system 130, and the web server 144 of the payment processing system 140.

[0044] The user network device 110 may include a digital wallet application module 111. The digital wallet application module 111 may encompass any application, hardware, software, or process the user computing device 110 may employ to assist the user 101 in completing a purchase. The digital wallet application module 111 can interact with the communication application 112 or can be embodied as a companion application of the communication application 112. As a companion application, the digital wallet application module 111 executes within the communication application 112. That is, the digital wallet application module 111 may be an application program embedded in the communication application 112. The digital wallet application module 111 may use a wallet account of the user 101 that is managed by the payment processing system 140 or another suitable system. The wallet account may execute on the user computing device 110 independent of the digital wallet application module 111 and the communication application 112.

[0045] The wallet account may allow the user 101 to set rules, confirm transactions, select preferred accounts for a transaction, receive notice of a account selection, and provide other suitable services. Any functions of the wallet account can be performed on the digital wallet application module 111. Additionally or alternatively, any function of

the wallet account and the digital wallet application module 111 can be performed on or by the payment processing system 140.

[0046] The user computing device 110 also includes a data storage unit 113 accessible by the digital wallet application module 111, the wallet account application 115, and the communication application 112. The example data storage unit 113 can include one or more tangible computer-readable storage devices. The data storage unit 113 can be stored on the user computing device 110 or can be logically coupled to the user computing device 110. For example, the data storage unit 113 can include on-board flash memory and/or one or more removable memory accounts or removable flash memory.

[0047] The user 101 may use the user computing device 110 or other network device to register the digital wallet application module 111 and/or access the payment processing system account of the user 101. The user computing device 110 may comprise appropriate technology that includes or is coupled to a web server.

[0048] The wallet account or other payment account can have thereto associated a magnetic stripe card. The magnetic stripe card can be a physical payment card comprising a magnetic stripe or other machine-readable portion comprising the user's wallet account identifier and other payment information. In this case, the user scans or swipes the magnetic stripe card at the merchant POS terminal 134 to communicate the wallet account identifier and other transaction data to the POS terminal 134. Additionally or alternatively, the wallet account can have thereto associated any other suitable payment instrument, such as an RFID device or a smartcard.

[0049] The payment processing system 140 includes a data storage unit 147 accessible by the web server 144. The example data storage unit 147 can include one or more tangible computer-readable storage devices. The payment processing system 140 is operable to conduct wireless and other payments between a user 101 and a merchant system 130. The payment processing system 140 is further operable to maintain a database to store transactions of the merchant system 130 and the user 101, recommend automatic payment recipients, and other suitable functions.

[0050] The user 101 can access a web server 141 on the payment processing system 140 to view, register, download, upload, or otherwise access the payment processing

system 140 via a website (not illustrated) and a communication network 105). The user 101 associates one or more registered financial accounts, including bank account debit cards, credit cards, gift cards, loyalty cards, coupons, offers, prepaid offers, store rewards cards, or other type of financial account that can be used to make a purchase or redeem value-added services with a payment account of the user 101. A financial account issuer may be the issuer of the financial account being registered. For example, the financial account issuer may be a credit card issuer, a debit card issuer, a stored value card issuer, a financial institution providing an account, or any other provider of a financial account. The payment processing system 140 also may function as the issuer for the associated financial account. The user's 101 registration information is saved in the payment processing system's 140 data storage unit 147 and is accessible the by web server 141.

[0051] The user 101 also may use the web server 141 to define payment rules. The creation of a backing account model for a user is discussed in more detail hereinafter with reference to the methods described in Figure 2.

[0052] The user 101 may request a purchase from the merchant system 130. In an example embodiment, the purchase is initiated by a wireless "tap" of the mobile device 110 with the POS terminal 134. In an alternative example embodiment, the purchase is initiated when the user 101 enters an account identification number at the POS terminal 134 or in the mobile device 110. In another alternative example embodiment, the purchase is initiated online with the merchant server 135. The purchase may be initiated via a merchant website (not pictured). In yet another alternative example embodiment, the purchase is initiated by use of a permanent/temporary virtual/physical token, QR code, bar code, or other suitable machine-readable medium captured by the POS terminal 134. The merchant's POS terminal 134 interacts with an acquirer, the card network, the payment processing system 140, and the issuer.

[0053] The POS terminal 134 may be separate and distinct from the merchant server 135. The merchant server 135 can be a server located at a physical location of the POS terminal 134 or in a remote location. The POS terminal 134 can communicate transaction information with the merchant server 135 in circumstances where it would be advantageous for transaction storage or for any suitable reason. In an example, the POS terminal 134 is utilized for transactions at a physical location and the merchant server is

utilized for online transactions. In another example, the POS terminal 134 and the merchant server 135 are logically connected to each other and are both utilized for a transaction at a location of a merchant system 130. In another example, the POS terminal 134 conducts all transactions at a location of a merchant system 130 and no merchant server 135 is utilized.

[0054] It will be appreciated that the network connections shown are example and other means of establishing a communications link between the computers and devices can be used. Moreover, those having ordinary skill in the art having the benefit of the present disclosure will appreciate that the merchant system 130, payment processing system 140, and the user computing device 110 illustrated in Figure 1 can have any of several other suitable computer system configurations. For example, a user computing device 110 embodied as a mobile phone or handheld computer may not include all the components described above.

Example Processes

[0055] The example methods illustrated in Figures 2-3 are described hereinafter with respect to the components of the example operating environment 100. The example methods of Figure 2-3 may also be performed with other systems and in other environments.

[0056] Figure 2 is a block flow diagram depicting a method 200 for using discretionary data fields to secure transactions, in accordance with certain example embodiments.

[0057] With reference to Figures 1 and 2, in block 205, user 101 establishes a wallet account with the user computing device 110 and the payment processing system 140. In an example embodiment, the user 101 requests a wallet account using a web server 141, and the wallet account is associate with the user 101. The user 101 may be issued an account number to be used for transactions via the Internet before or after a physical card is received. In an alternative example embodiment, the payment processing system 140 mails an inactivated wallet account card to the user 101. The wallet account is then activated by the user 101 before use. In an example embodiment, a physical wallet account card is not issued. The wallet account information can be stored in the user computing device 110 and is used to make a payment via a NFC, Bluetooth, barcode, Wi-

Fi, or other form of wireless tap of the user computing device 110 with the point of sale (“POS”) terminal 134. In an alternative example embodiment, the purchase is initiated when the user 101 enters an account identification number at the POS terminal 134 or in the user computing device 110. The account identification number may be the wallet account number or a different number that links the payment transaction to the wallet account. In yet another alternative example embodiment, a purchase is initiated by use of a permanent/temporary virtual/physical token QR code, bar code, or other suitable machine-readable medium that is read by the POS terminal 134. In these cases, the POS terminal 134 may comprise a scanner, camera, or other reading device that captures the wallet account information, such as a bar code or QR reader or other suitable reading device. The wallet account information may be printed in paper or other form.

[0058] In block 210, the user 101 and/or the payment processing system 140 establish a security procedure for transactions. The security procedure may be a particular challenge and response, an interrogation of the user computing device, a location verification, or any suitable procedure. The details of example security procedures are described herein.

