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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 December 2007 (27.12.2007)

PCT

(10) International Publication Number
WO 2007/149775 A2

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2007/071301

(22) International Filing Date: 15 June 2007 (15.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/815,059	19 June 2006 (19.06.2006)	US
60/815,430	20 June 2006 (20.06.2006)	US
60/884,089	9 January 2007 (09.01.2007)	US

(71) Applicants *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US). **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HAMMAD, Ayman** [US/US]; 6048 Corte Montanas, Pleasanton, California 94566 (US). **FAITH, Patrick** [US/US]; 2810 Jones Gate Court, Pleasanton, California 94566 (US).

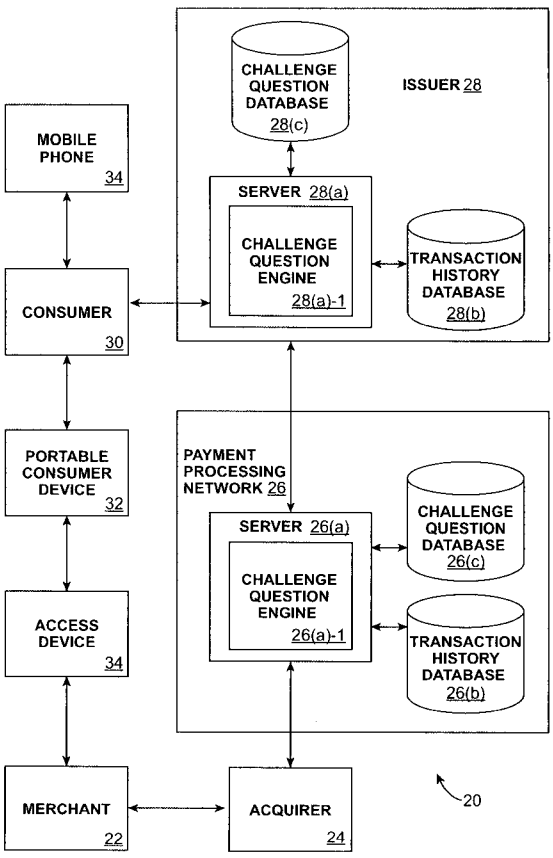
(74) Agents: **JEWIK, Patrick R.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: CONSUMER AUTHENTICATION SYSTEM AND METHOD



(57) Abstract: A method for authenticating a consumer. The method includes receiving an authorization request message associated with a consumer conducting a transaction with a portable consumer device. A challenge message is sent to the consumer, where the challenge message is dynamic or semi-dynamic. A challenge response message is received from the consumer, and an authorization response message is sent to the consumer. The authorization response message indicates whether or not the transaction is authorized.

WO 2007/149775 A2

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONSUMER AUTHENTICATION SYSTEM AND METHOD

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a non-provisional patent application of and claims the benefit of the filing dates of U.S. Provisional Patent Application No. 60/815,059, filed on June 19, 2006, U.S. Provisional Patent Application No. 60/815,430 filed on June 20, 2006, and U.S. Provisional Patent Application No. 60/884,089 filed on January 9, 2007. All of these applications are herein incorporated by reference in their entirety for all purposes.

BACKGROUND

[0002] It is desirable to have mechanisms that ensure that a consumer who is using a portable consumer device such as a credit card is really the consumer who is associated with the credit card. Fraudulent activity can be very costly to merchants, issuers of portable consumer devices, and others.

[0003] A number of consumer authentication mechanisms are known. In one example of a conventional consumer authentication process, a consumer may purchase gas at a gas station using his credit card. Before the consumer is allowed to buy the gas and before the authorization request message is sent to the issuer of the portable consumer device, the gas pump may request that the consumer supply his zip code. This authentication request may be provided by the merchant as a way to ensure that the consumer is in fact the consumer associated with the credit card. The gas station wants to verify that the consumer is authentic, since the gas station may bear some of the risk for any fraudulent activity that results from purchases made at the gas station.

[0004] While such conventional authentication methods are effective, a number of improvements can be made. For example, conventional authentication requests are typically static. If someone has stolen a consumer's portable consumer device and knows the consumer's zip code, for example, that person could still conduct fraudulent transactions using the authentic portable consumer device.

Moreover, merchants have limited information about the consumer, and the types of challenges that can be provided at the consumer are limited.

[0005] Better ways to authenticate consumers using portable consumer devices are desirable. Embodiments of the invention address the above problems, and other problems, individually and collectively.

SUMMARY OF THE INVENTION

[0006] Embodiments of the invention can authenticate a consumer.

[0007] One embodiment of the invention is directed to a method comprising receiving an authorization request message associated with a consumer conducting a transaction with a portable consumer device. A challenge message is sent to the consumer, where the challenge message is dynamic or semi-dynamic. A challenge response message is received from the consumer, and an authorization response message is sent to the consumer. The authorization response message indicates whether or not the transaction is authorized.

[0008] Another embodiment of the invention is directed to a method comprising initiating an authorization request message, where the authorization request message is associated with a consumer conducting a transaction with a portable consumer device and is sent to an issuer associated with the portable consumer device, receiving a challenge message, wherein the challenge message is dynamic or semi-dynamic, and then initiating a challenge response message, where the challenge response message is responsive to the challenge message. An authorization response message is received, where the authorization response message indicates whether or not the transaction is authorized.

[0009] Yet another embodiment of the invention is directed to a method comprising receiving, at an issuer, an authorization request message sent from an access device. In response to receipt of the authorization request message, one or more dynamic challenge questions are provided to the consumer before authorizing a transaction conducted by the consumer.

[0010] Yet another embodiment of the invention is directed to a method comprising receiving a first authorization request message associated with a

consumer conducting a transaction with a portable consumer device, sending a challenge message to the consumer, receiving a second authorization request message including a challenge response message, and sending an authorization response message to the consumer, wherein the authorization response message indicates whether or not the transaction is authorized.

[0011] Another embodiment of the invention is directed to a method comprising sending a first authorization request message associated with a consumer conducting a transaction with a portable consumer device, receiving a challenge message, sending a second authorization request message including a challenge response message; and receiving an authorization response message, wherein the authorization response message indicates whether or not the transaction is authorized.

[0012] Other embodiments of the invention are directed to systems, portable consumer devices, and computer readable media associated with the above-described methods.

[0013] These and other embodiments of the invention are described in further detail below with reference to the Figures and the Detailed Description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIG. 1 shows a block diagram of a system according to an embodiment of the invention.

[0015] FIG. 2 shows a block diagram of one type of portable consumer device.

[0016] FIG. 3 shows a plan view of a second type of portable consumer device.

[0017] FIG. 4 shows a flowchart illustrating a method according to an embodiment of the invention.

[0018] FIG. 5 shows another flowchart illustrating another method according to an embodiment of the invention.

[0019] FIG. 6 shows a block diagram of certain authentication aspects of embodiments of the invention.

[0020] FIG. 7 shows a block diagram of a computer apparatus.

DETAILED DESCRIPTION

[0021] Currently, consumer authentication using challenge questions is typically performed at the merchant. The merchant asks the consumer for identification such as a driver's license before allowing a purchase transaction with a portable consumer device to proceed. In some cases, it may be better to provide for more "back end" consumer authentication processes, whereby an issuer and/or a payment processing organization (such as Visa) verify the identity of the consumer. The issuer and/or the payment processing organization have much more data about the consumer than the merchant and are in a better position to authenticate the consumer. For example, the issuer has information such as the consumer's address, mother's maiden name, etc. In addition, the issuer and the payment processing organization have information such as recent purchase information and consumer purchasing behavior. Any of this information can be used to help authenticate the consumer in a purchase transaction.

[0022] Thus, in embodiments of the invention, the payment processing organization, the issuer, or any other non-merchant entity with information about the consumer may pose challenge questions to the consumer to authenticate the consumer. The challenge questions may be static where the same questions are asked for each purchase transaction or dynamic where different questions may be asked over time.

[0023] The questions asked may also have static or dynamic (semi-dynamic or fully dynamic) answers. For example, the question "What is your birthday?" requires a static answer, since the answer does not change. The question "What is your zip-code?" requires a semi-dynamic answer, since it could change or can change infrequently. Lastly, the question "What did you purchase yesterday at 4 pm?" would require a dynamic answer since the answer changes frequently. Thus, in preferred embodiments, the challenge questions would preferably be based on "real time" information that the issuer would most likely possess. For example, the consumer might be asked a more specific question such as "Did you eat out at a

Mexican restaurant last night?" By providing more specific knowledge based consumer challenges, the authentication of the consumer is ensured.

[0024] In one embodiment, the method includes conducting a transaction such as a purchase transaction using a portable consumer device. The portable consumer device may be a credit card or the like. The purchase transaction may take place at a merchant that has an access device such as a point of sale terminal.

[0025] The consumer may use the portable consumer device to interact with an access device such as a point of sale terminal and initiate the process. The point of sale terminal may initiate and then generate an authorization request message, which may thereafter be sent to a payment processing network, and then subsequently to the issuer of the portable consumer device. When the authorization request message is received, by either the payment processing network or the issuer, it is analyzed. A challenge message, which can be dynamic or semi-dynamic in nature, is then generated, and is sent to the consumer. The challenge message could be sent back to the access device, or to the consumer's portable consumer device (e.g., if the portable consumer device is a mobile phone).

[0026] The consumer then provides a response to the challenge message. The challenge response message is received from the consumer. The challenge response message is then verified and if it is verified, the authorization response message is analyzed to determine if the transaction is authorized (e.g., there are sufficient funds in the consumer's account or there is sufficient credit in the consumer's account). If the transaction is authorized, the issuer and also the payment processing network send an authorization response message to the consumer. The authorization response message indicates whether or not the transaction is authorized.

[0027] In the specific embodiments described above and below, challenge questions are described in detail, but embodiments of the invention are not limited thereto. Embodiments of the invention can generally relate to the use of challenge messages, which may include challenge questions. In some embodiments, as will be described in further detail below, challenge messages may or may not be read by a consumer, and may challenge the authenticity of the consumer in direct or indirect ways. Examples of challenge questions include questions relating to the consumer's

portable consumer device (e.g., what is the CVV2 or card verification value on the back of your card?), the consumer's location (e.g., what is your zip code?), the consumer's mobile or regular phone (e.g., what is your mobile phone number?), the consumer's personal information (e.g., what is your mother's maiden name?), etc. Examples of challenge messages that are not questions that are specifically answered by the consumer include messages which automatically query a phone as to its location or phone number, and cause the retrieval of such information. Another example of a challenge message may be a message which supplies a code (or other authentication token) to a phone, and the use of that code at an access device authenticates the user.

[0028] I. Systems

[0029] FIG. 1 shows an exemplary system **20** according to an embodiment of the invention. Other systems according to other embodiments of the invention may include more or less components than are shown in FIG. 1.

[0030] The system **20** shown in FIG. 1 includes a merchant **22** and an acquirer **24** associated with the merchant **22**. In a typical payment transaction, a consumer **30** may purchase goods or services at the merchant **22** using a portable consumer device **32**. The merchant **22** could be a physical brick and mortar merchant or an e-merchant. The acquirer **24** can communicate with an issuer **28** via a payment processing network **26**. The merchant **22** could alternatively be connected directly to the payment processing network **26**.

[0031] The consumer **30** may be an individual, or an organization such as a business that is capable of purchasing goods or services. In other embodiments, the consumer **30** may simply be a person who wants to conduct some other type of transaction such as a money transfer transaction or a transaction at an ATM. The consumer **30** may optionally operate a wireless phone **34**.

[0032] The portable consumer device **32** may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially

available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones (e.g., the phone **34** described above), personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (*e.g.*, a debit card), credit devices (*e.g.*, a credit card), or stored value devices (*e.g.*, a stored value card).

[0033] An exemplary portable consumer device **32'** in the form of a phone may comprise a computer readable medium and a body as shown in FIG. 2. (FIG. 2 shows a number of components, and the portable consumer devices according to embodiments of the invention may comprise any suitable combination or subset of such components.) The computer readable medium **32(b)** may be present within the body **32(h)**, or may be detachable from it. The body **32(h)** may be in the form a plastic substrate, housing, or other structure. The computer readable medium **32(b)** may be a memory that stores data and may be in any suitable form including a magnetic stripe, a memory chip, etc. The memory preferably stores information such as financial information, transit information (e.g., as in a subway or train pass), access information (e.g., as in access badges), etc. Financial information may include information such as bank account information, bank identification number (BIN), credit or debit card number information, account balance information, expiration date, consumer information such as name, date of birth, etc. Any of this information may be transmitted by the portable consumer device **32**.

[0034] Information in the memory may also be in the form of data tracks that are traditionally associated with credits cards. Such tracks include Track 1 and Track 2. Track 1 ("International Air Transport Association") stores more information than Track 2, and contains the cardholder's name as well as account number and other discretionary data. This track is sometimes used by the airlines when securing reservations with a credit card. Track 2 ("American Banking Association") is currently most commonly used. This is the track that is read by ATMs and credit card checkers. The ABA (American Banking Association) designed the specifications of this track and all world banks must abide by it. It contains the cardholder's account, encrypted PIN data, plus other discretionary data.

[0035] The portable consumer device **32** may further include a contactless element **32(g)**, which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Contactless element **32(g)** is associated with (e.g., embedded within) portable consumer device **32** and data or control instructions transmitted via a cellular network may be applied to contactless element **32(g)** by means of a contactless element interface (not shown). The contactless element interface functions to permit the exchange of data and/or control instructions between the mobile device circuitry (and hence the cellular network) and an optional contactless element **32(g)**.

[0036] Contactless element **32(g)** is capable of transferring and receiving data using a near field communications ("NFC") capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between the portable consumer device **32** and an interrogation device. Thus, the portable consumer device **32** is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0037] The portable consumer device **32** may also include a processor **32(c)** (e.g., a microprocessor) for processing the functions of the portable consumer device **32** and a display **32(d)** to allow a consumer to see phone numbers and other information and messages. The portable consumer device **32** may further include input elements **32(e)** to allow a consumer to input information into the device, a speaker **32(f)** to allow the consumer to hear voice communication, music, etc., and a microphone **32(i)** to allow the consumer to transmit her voice through the portable consumer device **32**. The portable consumer device **32** may also include an antenna **32(a)** for wireless data transfer (e.g., data transmission).

[0038] If the portable consumer device is in the form of a debit, credit, or smartcard, the portable consumer device may also optionally have features such as magnetic strips. Such devices can operate in either a contact or contactless mode.

[0039] An example of a portable consumer device **32"** in the form of a card is shown in FIG. 3. FIG. 3 shows a plastic substrate **32(m)**. A contactless element **32(o)** for interfacing with an access device **34** may be present on or embedded within the plastic substrate **32(m)**. Consumer information **32(p)** such as an account number, expiration date, and consumer name may be printed or embossed on the card. Also, a magnetic stripe **32(n)** may also be on the plastic substrate **32(m)**.

[0040] As shown in FIG. 3, the portable consumer device **32"** may include both a magnetic stripe **32(n)** and a contactless element **32(o)**. In other embodiments, both the magnetic stripe **32(n)** and the contactless element **32(o)** may be in the portable consumer device **32"**. In other embodiments, either the magnetic stripe **32(n)** or the contactless element **32(o)** may be present in the portable consumer device **32"**.

[0041] The payment processing network **26** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0042] The payment processing network **26** may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network **26** may use any suitable wired or wireless network, including the Internet.

[0043] As shown in FIG. 1, the payment processing network **26** may comprise a server **26(a)**, which may comprise a challenge question engine **26(a)-1**. The server **26(a)** may also be in communication with a transaction history database **26(b)** and a challenge question database **26(c)**. As will be explained in further detail below, the challenge question engine **26(a)-1** may simply extract challenge

questions from the challenge question database **26(c)**. Alternatively or additionally, the challenge question engine **26(a)-1** may generate challenge questions using information in the transaction history database **26(b)**.

[0044] As will be explained in further detail below, the challenge questions may be static or dynamic in nature. For example, the challenge question engine **26(a)-1** may receive an authorization request message, and the authorization request message may include the consumer's account number, as well as the purchase amount. It may then look up the consumer's account number, and any consumer information associated with the consumer's account number. It may thereafter retrieve suitable questions from the challenge question database **26(c)** or may generate suitable challenge questions on its own. For instance, in some cases, the challenge question engine **26(a)-1** may retrieve the question "What is your mobile phone number?" from the challenge question database **26(c)** after receiving an authorization request message. Alternatively, the challenge question engine **26(a)-1** may generate a dynamic question such as "Did you use this credit card at McDonald's last night?" The information pertaining to the particular restaurant that the consumer **30** was at the preceding day could be retrieved from the transaction history database **26(b)**.

[0045] The challenge question database **26(c)** may be populated with questions of any suitable type. The questions may relate to a past location (e.g., the consumer's current home, the city that the consumer recently visited) or current location (e.g., the current location of the store that the consumer is currently at), the type or name of the merchant that the consumer is presently visiting or has visited in the past, the consumer's family or personal data (e.g., name, phone number, social security number, etc.), etc. The questions in the challenge question database **26(c)** may be generated by the challenge question engine **26(a)-1** and subsequently stored in the challenge question database **26(c)**.