[0059] In block 215, the user 101 initiates a purchase at a merchant system 130 location, a website, or at any virtual location. The user 101 opens the digital wallet application module 111 executing on the user computing device. The digital wallet application module 111 represents any application or other user interface system the user 101 employs to conduct wallet account transactions and other transactions via the user computing device 110. The user 101 accesses the wallet account of the user 101 via the digital wallet application module 111 of the user computing device 110. The user 101 may select a payment account associated with the wallet account to be the used for the subsequent transaction.

[0060] In block 220, at the time that the user 101 indicates that a transaction is imminent, the user computing device 110 accesses the authentication challenge that has been configured for the account. In one example embodiment, the authentication challenge is stored in the digital wallet application module 111, on the secure element or other secure memory, or in any suitable location on the user computing device 110. In certain embodiments, the challenge request may be updated by the payment processing system 140 when the user computing device 110 and the payment processing system 140

are in communication. In an alternate example embodiment, at the time that a user 101 indicates that a transaction is imminent, the user computing device 110 contacts the payment processing system 140 to request an authentication challenge. The user computing device 110 may contact the payment processing system 140 over the Internet via a Wi-Fi signal, a cellular communication, an email, a text, or any suitable communication technology. When contacted, the payment processing system 140 transmits the authentication challenge request to the user computing device 110.

[0061] In alternate embodiments, the user computing device 110 accesses the authentication challenge after the merchant POS terminal 134 provides a transaction request to the user computing device 110. For example, the POS terminal 134 receives an initiation of a transaction from the user 101 or a merchant system operator, and transmits a request to the user computing device 110 to provide payment information. At the time of the request from the POS terminal 134, the user computing device 110 may access the authentication challenge.

[0062] The authentication challenge may be a challenge/response question for the user 101. For example, the challenge may be a question for which an answer has been previously configured with the payment processing system 140. One example question may be “What is your mother’s maiden name?” Another question may be “In what city were you born?” Any suitable question may be used. The challenge question may be displayed on the user interface of the user computing device 110. The user enters the appropriate response into the user interface of the user computing device.

[0063] Figure 4 is illustration of a user computing device requesting authentication data, in accordance with certain example embodiments. The user computing device 110 is illustrated on a user interface screen 305 of the user computing device 110. The user interface displays a credit card 102 which the user 101 has indicated will be used for a transaction. The user interface displays the challenge question 310 “In what city were you born?” The user 101 is provided a module 315 to enter the response challenge. In the example, the user may type the response with a keyboard associated with the user computing device 110.

[0064] In another example, the authentication challenge may be directed to the user computing device 110. For example, the challenge may be a request for the identification

number of the user computing device 110, the model number of the user computing device 110, or a similar request. In another example, the authentication challenge may request the location of the user computing device 110. The location may be accessed from a global positioning system (“GPS”) technology on the user computing device, from a Wi-Fi location technology, or any suitable technology. In another example, data from the transaction history of the user computing device 110 may be used. For example, the time or location of the last successful transaction may be requested. The user computing device 110 accesses the challenge request and determines the appropriate response. The response may be accessed from the memory of user computing device 110 or received from the user 101 input.

[0065] Returning to Figure 2, in block 225, the user computing device 110 communicates payment account information to the merchant POS terminal 134 in the discretionary data field of the payment account information. The details of block 225 are described in further detail with regard to method 225 in Figure 3.

[0066] Figure 3 is a block flow diagram depicting a method for the user computing device 110 to communicate payment account information to the merchant POS terminal 134 in the discretionary data field of the payment account information, in accordance with certain example embodiments.

[0067] In block 226, the user computing device 110 identifies the challenge response from user computing device 110 data or from user 101 input. In an example, the user computing device 110 accesses the challenge from the memory of the user computing device 110 or from the payment processing system 140. The user computing device 110 accesses the challenge response from the memory of the user computing device 110 or from an input of the user 101.

[0068] In block 227, the user computing device 110 incorporates the response into the discretionary data field of the wallet account information. The user computing device 110 identifies the discretionary data field of the payment account information that is available for discretionary data input. The user computing device 110 inserts the challenge response into the discretionary data field.

[0069] In block 228, user computing device 110 communicates the wallet account information to the POS terminal 134. The wallet account information is transferred to the

POS terminal 134 via NFC, Bluetooth, barcode, Wi-Fi, or other form of communication. The user 101 can initiate the communication by performing a wireless “tap” of the user computing device 110 with the POS terminal 134 or any other suitable action, such as by actuating a real or virtual button on the user computing device 110 or speaking a command into the user computing device 110. In an alternative example embodiment, a purchase is initiated by use of an RFID device, smartcard, barcode displayed on the user computing device 110, or other suitable medium that can be read by the POS terminal 134.

[0070] When a transaction is initiated, the digital wallet application module 111 can access the wallet account information residing in the digital wallet application module 111 including the challenge response. If a challenge response has been supplied by the user 101 or by the user computing device 110, then the digital wallet application module 111 can include the response in the transaction details being transmitted to the POS terminal 134.

[0071] The response may be transmitted to the POS terminal 134 in the discretionary data field of the wallet account information. Data fields of conventional wallet account information may be made up of information related to the wallet account. For example, a data field may contain a format code, a primary account number, a user name, an expiration date, a longitudinal redundancy check, or other suitable data. A discretionary data field may be included in the conventional wallet account information. Conventional wallet accounts may include in the discretionary data field a PIN verification key a card verification code. In the example, the challenge response is incorporated into the discretionary data field. The challenge response may replace other discretionary data or be added to other discretionary data.

[0072] As the challenge response can be located in a discretionary data field, the response is not utilized by the merchant system 130 or the POS terminal 134; however, the merchant system 130 communicates the challenge response in the discretionary data field to the payment processing system 140 with the transaction details.

[0073] In an example embodiment, the challenge response is the answer provided by the user 101 to a challenge question. In another example, the challenge response is a GPS location of the user computing device 110. In another example, the challenge

response is an identification number of the user computing device 110. In another example, the challenge response is specific transaction related data that was requested from the user computing device 110, such as the time of the last transaction.

[0074] Returning to Figure 2, in block 230, a payment authorization request is communicated to the payment processing system 130 from the POS terminal 134. The request includes the wallet account identification and challenge response. The POS terminal 134 communicates a payment authorization request to the payment processing system 140 to obtain payment for the purchase transaction between the user 101 and the merchant system 130. The payment authorization request comprises transaction details, such as the product being purchased, the total price, the merchant system information, the wallet account information, and other suitable data. The request may be transmitted via an acquirer, to the credit card network, and then to the payment processing system 140.

[0075] In block 235, the payment processing system 140 receives the payment authorization request and determines if the challenge response is accepted. Along with the wallet account information, the payment processing system 140 identifies the challenge response from the provided data. The payment processing system 140 accesses the wallet account of the user 101 and determines if the challenge response is appropriate. The payment processing system 140 reads the wallet account identification information from the payment authorization request and identifies the wallet account from the account identifier information. The payment processing system 140 identifies the challenge response that is stored in the discretionary data field. The payment processing system 140 determines if the challenge response matches an expected response. If the response matches, the payment processing system 140 approves the transaction as long as the other transaction details are appropriate (such as, the payment amount being within an amount authorized).

[0076] For example, to determine if the challenge response matches and expected response, the payment processing system 140 can determine if an answer provided by the user matches the configured expected answer. In an example, the expected answer to the question “What is your mother’s maiden name?” is “Jones.” If the user answered “Jones” and the answer was transmitted to the payment processing system 140, then the payment processing system 140 determines that the challenge response is accepted.

[0077] In another example, the challenge response is the GPS location of the user computing device 110. The payment processing system 140 determines the expected GPS location of the user computing device 110 based on the location of the merchant system 130 identified in the transaction details. For example, when the payment processing system 140 identifies the challenge response in the discretionary data field of the wallet account information, the user computing device 110 identifies the merchant system 130 from the transaction information. The payment processing system 140 accesses the location of the merchant system 130 from a database of merchant system 130 locations. The payment processing system 140 compares the location of the merchant system 130 with the location of the user computing device 110. If the locations match, then the payment processing system 140 determines that the user computing device 110 is located at the merchant system 130 and the likelihood of a fraudulent transaction is reduced.

[0078] In another example, the challenge response is a detail from a recent transaction. The user computing device 110 determines the last transaction conducted by the user 101 with the user computing device 110 and extracts a particular detail, such as the time of the last transaction. The payment processing system 140 compares the time of the last transaction of the user computing device 110 with the time of the last transaction stored in a server 141 of the payment processing system 140. If the times match, then the payment processing system 140 determines that the user computing device 110 is likely to be the same user computing device 110 previously used and the likelihood of a fraudulent transaction is reduced.

[0079] Any suitable response to a suitable challenge may be provided. For example, an identification number of the user computing device 110 or a personal identification number from the user 101.

[0080] In block 240, if the wallet account on the payment processing system 140 functions as a proxy account, then the payment processing system 140 may initiate a second transaction with an issuer of the selected backing account to fund the merchant transaction. The payment processing system 140 may transmit an approval or refusal of the transaction to the merchant system 130, based on approval or refusal of the transaction with the selected backing account. If the payment processing system 140 is

the issuer of the payment account, the payment processing system 140 authorizes the transactions, if all conditions are met and the challenge response is accepted.

[0081] The payment processing system 140 approves transaction based on transaction details and challenge response. If the challenge response is accepted and the transaction is approved, then the payment processing system 140 transmits the approval to the POS terminal 134. For the transaction to be approved, the payment processing system 140 determines if certain configurable conditions are met, such as determining if the account is active, if the funds available must be lower than the amount of funds requested in the authorization requested, if certain fraudulent transaction conditions are not met, or any other suitable determinations. The merchant system 130 receives the approval, provides the purchased product or service to the user 101, and logs the transaction.

[0082] The transaction funds are remitted to the merchant system 130 from the payment processing system 140. The funds may be transmitted at a later time upon settlement of the transaction.

[0083] In certain embodiments, the transaction is an online transaction. In an example, the challenge response is included in the discretionary data field of the account identifier that is provided to a merchant server 135 in the online transaction. The challenge request and the challenge response may utilize any of the techniques described herein in a manner consistent with an online transaction.

Example Systems

[0084] Figure 4 depicts a computing machine 2000 and a module 2050 in accordance with certain example embodiments. The computing machine 2000 may correspond to any of the various computers, servers, mobile devices, embedded systems, or computing systems presented herein. The module 2050 may comprise one or more hardware or software elements configured to facilitate the computing machine 2000 in performing the various methods and processing functions presented herein. The computing machine 2000 may include various internal or attached components such as a processor 2010, system bus 2020, system memory 2030, storage media 2040, input/output interface 2060, and a network interface 2070 for communicating with a network 2080.

[0085] The computing machine 2000 may be implemented as a conventional computer system, an embedded controller, a laptop, a server, a mobile device, a smartphone, a set-

top box, a kiosk, a vehicular information system, one more processors associated with a television, a customized machine, any other hardware platform, or any combination or multiplicity thereof. The computing machine 2000 may be a distributed system configured to function using multiple computing machines interconnected via a data network or bus system.

[0086] The processor 2010 may be configured to execute code or instructions to perform the operations and functionality described herein, manage request flow and address mappings, and to perform calculations and generate commands. The processor 2010 may be configured to monitor and control the operation of the components in the computing machine 2000. The processor 2010 may be a general purpose processor, a processor core, a multiprocessor, a reconfigurable processor, a microcontroller, a digital signal processor (“DSP”), an application specific integrated circuit (“ASIC”), a graphics processing unit (“GPU”), a field programmable gate array (“FPGA”), a programmable logic device (“PLD”), a controller, a state machine, gated logic, discrete hardware components, any other processing unit, or any combination or multiplicity thereof. The processor 2010 may be a single processing unit, multiple processing units, a single processing core, multiple processing cores, special purpose processing cores, co-processors, or any combination thereof. According to certain embodiments, the processor 2010 along with other components of the computing machine 2000 may be a virtualized computing machine executing within one or more other computing machines.

[0087] The system memory 2030 may include non-volatile memories such as read-only memory (“ROM”), programmable read-only memory (“PROM”), erasable programmable read-only memory (“EPROM”), flash memory, or any other device capable of storing program instructions or data with or without applied power. The system memory 2030 may also include volatile memories such as random access memory (“RAM”), static random access memory (“SRAM”), dynamic random access memory (“DRAM”), and synchronous dynamic random access memory (“SDRAM”). Other types of RAM also may be used to implement the system memory 2030. The system memory 2030 may be implemented using a single memory module or multiple memory modules. While the system memory 2030 is depicted as being part of the computing machine 2000, one skilled in the art will recognize that the system memory 2030 may be separate from the

computing machine 2000 without departing from the scope of the subject technology. It should also be appreciated that the system memory 2030 may include, or operate in conjunction with, a non-volatile storage device such as the storage media 2040.

[0088] The storage media 2040 may include a hard disk, a floppy disk, a compact disc read only memory (“CD-ROM”), a digital versatile disc (“DVD”), a Blu-ray disc, a magnetic tape, a flash memory, other non-volatile memory device, a solid state drive (“SSD”), any magnetic storage device, any optical storage device, any electrical storage device, any semiconductor storage device, any physical-based storage device, any other data storage device, or any combination or multiplicity thereof. The storage media 2040 may store one or more operating systems, application programs and program modules such as module 2050, data, or any other information. The storage media 2040 may be part of, or connected to, the computing machine 2000. The storage media 2040 may also be part of one or more other computing machines that are in communication with the computing machine 2000 such as servers, database servers, cloud storage, network attached storage, and so forth.

[0089] The module 2050 may comprise one or more hardware or software elements configured to facilitate the computing machine 2000 with performing the various methods and processing functions presented herein. The module 2050 may include one or more sequences of instructions stored as software or firmware in association with the system memory 2030, the storage media 2040, or both. The storage media 2040 may therefore represent examples of machine or computer readable media on which instructions or code may be stored for execution by the processor 2010. Machine or computer readable media may generally refer to any medium or media used to provide instructions to the processor 2010. Such machine or computer readable media associated with the module 2050 may comprise a computer software product. It should be appreciated that a computer software product comprising the module 2050 may also be associated with one or more processes or methods for delivering the module 2050 to the computing machine 2000 via the network 2080, any signal-bearing medium, or any other communication or delivery technology. The module 2050 may also comprise hardware circuits or information for configuring hardware circuits such as microcode or configuration information for an FPGA or other PLD.