[0046] Alternatively, or additionally, the challenge questions may be generated from an external source and then subsequently stored in the challenge question database **26(c)**. For example, the consumer **30** may use a browser on a personal computer or the like to supply specific challenge questions to the server **26(a)** via a communication medium (not shown) such as the Internet.

[0047] In some embodiments, a consumer may determine the kinds and/or quantity of challenge questions to ask himself or herself. For example, the consumer may specify that the consumer wants to be asked three challenge questions if the consumer visits a jewelry store, but only one question if the consumer visits a fast food restaurant. The types of questions posed by the consumer may be based on the merchant type, frequency of purchasing, etc. Some concepts relating to user-defined authorization parameters are described in U.S. Patent Application No. 10/093,002, filed on March 5, 2002, which is herein incorporated by reference in its entirety for all purposes.

[0048] In preferred embodiments, the challenge questions are derived from past transaction data in the transaction history database **26(b)**. The consumer **30** may conduct many, many transactions with the payment processing network **26** (and/or the issuer **28**) over time. This consumer transaction information may be stored in the transaction history database **26(b)** over time, and challenge questions may be generated using the transaction information. The past transaction information provides a good basis for authenticating the consumer **30**, since the consumer **30** will know about what transactions that the consumer **30** has conducted in the past. For example, the consumer **30** may have used his credit card to pay for a hotel room in New York the previous day, and on the next day may be asked a question such as "Did you stay at a hotel in New York yesterday?" In another example, the consumer **30** may have purchased an item that is more than $2000 the day before, and on the next day may be asked "Did you make a purchase for more than $2000 yesterday?" The questions/answers that are presented to the consumer **30** may be free form in nature and/or may include pre-formatted answers such as multiple choice or true-false answers from which the user may select.

[0049] The merchant **22** may also have, or may receive communications from, an access device **34** that can interact with the portable consumer device **32**. The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

[0050] If the access device **34** is a point of sale terminal, any suitable point of sale terminal may be used including card readers. The card readers may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer devices **32**.

[0051] The issuer **28** may be a bank or other organization that may have an account associated with the consumer **30**. The issuer **26** may operate a server **28(a)** which may have a challenge question engine **28(a)-1**. A transaction history database **26(b)** and a challenge question database **28(c)** may be in communication with the server **28(a)**. The issuer server **28(a)**, challenge question engine **28(a)-1**, transaction history database **26(b)**, and challenge question database **28(c)** may operate in the same way or a different way than the payment processing network server **28(a)**, challenge question engine **28(a)-1**, transaction history database **28(b)**, and challenge question database **28(c)**. The above-descriptions as to elements **26(a)**, **26(a)-1**, **26(b)**, and **26(c)** may apply to elements **28(a)**, **28(a)-1**, **28(b)**, and **28(c)**.

[0052] Embodiments of the invention are not limited to the above-described embodiments. For example, although separate functional blocks are shown for an issuer, payment processing network, and acquirer, some entities perform all or any suitable combination of these functions and may be included in embodiments of invention. Additional components may also be included in embodiments of the invention.

[0053] FIG. 7 shows typical components or subsystems of a computer apparatus. Such components or any subset of such components may be present in various components shown in FIG. 1, including the access device **34**, server computers **26(a)**, **28(a)**, etc. The subsystems shown in FIG. 7 are interconnected via a system bus **775**. Additional subsystems such as a printer **774**, keyboard **778**, fixed disk **779**, monitor **776**, which is coupled to display adapter **782**, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller **771**, can be connected to the computer system by any number of means known in the art, such as serial port **777**. For example, serial port **777** or external interface **781** can be used to connect the computer apparatus to a wide area network such as

the Internet, a mouse input device, or a scanner. The interconnection via system bus **775** allows the central processor **773** to communicate with each subsystem and to control the execution of instructions from system memory **772** or the fixed disk **779**, as well as the exchange of information between subsystems. The system memory **772** and/or the fixed disk **779** may embody a computer readable medium.

[0054] II. Methods

[0055] Methods according to embodiments of the invention can be described with reference to FIGS. 1 and 4. In a typical purchase transaction, the consumer **30** purchases a good or service at the merchant **22** using a portable consumer device **32** such as a credit card. The consumer's portable consumer device **32** can interact with an access device **34** such as a POS (point of sale) terminal at the merchant **22** (step **102**). For example, the consumer **30** may take a credit card and may swipe it through an appropriate slot in the POS terminal. Alternatively, the POS terminal may be a contactless reader, and the portable consumer device **32** may be a contactless device such as a contactless card.

[0056] A first authorization request message is then forwarded to the acquirer **24**. After the acquirer **24** receives the first authorization request message, the first authorization request message is then sent to the payment processing network **26** (step **104**). The first authorization request message is then received at the payment processing network server **26(a)** and the payment processing network server **26(a)** then determines if a challenge is needed.

[0057] Various criteria may be used to determine if a challenge is needed. For example, the payment processing network server **26(a)** may determine that the particular transaction is a high value transaction (e.g., greater than $1000) and that a challenge is therefore appropriate. In another example, the payment processing network server **26(a)** may determine that there is something suspicious about the present transaction and may thereafter determine that a challenge is appropriate. For example, the payment processing network server **26(a)** may determine that the portable consumer device **32** is currently being used at a location which is different from the consumer's home state, and the consumer's recent purchase history suggests that the consumer is not traveling.

[0058] Once it has been determined that a challenge is appropriate for the present transaction, the challenge question engine **26(a)-1** may then fetch (local or remote) a challenge question (step **108**). In some embodiments, the challenge question engine **26(a)-1** may retrieve the question from the challenge question database **26(c)**.

[0059] At this point, rather than sending the first authorization request message to the issuer **26**, the payment processing network **26** sends a first authorization response message back to the access device **34** via the merchant **22** and the acquirer **24** (step **110**). The first authorization response message may contain data representing the challenge request that was previously obtained by the challenge question engine **26(a)-1**. The challenge request may be a challenge question sent by the backend or an order to the access device to issue a challenge based on a set of preloaded question in the access device. The first authorization response message may be characterized as an initial decline, since it does not indicate approval of the transaction.

[0060] Once the challenge question is received at the access device **34**, the consumer **30** supplies the challenge response to the access device **34**. The challenge response may be supplied to the access device **34** in any suitable manner (e.g., through a keypad, contactless reader, etc.). Once the access device **34** receives the challenge response, the access device **34** then forwards the challenge response to the payment processing network server **26(a)** via the merchant **22** and the acquirer **24**, and it is received by them (step **112**). The challenge response (or the challenge and response or the challenge pointer and response) message may be part of a second authorization request message.

[0061] The payment processing network server **26(a)** then validates the challenge response message (step **114**). If the challenge response message is not validated, then the payment processing network server **26(a)** may send a response message back to the access device **34** indicating that that transaction is not approved. Alternatively or additionally, the payment processing network server **26(a)** may send another challenge question to the access device **34**. On other hand, if the challenge is validated, the payment processing network server **26(a)** may send the second authorization request message to the issuer **28** (step **116**) along with an

indication that the consumer **30** has satisfied any challenges posed by the payment processing network **26**.

[0062] After the issuer **28** receives the second authorization request, the issuer **28**, using the issuer server **28(a)**, determines if the transaction is authorized or is not authorized (step **118**). The transaction may not be authorized because the consumer **30** has insufficient funds or credit. If the consumer **30** does have sufficient funds or credit, the issuer **28** may then send a second authorization response message indicating that the transaction is authorized back to the access device **34** via the payment processing network **26**, the acquirer **24**, and the merchant **22** (step **122**).

[0063] At the end of the day, a normal clearing and settlement process can be conducted by the transaction processing system **26**. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position. Clearing and settlement can occur simultaneously.

[0064] A number of alternative embodiments are also possible. For example, the issuer **28** could generate challenge questions and send them to the consumer **30** instead of or in addition to the payment processing network **26**. The challenge question engine **28(b)-1**, the transaction history database **28(b)**, and the challenge question database **26(c)** operated by the issuer **28** may be used in the same or different way as the above-described challenge question engine **26(a)-1**, the transaction history database **26(b)**, and the challenge question database **26(c)** operated by the payment processing network **26**.