[0090] The input/output (“I/O”) interface 2060 may be configured to couple to one or more external devices, to receive data from the one or more external devices, and to send data to the one or more external devices. Such external devices along with the various internal devices may also be known as peripheral devices. The I/O interface 2060 may include both electrical and physical connections for operably coupling the various peripheral devices to the computing machine 2000 or the processor 2010. The I/O interface 2060 may be configured to communicate data, addresses, and control signals between the peripheral devices, the computing machine 2000, or the processor 2010. The I/O interface 2060 may be configured to implement any standard interface, such as small computer system interface (“SCSI”), serial-attached SCSI (“SAS”), fiber channel, peripheral component interconnect (“PCI”), PCI express (PCIe), serial bus, parallel bus, advanced technology attached (“ATA”), serial ATA (“SATA”), universal serial bus (“USB”), Thunderbolt, FireWire, various video buses, and the like. The I/O interface 2060 may be configured to implement only one interface or bus technology. Alternatively, the I/O interface 2060 may be configured to implement multiple interfaces or bus technologies. The I/O interface 2060 may be configured as part of, all of, or to operate in conjunction with, the system bus 2020. The I/O interface 2060 may include one or more buffers for buffering transmissions between one or more external devices, internal devices, the computing machine 2000, or the processor 2010.

[0091] The I/O interface 2060 may couple the computing machine 2000 to various input devices including mice, touch-screens, scanners, electronic digitizers, sensors, receivers, touchpads, trackballs, cameras, microphones, keyboards, any other pointing devices, or any combinations thereof. The I/O interface 2060 may couple the computing machine 2000 to various output devices including video displays, speakers, printers, projectors, tactile feedback devices, automation control, robotic components, actuators, motors, fans, solenoids, valves, pumps, transmitters, signal emitters, lights, and so forth.

[0092] The computing machine 2000 may operate in a networked environment using logical connections through the network interface 2070 to one or more other systems or computing machines across the network 2080. The network 2080 may include wide area networks (WAN), local area networks (LAN), intranets, the Internet, wireless access networks, wired networks, mobile networks, telephone networks, optical networks, or

combinations thereof. The network 2080 may be packet switched, circuit switched, of any topology, and may use any communication protocol. Communication links within the network 2080 may involve various digital or an analog communication media such as fiber optic cables, free-space optics, waveguides, electrical conductors, wireless links, antennas, radio-frequency communications, and so forth.

[0093] The processor 2010 may be connected to the other elements of the computing machine 2000 or the various peripherals discussed herein through the system bus 2020. It should be appreciated that the system bus 2020 may be within the processor 2010, outside the processor 2010, or both. According to some embodiments, any of the processor 2010, the other elements of the computing machine 2000, or the various peripherals discussed herein may be integrated into a single device such as a system on chip (“SOC”), system on package (“SOP”), or ASIC device.

[0094] In situations in which the systems discussed here collect personal information about users, or may make use of personal information, the users may be provided with a opportunity to control whether programs or features collect user information (e.g., information about a user’s social network, social actions or activities, profession, a user’s preferences, or a user’s current location), or to control whether and/or how to receive content from the content server that may be more relevant to the user. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user’s identity may be treated so that no personally identifiable information can be determined for the user, or a user’s geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over how information is collected about the user and used by a content server.

[0095] Embodiments may comprise a computer program that embodies the functions described and illustrated herein, wherein the computer program is implemented in a computer system that comprises instructions stored in a machine-readable medium and a processor that executes the instructions. However, it should be apparent that there could be many different ways of implementing embodiments in computer programming, and the embodiments should not be construed as limited to any one set of computer program

instructions. Further, a skilled programmer would be able to write such a computer program to implement an embodiment of the disclosed embodiments based on the appended flow charts and associated description in the application text. Therefore, disclosure of a particular set of program code instructions is not considered necessary for an adequate understanding of how to make and use embodiments. Further, those skilled in the art will appreciate that one or more aspects of embodiments described herein may be performed by hardware, software, or a combination thereof, as may be embodied in one or more computing systems. Moreover, any reference to an act being performed by a computer should not be construed as being performed by a single computer as more than one computer may perform the act.

[0096] The example embodiments described herein can be used with computer hardware and software that perform the methods and processing functions described previously. The systems, methods, and procedures described herein can be embodied in a programmable computer, computer-executable software, or digital circuitry. The software can be stored on computer-readable media. For example, computer-readable media can include a floppy disk, RAM, ROM, hard disk, removable media, flash memory, memory stick, optical media, magneto-optical media, CD-ROM, etc. Digital circuitry can include integrated circuits, gate arrays, building block logic, field programmable gate arrays (FPGA), etc.

[0097] The example systems, methods, and acts described in the embodiments presented previously are illustrative, and, in alternative embodiments, certain acts can be performed in a different order, in parallel with one another, omitted entirely, and/or combined between different example embodiments, and/or certain additional acts can be performed, without departing from the scope and spirit of various embodiments. Accordingly, such alternative embodiments are included in the inventions described herein.

[0098] Although specific embodiments have been described above in detail, the description is merely for purposes of illustration. It should be appreciated, therefore, that many aspects described above are not intended as required or essential elements unless explicitly stated otherwise. Modifications of, and equivalent components or acts corresponding to, the disclosed aspects of the example embodiments, in addition to those

described above, can be made by a person of ordinary skill in the art, having the benefit of the present disclosure, without departing from the spirit and scope of embodiments defined in the following claims, the scope of which is to be accorded the broadest interpretation so as to encompass such modifications and equivalent structures.

What is claimed is:

1. A computer-implemented method to use discretionary data fields to secure transactions, comprising:

storing, by one or more computing devices, a payment account identifier that identifies a payment account associated with an account of a user, the payment account identifier being arranged in a plurality of fields and comprising a discretionary data field;

receiving, by the one or more computing devices, an authentication challenge;

determining, by the one or more computing devices, a challenge response to the authentication challenge;

communicating, by the one or more computing devices, the challenge response to a payment processing system;

receiving, by the one or more computing devices, a payment request from a merchant computing system, the payment request comprising a request for payment account information for a payment account to use to fund a payment transaction;

obtaining, by the one or more computing devices, the challenge response and the payment account identifier;

embedding, by the one or more computing devices, the challenge response in the discretionary data field associated with the payment account identifier; and

communicating, by the one or more computing devices, the payment account identifier including the discretionary data field having embedded therein the challenge response to the merchant computing system,

wherein the receiving of the authentication challenge comprises:

communicating, by the one or more computing devices, to the payment processing system that a transaction is pending;

receiving, by the one or more computing devices, the authentication challenge from the payment processing system, wherein the one or more computing devices access the authentication challenge after the merchant computing system provides the payment request to the one or more computing devices.

2. The computer-implemented method of claim 1, wherein the receiving of the authentication challenge comprises identifying, by the one or more computing devices, the authentication challenge request stored on the one or more computing devices.

3. The computer-implemented method of claim 2, wherein the challenge request stored on the one or more computing devices is provided by the payment processing system at a time before the receiving of the indication that a transaction is pending.

4. The computer-implemented method of claim 1, wherein the challenge response is received as an input for an operator interface associated with the user computing device.

5. The computer-implemented method of claim 1, wherein the challenge response is received from a set of stored data on the user computing device.

6. The computer-implemented method of claim 1, wherein the challenge response comprises location data of the one or more computing devices.

7. The computer-implemented method of claim 1, wherein the challenge response comprises stored transaction data from a previous transaction.

8. A computer program product, comprising:
a non-transitory computer-readable memory having computer-executable program instructions embodied thereon that when executed by a computer cause the computer to use discretionary data fields to secure transactions, the computer-executable program instructions comprising:

computer-executable program instructions to associate a payment account identifier that identifies a payment account associated with a user computing device, the payment account identifier being arranged in a plurality of fields and comprising a discretionary data field;

computer-executable program instructions to establish an authentication challenge and a corresponding challenge response, including computer-executable program instructions to receive a request for an authentication challenge from a user computing device to be associated with a pending transaction; and computer-executable program instructions to transmit the challenge request to the user computing device, wherein the user computing device accesses the authentication challenge after a merchant computing system provides a payment transaction request to the user computing device;

computer-executable program instructions to receive a first payment authorization request originating from the merchant computing system, the first payment authorization request comprising the

payment account identifier including the discretionary data field having embedded therein the challenge response and a request to fund a transaction using the payment account;

computer-executable program instructions to compare the received challenge response with the corresponding challenge response; and

computer-executable program instructions to reply to the merchant computing system with a responsive authorization state, wherein the responsive authorization state is determined based on the determination whether the provided challenge response and the corresponding challenge response match.

9. The computer program product of claim 8, further comprising computer-executable program instructions to access a previous transaction associated with the payment account to determine the corresponding challenge response.

10. The computer program product of claim 8, further comprising:
computer-executable program instructions to receive a location of the user computing device as the provided challenge response;
computer-executable program instructions to access a database of merchant locations; and
computer-executable program instructions to determine if the provided location of the user computing device matches an expected location based on an identity of the merchant in the transaction details.

11. The computer program product of claim 8, wherein the authentication challenge is provided to the user computing device at a time before the transaction is initiated.

12. The computer program product of claim 8, further comprising computer-executable program instructions to configure the corresponding challenge response to an authentication question based on an input from a user.

13. A system to select payment accounts to use discretionary data fields to secure transactions, comprising:
a storage resource; and

a processor communicatively coupled to the storage resource, wherein the processor executes application code instructions that are stored in the storage resource and that cause the system to:

associate a payment account identifier that identifies a payment account associated with a user computing device, the payment account identifier being arranged in a plurality of fields and comprising a discretionary data field;

establish an authentication challenge and a corresponding challenge response, including to receive a request for an authentication challenge from a user computing device to be associated with a pending transaction; and to transmit the challenge request to the user computing device, wherein the user computing device accesses the authentication challenge after a merchant computing system provides a payment transaction request to the user computing device;

receive a first payment authorization request originating from a merchant computing system, the first payment authorization request comprising the payment account identifier including the discretionary data field having embedded therein the challenge response and a request to fund a transaction using the payment account;

compare the received challenge response with the corresponding challenge response; and

reply to the merchant computing system with a responsive authorization state, wherein the responsive authorization state is determined based on the determination whether the provided challenge response and the corresponding challenge response match.

14. The system of claim 13, the processor executing further application code instructions that are stored in the storage device and that cause the system to access a previous transaction associated with the payment account to determine the corresponding challenge response.

15. The system of claim 13, wherein the authentication challenge is provided to the user computing device at a time before the transaction is initiated.

16. The system of claim 13, the processor executing further application code instructions that are stored in the storage device and that cause the system to configure the corresponding challenge response to an authentication question based on an input from a user.

17. The system of claim 13, wherein the challenge response comprises location data of the one or more computing devices.

18. A computer-implemented method to use discretionary data fields to secure transactions, comprising:

storing, by one or more computing devices, a payment account identifier that identifies a payment account associated with an account of a user that is issued by a payment processing system, the payment account identifier identifying the payment account and being arranged in a plurality of fields and comprising a discretionary data field;

receiving, by the one or more computing devices, a payment request in a communication from a merchant computing system, the payment request comprising a request for payment account information for a payment account to use to fund a payment transaction;

at a time after receiving the payment request, notifying, by the one or more computing devices, the payment processing system that a transaction is pending, the notifying being in a separate communication from the communication with the merchant computing system;

receiving, by the one or more computing devices, an authentication challenge from the payment processing system, the authentication challenge being communicated from the payment processing system upon receipt of the notification;

obtaining, by the one or more computing devices, the payment account identifier and a challenge response to the authentication challenge;

embedding, by the one or more computing devices, the challenge response in the discretionary data field associated with the payment account identifier; and

communicating, by the one or more computing devices, the payment account identifier including the discretionary data field having embedded therein the challenge response to the merchant computing system to be communicated from the merchant computing system to the payment processing system to authorize the payment transaction based on a match between the challenge response and a challenge response stored on the payment processing system.

19. The computer-implemented method of claim 18, wherein the receiving of the authentication challenge comprises identifying, by the one or more computing devices, the authentication challenge request stored on the one or more computing devices.

20. The computer-implemented method of claim 19, wherein the challenge request stored on the one or more computing devices is provided by the payment processing system at a time before the receiving of the payment request.

21. The computer-implemented method of claim 18, wherein the challenge response is received as an input for an operator interface associated with a user computing device.

22. The computer-implemented method of claim 18, wherein the challenge response is received from a set of stored data on a user computing device.

23. The computer-implemented method of claim 18, wherein the challenge response comprises location data of the one or more computing devices.

24. The computer-implemented method of claim 18, wherein the challenge response comprises stored transaction data from a previous transaction.

25. A computer program product, comprising:

a non-transitory computer-readable storage device having computer-executable program instructions embodied thereon that when executed by a computer cause the computer to use discretionary data fields to secure transactions, the computer-executable program instructions comprising:

computer-executable program instructions to associate a payment account identifier that identifies a payment account associated with a user computing device, the payment account comprising a payment account identifier that identifies the payment account, the payment account identifier being arranged in a plurality of fields and comprising a discretionary data field; computer-executable program instructions to receive a communication from the user computing device that a transaction is being initiated;

computer-executable program instructions to communicate an authentication challenge and a corresponding challenge response to the user computing device upon receiving the communication from the user computing device that the transaction is being initiated;

computer-executable program instructions to receive a first payment authorization request originating from a merchant computing system, the first payment authorization request comprising the payment account identifier including the discretionary data field having embedded therein the challenge response and a request to fund a transaction using the payment account;

computer-executable program instructions to compare the received challenge response with the corresponding challenge response; and

computer-executable program instructions to reply to the merchant computing system with a responsive authorization state, wherein the responsive authorization state is determined based on the determination whether the provided challenge response and the corresponding challenge response match.