[0065] In the above-described embodiments, there are two authorization request messages that are sent to the payment processing network **26** (and/or the issuer **28**). This is desirable, since existing payment processing systems have "timers" that are set at various points between the access device **34** and the issuer **28** during a payment authorization process. The timers time how long various events should take place during the payment authorization process. The timers may be set and embodied as computer code at the acquirer **24**, the payment processing network **26**, and the issuer **28**. For example, the timers at the acquirer **24**, payment processing network **26**, and issuer **28** may be respectively set to 3 seconds, 6

seconds, and 10 seconds. If an authorization request message is not received within these respective times, then some event may be triggered. For instance, an error message may be sent back to the access device **34** requesting that the merchant **22** resubmit the authorization request message, if an authorization request message is not received at the issuer **28** within 10 seconds. If a challenge request is created during the authorization process and before the authorization request message reaches the issuer **28**, the issuer's timer may trigger an event indicating that an error has occurred. Creating challenge requests and responses during a single authorization process could potentially conflict with pre-existing timers in a payment system.

[0066] By using at least two authorization request messages in two separate authorization processes, the above-described timers are advantageously not affected. The timers need not be changed to send challenge questions to the consumer **30**. This allows embodiments of the invention to be used with an existing payments infrastructure and widespread changes are not needed in embodiments of the invention. In comparison, if the retrieval of a challenge question during a payment authorization process occurs using a single authorization request message, this may delay the authorization request message and may necessitate changes in timers present in a payment processing system.

[0067] The at least two authorization request messages may have information such as BINs (bank identification numbers), transaction amounts, account numbers, service codes, etc. They may also contain the same transaction amount for the transaction being conducted, and/or different transaction amounts. For example, the first authorization request message may have the actual transaction amount, and the second authorization request message may have a zero dollar amount or other identifier to indicate that that prior authentication request with a transaction amount has already been submitted. A transaction code may be used to link the first and second authorization requests in some embodiments.

[0068] The method described with respect to FIG. 4 can be characterized as a "closed channel" process since the access device **34** receives a challenge question and provides a response to the challenge question. However, other embodiments of the invention may use open channel solutions whereby a challenge question may be

sent to a device other than the access device which sent the first authorization response message.

[0069] Examples of open channel methods according to embodiments of the invention can be described with reference to FIGS. 1 and 5. In a typical purchase transaction, the consumer **30** purchases a good or service at the merchant **22** using a portable consumer device **32** such as a credit card. The consumer's portable consumer device **32** can interact with an access device **34** such as a POS (point of sale) terminal at the merchant **22** (step **202**). For example, the consumer **30** may take a credit card and may swipe it through an appropriate slot in the POS terminal. Alternatively, the POS terminal may be a contactless reader, and the portable consumer device **32** may be a contactless device such as a contactless card.

[0070] A first authorization request message is then forwarded to the acquirer **24**. After receiving the first authorization request message, the first authorization request message is then sent to the payment processing network **26** (step **204**). The first authorization request message is received at the payment processing network server **26(a)** and the payment processing network server **26(a)** then determines if a challenge is needed.

[0071] Various criteria may be used to determine if a challenge is needed. For example, the payment processing network server **26(a)** may determine that the particular transaction is a high value transaction (e.g., greater than $1000) and that a challenge is therefore appropriate. In another example, the payment processing network server **26(a)** may determine that there is something suspicious about the present transaction and may thereafter determine that a challenge is appropriate.

[0072] Once it has been determined that a challenge is appropriate for the present transaction, the challenge question engine **26(a)-1** may then fetch (local or remote) a challenge question (step **208**). In some embodiments, the challenge question engine **26(a)-1** may retrieve the question from the challenge question database **26(c)**.

[0073] Rather than sending the first authorization request message to the issuer **26**, and rather than sending a first authorization response message back to the access device **34**, the payment processing network **26** sends a first authorization response message back to the consumer's mobile phone **34** (step **210**) or other type

of access device. The first authorization response message may be sent back to the consumer's mobile phone **34**. This can be done directly or through some intermediate entity. The first authorization response message may contain data representing the challenge request that we previously obtained by the challenge question engine **26(a)-1**. The first authorization response message may be characterized as an initial decline, since it does not indicate approval of the transaction.

[0074] Once the challenge question is received at the mobile phone **34**, the consumer **30** supplies the challenge response to the access device **34** (step **212**) The access device **34** then forwards the challenge response to the payment processing network server **26(a)** via the merchant **22** and the acquirer **24**, and it is received by them (step **214**). The challenge response message may be part of a second authorization response message.

[0075] Note that although challenge questions that the user actively answers are described in detail with respect to FIG. 5, other types of challenge requests may be sent to the mobile phone **34**. For example, in some cases, the challenge requests may not require an answer that is actively provided by the consumer **30**. Passive answers to challenge requests may be provided. For example, in some embodiments, the challenge request supplied to the mobile phone **34** may be a query regarding the physical location of the mobile phone **34**. The mobile phone **34** may have a GPS device or other location device and this information (or other information such as a cryptogram, etc.) may be transmitted to the payment processing network **26**, and the payment processing network **26** may authenticate the consumer **34** using this location information.

[0076] Once the payment processing network server **26(a)** receives the challenge response message, the payment processing network server **26(a)** then validates the challenge response message (step **216**). If the challenge response message is not validated, then the payment processing network server **26(a)** may send a response message back to the access device **34** indicating that that transaction is not approved. Alternatively or additionally, the payment processing network server **26(a)** may send another challenge message to the access device **34** and/or the mobile phone **34**. On other hand, if the challenge is validated, the

payment processing network server **26(a)** may then send the second authorization request message to the issuer **28** (step **218**) along with an indication that the consumer **30** has satisfied any challenges posed by the payment processing network **26**.

[0077] After the issuer **28** receives the second authorization request, the issuer **28** using the issuer server **28(a)** determines if the transaction is authorized or is not authorized (step **220**). The transaction may not be authorized because the consumer **30** has insufficient funds or credit. If the consumer **30** does have sufficient funds or credit, the issuer **28** may then send a second authorization response message indicating that the transaction is authorized back to the access device **34** via the payment processing network **26**, the acquirer **24**, and the merchant **22** (step **222**).

[0078] At the end of the day, a normal clearing and settlement process can be conducted by the transaction processing system **26**. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position. Clearing and settlement can occur simultaneously.

[0079] A number of alternative embodiments are also possible. For example, the issuer **28** could generate challenge questions and send them to the mobile phone **34** instead of or in addition to the payment processing network **26**. The challenge question engine **28(b)-1**, the transaction history database **28(b)**, and the challenge question database **26(c)** operated by the issuer **28** may be used in the same or different way as the above-described challenge question engine **26(a)-1**, the transaction history database **26(b)**, and the challenge question database **26(c)** operated by the payment processing network **26**.

[0080] In another embodiment, instead of sending a challenge question, the payment processing network server **26(a)** may send an electronic coupon to the consumer's mobile phone **34**. The payment processing network **26** may determine that a challenge is appropriate and may send the electronic coupon to the phone **34**. Upon receipt of this electronic coupon, the consumer may then be prompted to use the coupon at the access device **34**. If the consumer **30** uses the coupon at the access device **34**, then access device **34** forwards the coupon to the payment

processing network **26**, and receipt of the coupon by the payment processing network **26** indicates that the consumer **30** is authenticated. It is presumed that the consumer **30** is authentic since a non-authentic consumer would not be in possession of the consumer's phone **34**.

[0081] **III. Transaction Authentication**

[0082] The above-described challenge authentication process is a process for authenticating a consumer and can be part of a larger overall "transaction authentication" process.

[0083] FIG. 6 shows a conceptual block diagram **100**, the authentication of a purchase transaction can have various aspects. Such aspects include portable consumer device authentication **100(a)**, consumer authentication **100(b)**, back end processing including real time risk analysis **100(c)**, and consumer notification of the purchase transaction **100(d)**.

[0084] Portable consumer device authentication relates to the authentication of the portable consumer device. That is, in a portable consumer device authentication process, a determination is made as to whether the portable consumer device that is being used in the purchase transaction is the authentic portable consumer device or a counterfeit portable consumer device. Specific exemplary techniques for improving the authentication of a portable consumer device include:

- Dynamic CVV on portable consumer devices such as magnetic stripe cards
- Card security features (existing and new)
- Contactless chips (limited use)
- Magnetic stripe identification
- Card Verification Values (CVV and CVV2)
- Contact EMV chips

[0085] Consumer authentication relates to a determination as to whether or not the person conducting the transaction is in fact the owner or authorized user of

the portable consumer device. Conventional consumer authentication processes are conducted by the merchants. For example, merchants may ask to see a credit card holder's driver's license, before conducting a business transaction with the credit card holder. Other ways to authenticate the consumer would be desirable, since consumer authentication at the merchant does not occur in every instance. Specific examples of possible ways to improve the consumer authentication process include at least the following:

- Knowledge-based challenge-responses
- Hardware tokens (multiple solution options)
- OTPs (one time password, limited use)
- AVSs (not as a stand alone solution)
- Signatures
- Software tokens
- PINs (online/offline)
- User IDs/Passcodes
- Two-channel authentication processes (e.g., via phone)
- Biometrics

[0086] Back end processing relates to processing that may occur at the issuer or payment processing network, or other non-merchant location. Various processes may be performed at the "back end" of the payment transaction to help ensure that any transactions being conducted are authentic. Back end processing may also prevent transactions that should not be authorized, and can allow transactions that should be authorized.