26. The computer program product of claim 25, further comprising: computer-executable program instructions to receive a request for an authentication challenge from a user computing device to be associated with a pending transaction; and computer-executable program instructions to transmit the challenge request to the user computing device.

27. The computer program product of claim 25, further comprising computer-executable program instructions to access a previous transaction associated with the payment account to determine the corresponding challenge response.

28. The computer program product of claim 25, further comprising:

computer-executable program instructions to receive a location of the user computing device as the provided challenge response; computer-executable program instructions to access a database of merchant locations; and

computer-executable program instructions to determine if the provided location of the user computing device matches an expected location based on an identity of the merchant in the transaction details.

29. The computer program product of claim 25, wherein the authentication challenge is provided to the user computing device at a time before the transaction is initiated.

30. The computer program product of claim 25, further comprising computer-executable program instructions to configure the corresponding challenge response to an authentication question based on an input from a user.

31. A system to select payment accounts to use discretionary data fields to secure transactions, comprising:

- a storage resource; and

- a processor communicatively coupled to the storage resource, wherein the processor executes application code instructions that are stored in the storage resource to cause the system to:

- associate a payment account identifier that identifies a payment account associated with a user computing device, the payment account comprising a payment account identifier that identifies the payment account, the payment account identifier being arranged in a plurality of fields and comprising a discretionary data field;

- receive a communication from the user computing device that a transaction is being initiated;

- communicate an authentication challenge and a corresponding challenge response to the user computing device upon receiving the communication from the user computing device that the transaction is being initiated;

- receive a first payment authorization request originating from a merchant computing system, the first payment authorization request comprising the payment account identifier including the discretionary data field having embedded therein the challenge response and a request to fund a transaction using the payment account;

- compare the received challenge response with the corresponding challenge response; and

- reply to the merchant computing system with a responsive authorization state, wherein the responsive authorization state is determined based on the determination whether the provided challenge response and the corresponding challenge response match.

32. The system of claim 31, the processor executing further application code instructions that are stored in the storage device and that cause the system to access a previous transaction associated with the payment account to determine the corresponding challenge response.

33. The system of claim 31, wherein the authentication challenge is provided to the user computing device at a time before the transaction is initiated.

34. The system of claim 31, the processor executing further application code instructions that are stored in the storage device and that cause the system to configure the corresponding challenge response to an authentication question based on an input from a user.