[0087] Lastly, consumer notification is another aspect of transaction authentication. In some cases, a consumer may be notified that a purchase transaction is occurring or has occurred. If the consumer is notified (e.g., via cell phone) that a transaction is occurring using his portable consumer device, and the consumer is in fact not conducting the transaction, then appropriate steps may be

taken to prevent the transaction from occurring. Specific examples of consumer notification processes include:

- Purchase notification via SMS
- Purchase notification via e-mail
- Purchase notification by phone

[0088] Other details regarding some of the above-described aspects are provided in U.S. Provisional Patent Application No. 60/815,059, filed on June 19, 2006, U.S. Provisional Patent Application No. 60/815,430 filed on June 20, 2006, and U.S. Provisional Patent Application No. 60/884,089 filed on January 9, 2007, which are herein incorporated by reference in their entirety for all purposes. The specific details of the specific aspects may be combined in any suitable manner without departing from the spirit and scope of embodiments of the invention. For example, portable consumer device authentication, consumer authentication, back end processing, and consumer transaction notification may all be combined in some embodiments of the invention. However, other embodiments of the invention may be directed to specific embodiments relating to each individual aspects, or specific combinations these individual aspects.

[0089] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software

[0090] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a

single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0091] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0092] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0093] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0094] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving an authorization request message associated with a consumer conducting a transaction with a portable consumer device;

sending a challenge message to the consumer, wherein the challenge message is dynamic or semi-dynamic;

receiving a challenge response message from the consumer; and

sending an authorization response message to the consumer, wherein the authorization response message indicates whether or not the transaction is authorized.

2. The method of claim 1 wherein the portable consumer device is in the form of a card or a mobile phone.

3. The method of claim 1 wherein the challenge message includes a question which is dynamic.

4. The method of claim 1 wherein the challenge question is dynamic, and uses the consumer's transaction history to create the challenge question.

5. The method of claim 1 wherein the authorization request message is received at a payment processing network, and wherein the payment processing network sends the challenge message to the consumer, and receives the challenge response message from the consumer, and if the consumer provides a correct challenge response message:

forwarding the authorization request message to an issuer of the portable consumer device; and

receiving the authorization response message from the issuer before sending the authorization response message to the consumer.

6. The method of claim 5 wherein the transaction involves a merchant, and wherein the authorization response message is sent to the consumer via an access device operated by a merchant.

7. The method of claim 5 wherein the transaction involves a merchant, and wherein the authorization response message is sent to the portable consumer device.

8. The method of claim 1 wherein the authorization request message is received at an issuer, and the issuer sends the challenge message to the consumer, and receives the challenge response message from the consumer, and wherein the issuer further analyzes the challenge response message from the consumer to determine if the consumer provides a correct challenge response message before sending the authorization response message to the consumer.

9. The method of claim 1 wherein the challenge message includes a question which is dynamic, and uses the consumer's location to create the challenge message.

10. A computer readable medium comprising:
code for performing the method of claim 1.

11. A server computer comprising the computer readable medium of claim 10.

12. A system comprising the server computer of claim 11.

13. A system comprising:
means for receiving an authorization request message associated with a consumer conducting a transaction with a portable consumer device;
means for sending a challenge message to the consumer, wherein the challenge question is dynamic or semi-dynamic;
means for receiving a challenge response message from the consumer; and
means for sending an authorization response message to the consumer, wherein the authorization response message indicates whether or not the transaction is authorized.

14. A method comprising:

initiating an authorization request message, wherein the authorization request message is associated with a consumer conducting a transaction with a portable consumer device and is sent to an issuer associated with the portable consumer device;

receiving a challenge message, wherein the challenge message is dynamic or semi-dynamic;

initiating a challenge response message, wherein the challenge response message is responsive to the challenge message; and

receiving an authorization response message, wherein the authorization response message indicates whether or not the transaction is authorized.

15. The method of claim 14 wherein the authorization request message and the challenge question are initiated by at least one of a merchant who is a party to the transaction or the consumer.

16. A computer readable medium comprising:

code for initiating an authorization request message, wherein the authorization request message is associated with a consumer conducting a transaction with a portable consumer device and is sent to an issuer associated with the portable consumer device;

code for receiving a challenge message, wherein the challenge message is dynamic or semi-dynamic;

code for initiating a challenge response message, wherein the challenge response message is responsive to the challenge message; and

code for receiving an authorization response message, wherein the authorization response message indicates whether or not the transaction is authorized.

17. A phone comprising the computer readable medium of claim 16.

18. A system comprising:

means for initiating an authorization request message, wherein the authorization request message is associated with a consumer conducting a transaction with a portable consumer device and is sent to an issuer associated from the portable consumer device;

means for receiving a challenge message, wherein the challenge message is dynamic or semi-dynamic;

means for initiating a challenge response message, wherein the challenge response message is responsive to the challenge message; and

means for receiving an authorization response message, wherein the authorization response message indicates whether or not the transaction is authorized.

19. An authentication method comprising:

receiving, at an issuer, an authorization request message sent from an access device; and

in response to receipt of the authorization request, providing one or more dynamic challenge questions to the consumer before authorizing a transaction.

20. The authentication method of claim 19 wherein the dynamic challenge questions are generated by the issuer and are related to past transactions conducted by a consumer.

21. A computer readable medium comprising:

code for receiving, at an issuer, an authorization request message sent from an access device; and

code for providing one or more dynamic challenge questions to the consumer before authorizing a transaction conducted by a consumer.

22. A method comprising:

receiving a first authorization request message associated with a consumer conducting a transaction with a portable consumer device;

sending a challenge message to the consumer;

receiving a second authorization request message including a challenge response message; and

sending an authorization response message, wherein the authorization response message indicates whether or not the transaction is authorized.

23. The method of claim 22 wherein the challenge message is sent to a mobile phone operated by the consumer.

24. A computer readable medium comprising code for performing the method of claim 22.

25. A server comprising the computer readable medium of claim 24.

26. A method comprising:

sending a first authorization request message associated with a consumer conducting a transaction using a portable wireless device;

receiving a challenge message;

sending a second authorization request message including a challenge response message; and

receiving an authorization response message, wherein the authorization response message indicates whether or not the transaction is authorized.

27. The method of claim 26 wherein the challenge message is received at a mobile phone operated by the consumer and wherein the authorization response message is received an access device, wherein the access device comprises a point of sale terminal.

28. The method of claim 26 wherein the challenge message is a challenge question.

29. A computer readable medium comprising code for performing the method of claim 26.

30. A point of sale device comprising the computer readable medium of claim 29.

31. The method of claim 22 wherein the challenge message is passive and does not require an active response by the consumer.