35. The system of claim 31, wherein the challenge response comprises location data of the one or more computing devices.

1/5

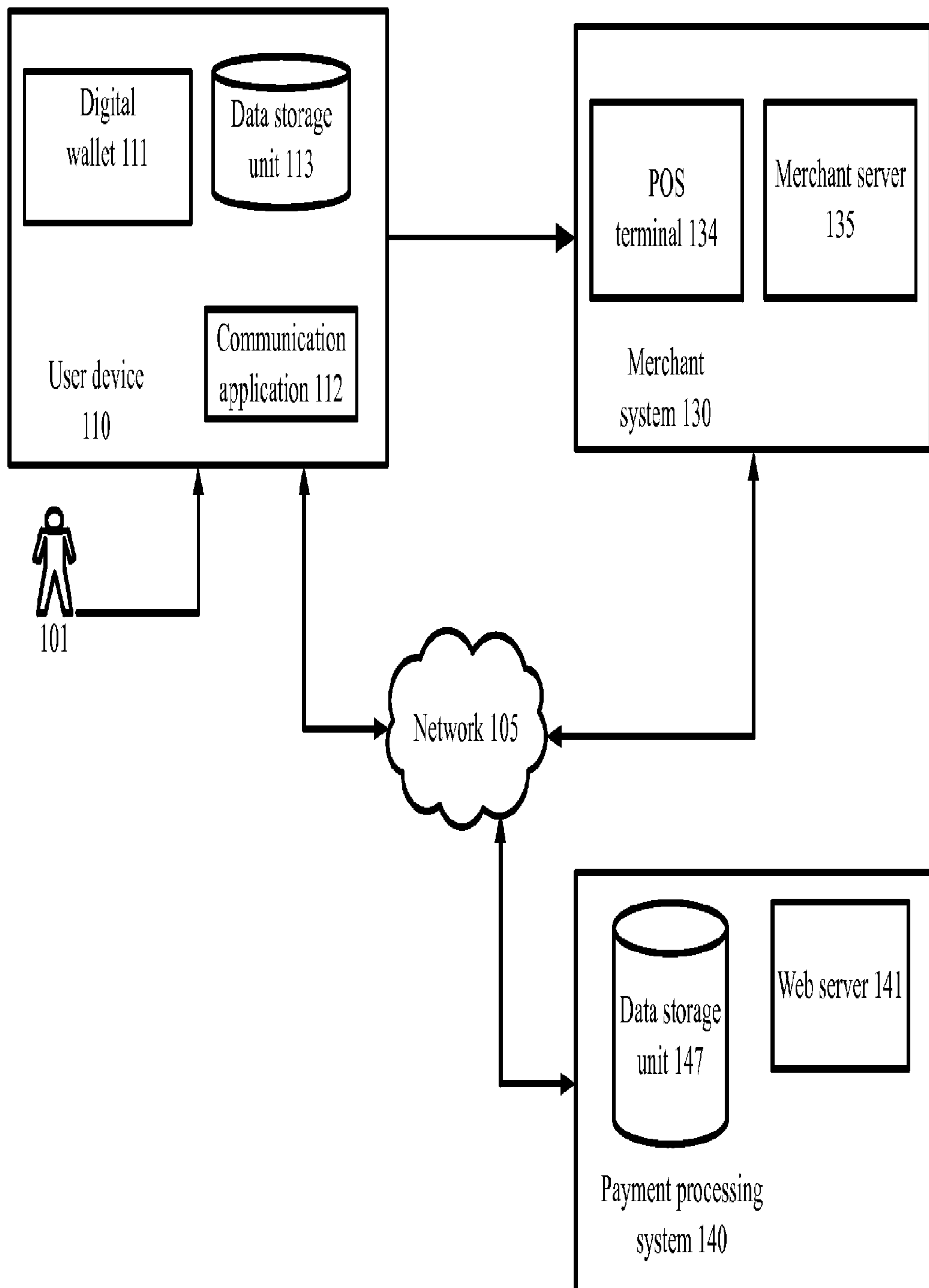
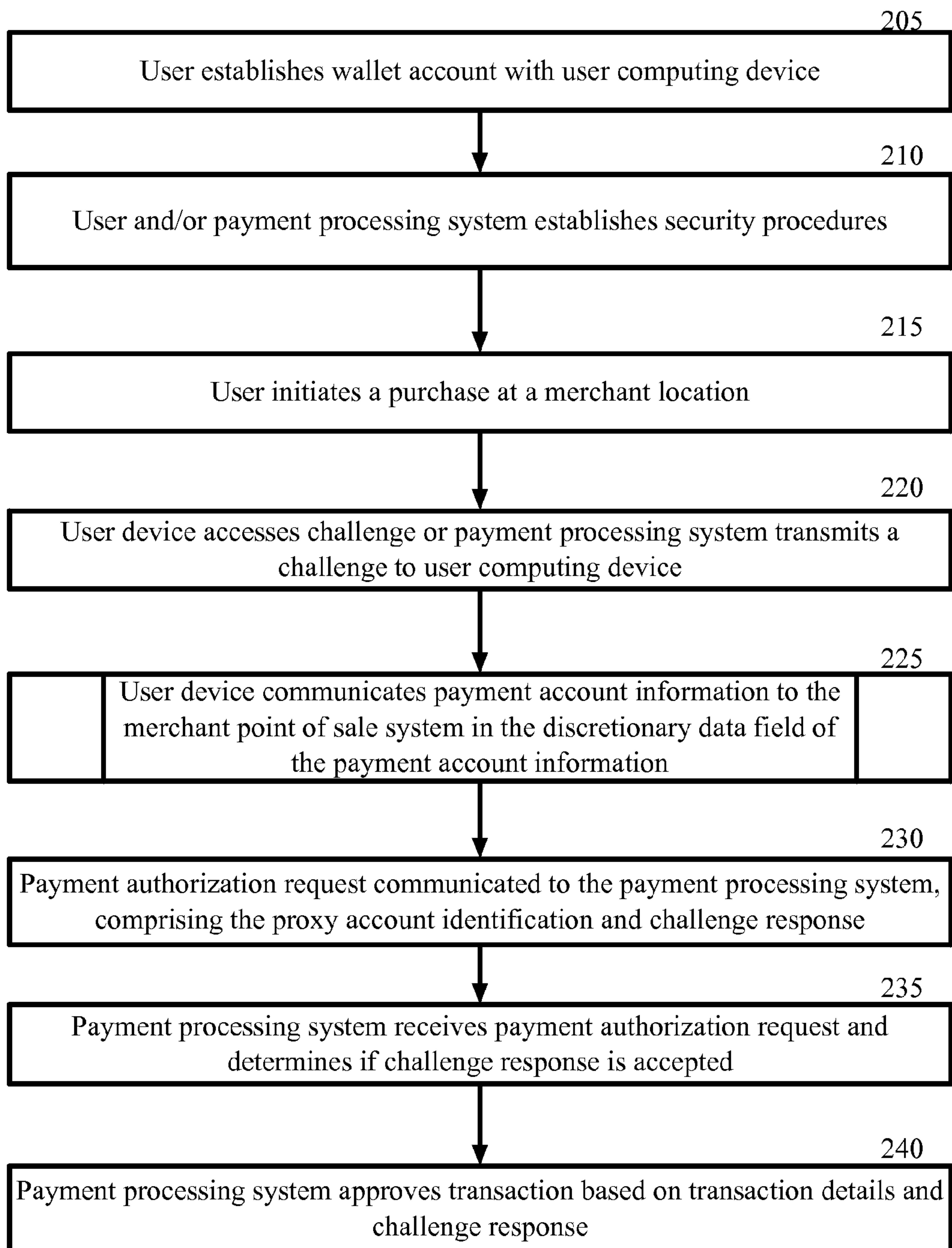
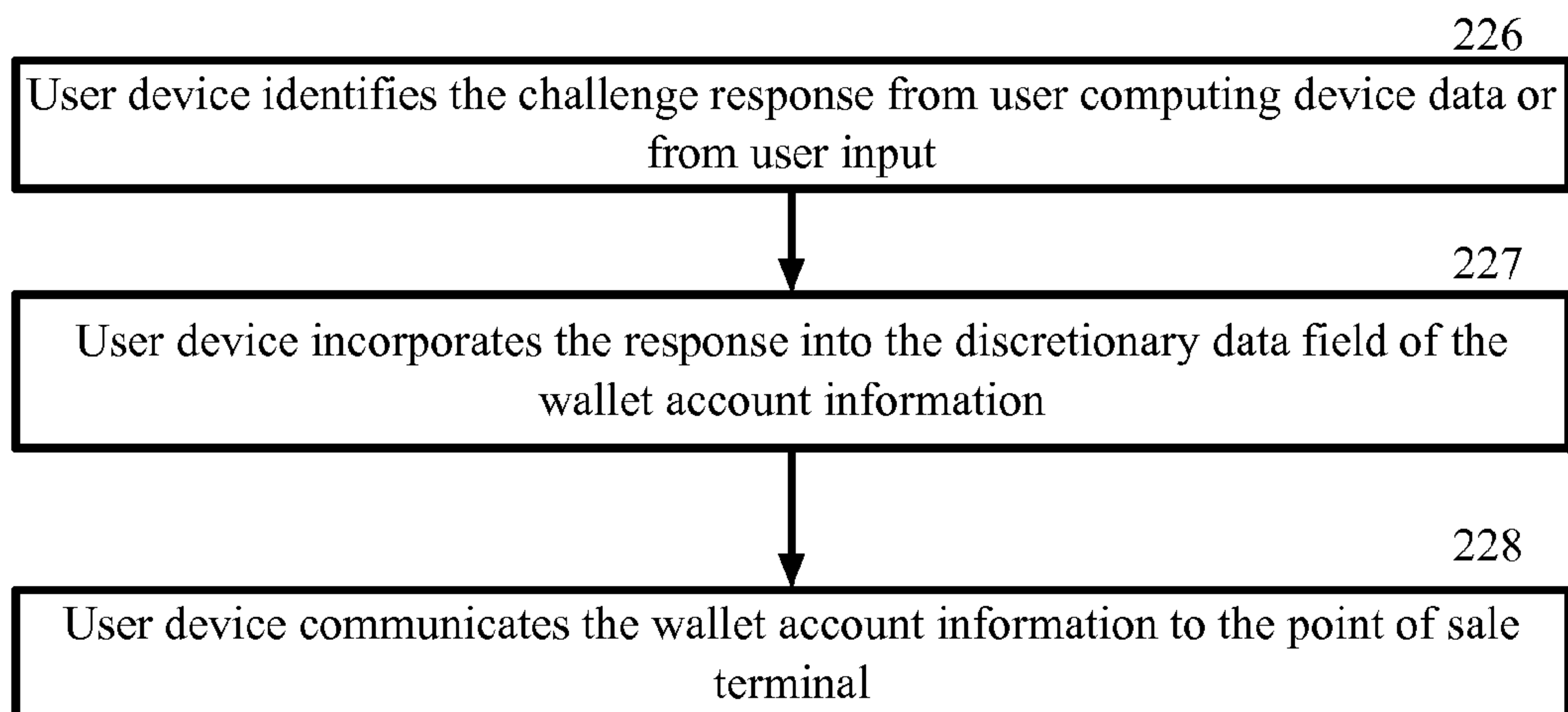
100