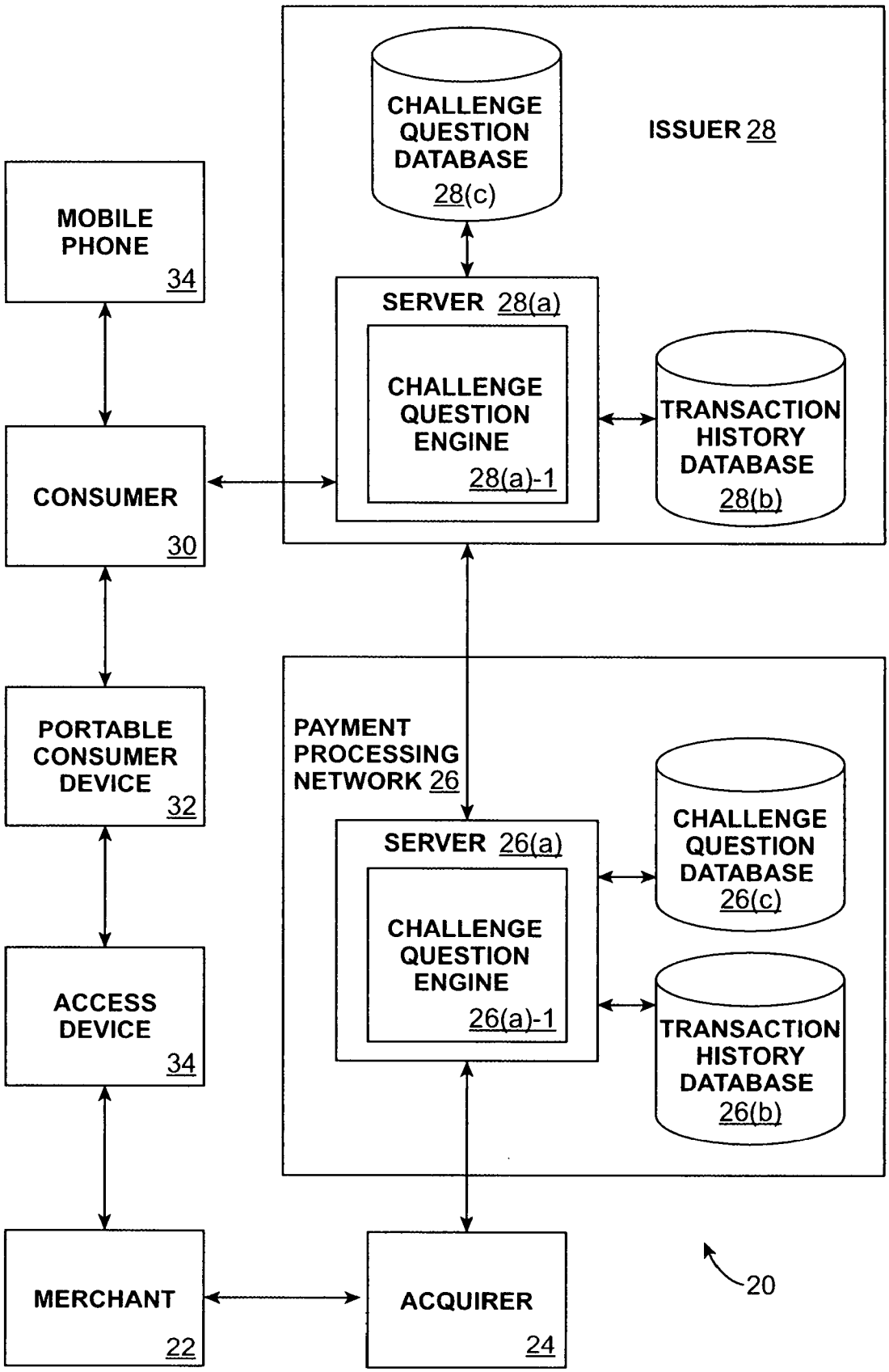

CHALLENGE QUESTION DATABASE 28(c)
ISSUER 28
MOBILE PHONE 34
SERVER 28(a)
CHALLENGE QUESTION ENGINE 28(a)-1
TRANSACTION HISTORY DATABASE 28(b)
CONSUMER 30
PORTABLE CONSUMER DEVICE 32
PAYMENT PROCESSING NETWORK 26
SERVER 26(a)
CHALLENGE QUESTION DATABASE 26(c)
CHALLENGE QUESTION ENGINE 26(a)-1
TRANSACTION HISTORY DATABASE 26(b)
ACCESS DEVICE 34
MERCHANT 22
ACQUIRER 24
20

FIG. 1

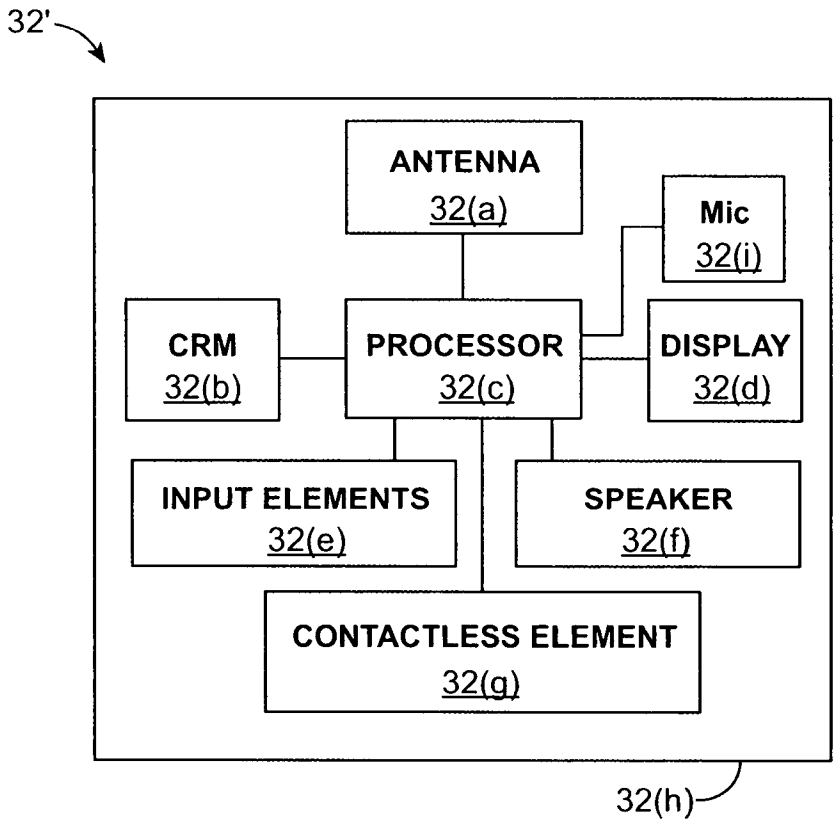

32'
ANTENNA
32(a)
Mic
32(i)
CRM
32(b)
PROCESSOR
32(c)
DISPLAY
32(d)
INPUT ELEMENTS
32(e)
SPEAKER
32(f)
CONTACTLESS ELEMENT
32(g)
32(h)

FIG. 2

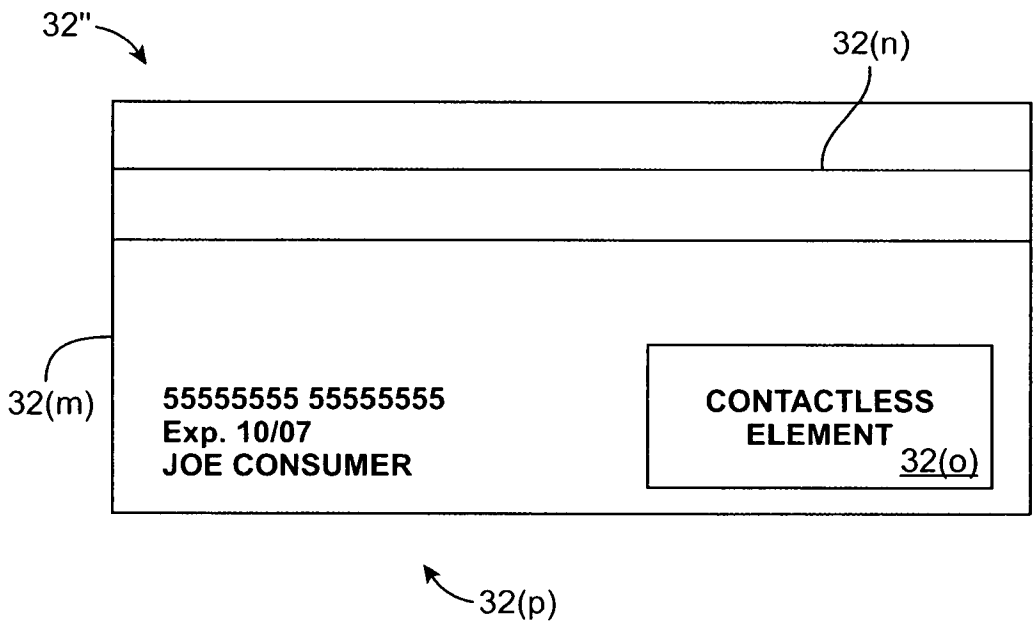

32"
32(n)
32(m)
55555555 55555555
Exp. 10/07
JOE CONSUMER
CONTACTLESS ELEMENT
32(o)
32(p)

FIG. 3

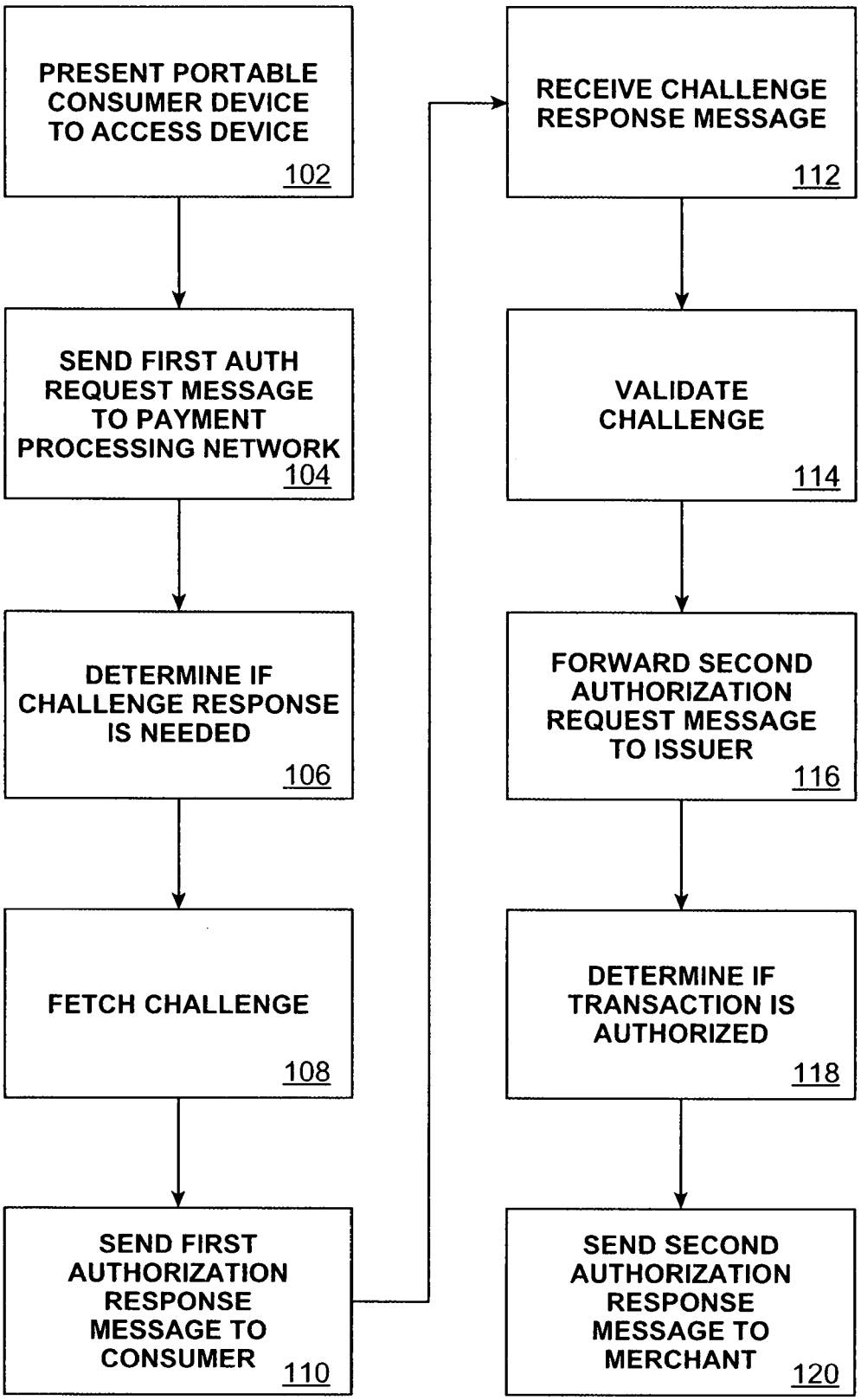

PRESENT PORTABLE CONSUMER DEVICE TO ACCESS DEVICE
102
SEND FIRST AUTH REQUEST MESSAGE TO PAYMENT PROCESSING NETWORK
104
DETERMINE IF CHALLENGE RESPONSE IS NEEDED
106
FETCH CHALLENGE
108
SEND FIRST AUTHORIZATION RESPONSE MESSAGE TO CONSUMER
110
RECEIVE CHALLENGE RESPONSE MESSAGE
112
VALIDATE CHALLENGE
114
FORWARD SECOND AUTHORIZATION REQUEST MESSAGE TO ISSUER
116
DETERMINE IF TRANSACTION IS AUTHORIZED
118
SEND SECOND AUTHORIZATION RESPONSE MESSAGE TO MERCHANT
120

FIG. 4

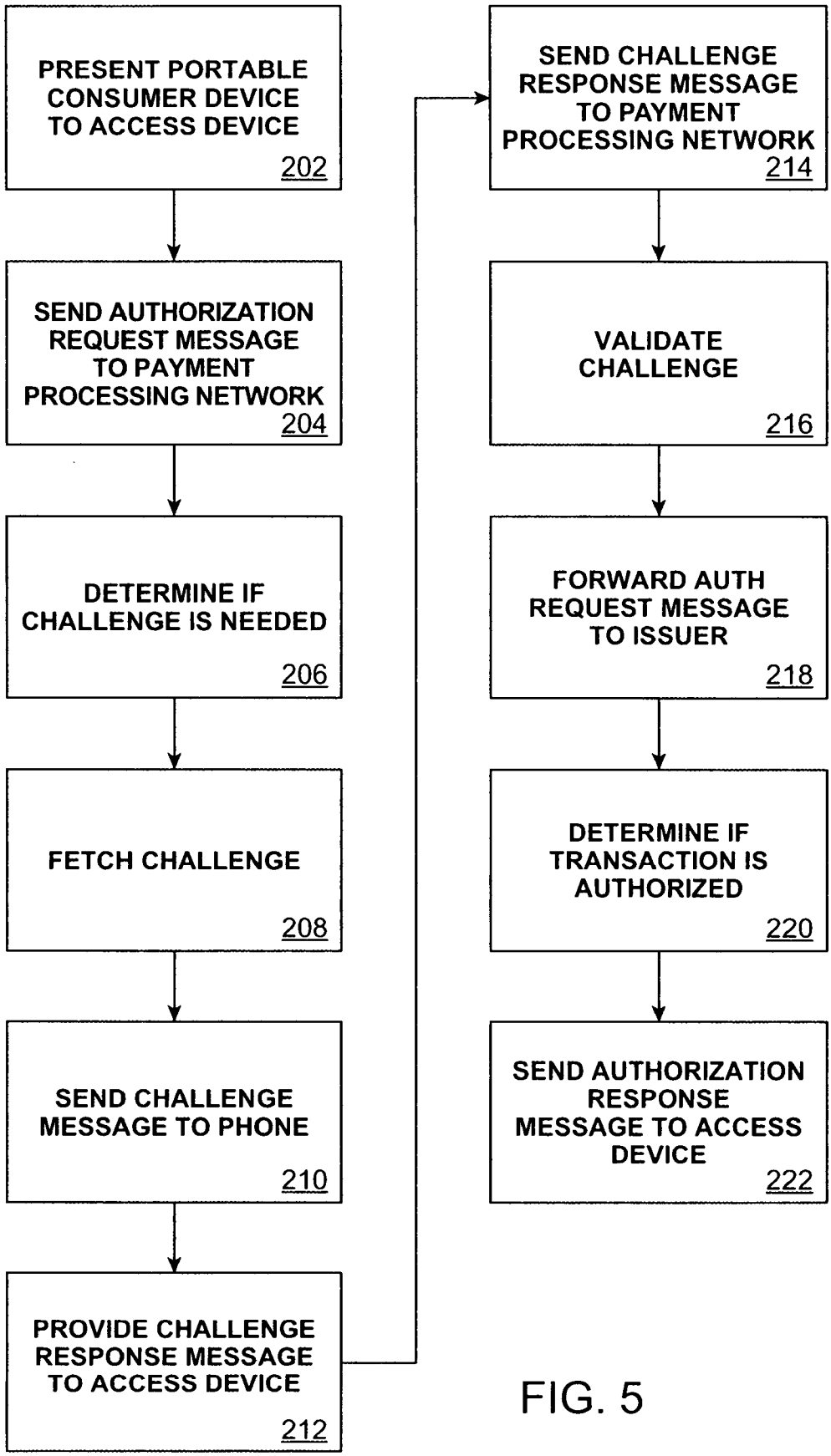

PRESENT PORTABLE CONSUMER DEVICE TO ACCESS DEVICE
202
SEND AUTHORIZATION REQUEST MESSAGE TO PAYMENT PROCESSING NETWORK
204
DETERMINE IF CHALLENGE IS NEEDED
206
FETCH CHALLENGE
208
SEND CHALLENGE MESSAGE TO PHONE
210
PROVIDE CHALLENGE RESPONSE MESSAGE TO ACCESS DEVICE
212
SEND CHALLENGE RESPONSE MESSAGE TO PAYMENT PROCESSING NETWORK
214
VALIDATE CHALLENGE
216
FORWARD AUTH REQUEST MESSAGE TO ISSUER
218
DETERMINE IF TRANSACTION IS AUTHORIZED
220
SEND AUTHORIZATION RESPONSE MESSAGE TO ACCESS DEVICE
222