Fig. 1

2/5

200**Fig. 2**

3/5

225**Fig. 3**

110

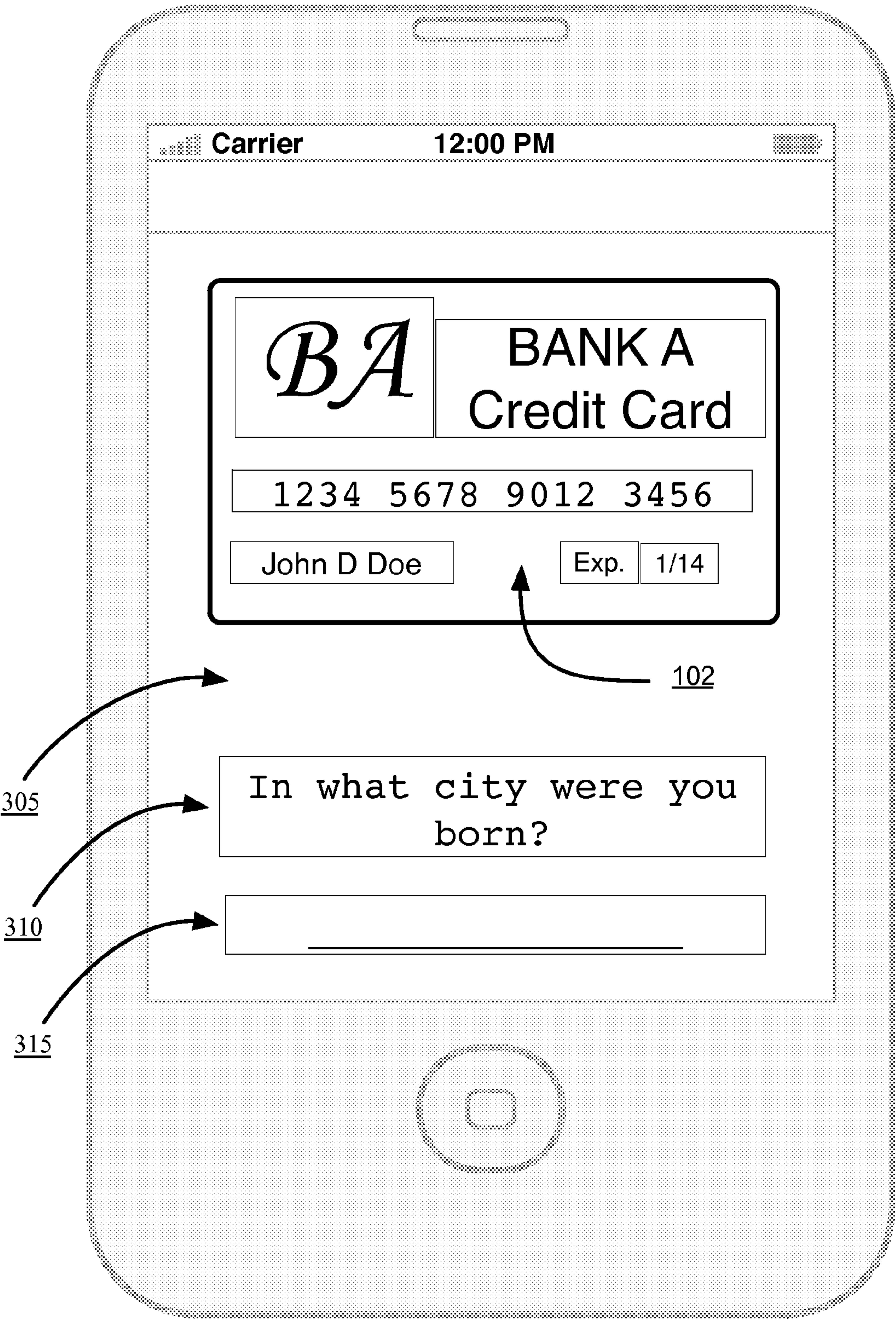
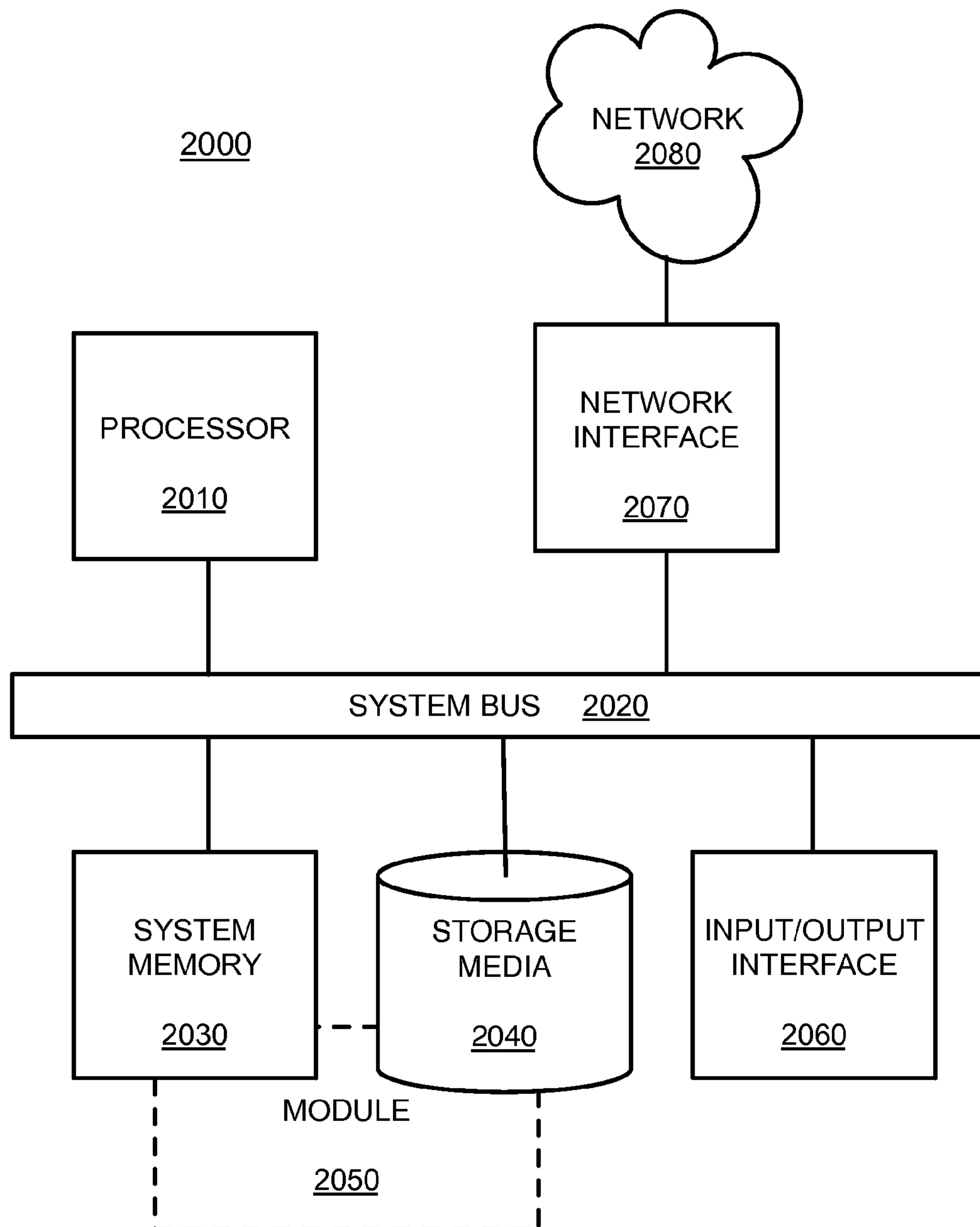


Fig. 4

5/5

**Fig. 5**