FIG. 5

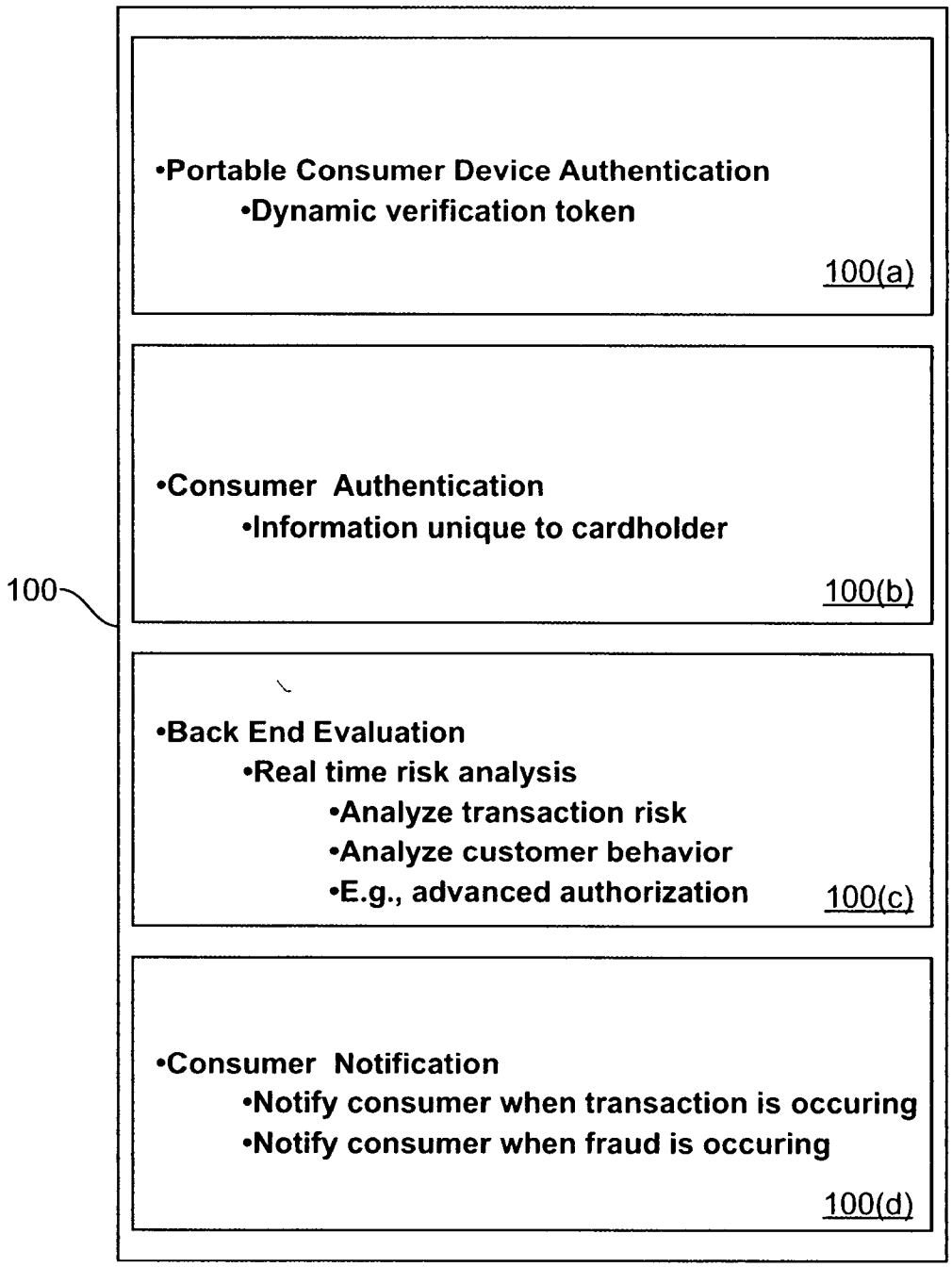

•Portable Consumer Device Authentication
•Dynamic verification token
100(a)
•Consumer Authentication
•Information unique to cardholder
100(b)
100
•Back End Evaluation
•Real time risk analysis
•Analyze transaction risk
•Analyze customer behavior
•E.g., advanced authorization
100(c)
•Consumer Notification
•Notify consumer when transaction is occuring
•Notify consumer when fraud is occuring
100(d)

FIG. 6

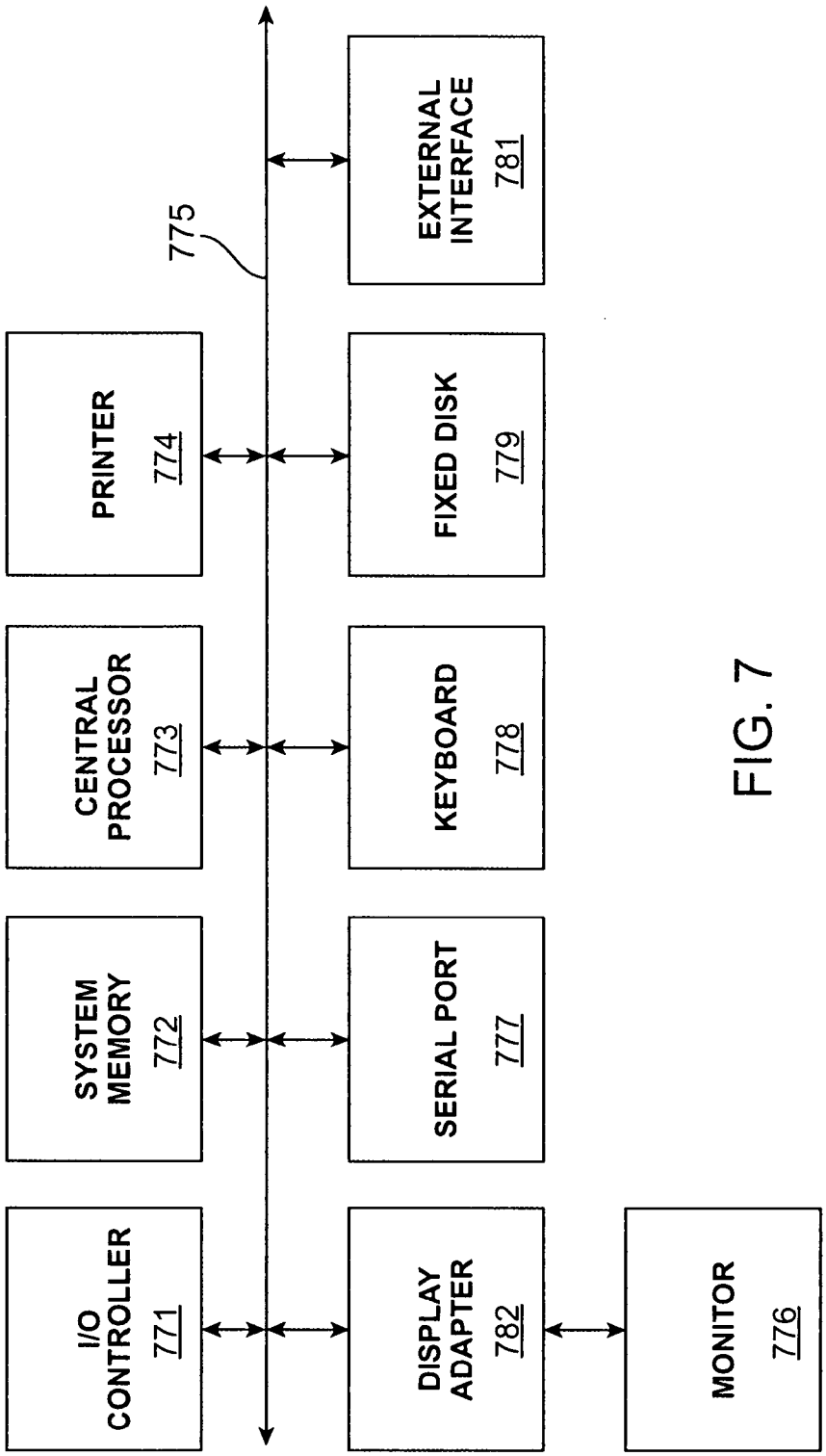

775
I/O CONTROLLER 771
SYSTEM MEMORY 772
CENTRAL PROCESSOR 773
PRINTER 774
DISPLAY ADAPTER 782
SERIAL PORT 777
KEYBOARD 778
FIXED DISK 779
MONITOR 776
EXTERNAL INTERFACE 781

FIG. 7