(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 2007/149785 A2

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

(21) International Application Number:
PCT/US2007/071376

(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).

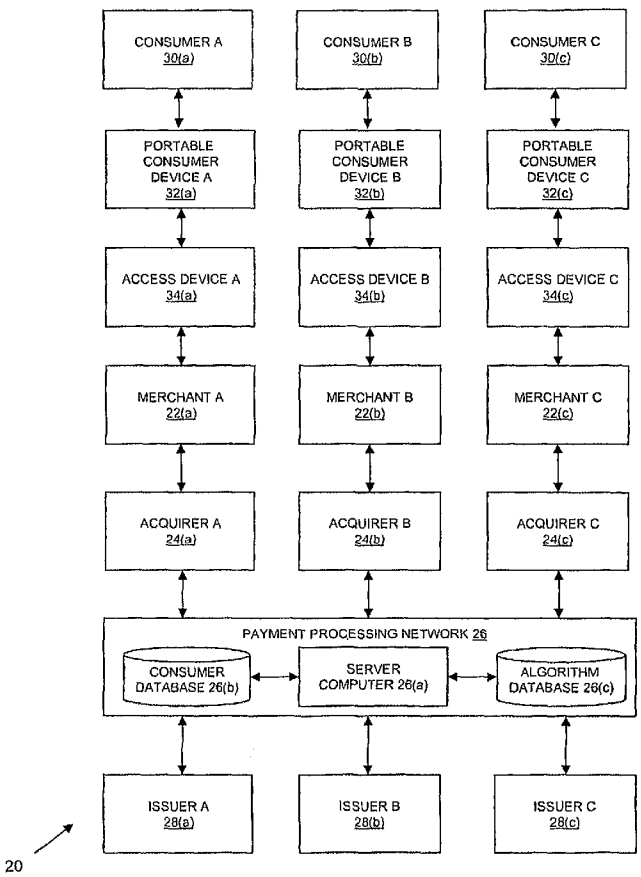
(74) Agents: **JEWIK, Patrick R.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, California 94111-3834 (US).

(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: PORTABLE CONSUMER DEVICE VERIFICATION SYSTEM



(57) Abstract: A method for verifying a portable consumer device. The method includes receiving an authorization request message associated with a transaction conducted using a portable consumer device. The portable consumer device includes a portable consumer device fingerprint. The authorization request message includes an altered portable consumer device fingerprint and an algorithm identifier. The method also includes selecting an algorithm from among a plurality of algorithms using the algorithm identifier, determining the portable consumer device fingerprint using selected algorithm and the altered portable consumer device fingerprint, determining if the portable consumer device fingerprint matches a stored portable consumer device fingerprint, and sending an authorization response message after determining if the portable consumer device fingerprint matches the stored portable consumer device fingerprint.

WO 2007/149785 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.

PORTABLE CONSUMER DEVICE VERIFICATION SYSTEM

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 OF THE INVENTION

[0002] Under certain circumstances, thieves can "skim" a card, by copying the data on the magnetic stripe of the card. If the data on the magnetic stripe on a payment card is skimmed, an unauthorized user can create a fake card with the copied data. The fake card can then be used in a fraudulent manner.

[0003] A number of security mechanisms are offered by a number of companies. Some companies have developed ways in which a specific pattern of magnetic particles can be embedded in the magnetic stripe of a credit card. The magnetic stripe may encode consumer data such as an account number, and the magnetic stripe itself may have a unique fingerprint that is defined by the specific pattern of magnetic particles. The fingerprint may be used to identify and authenticate the card that is being used. That is, even if thief is able to skim consumer data from a portable consumer device, the thief will not be able to obtain the unique fingerprint. This technology is commercially available from Magtek™.

[0004] Although the use of this technology would help authenticate credit cards and the like, the widespread adoption of this technology is not practical as software and hardware changes would be needed for thousands of point of sale terminals. In practice, in a payment processing system, many different types of authentication technologies would be used and there is a need to provide for systems which can use many of these types of different technologies. Hence, there

is a need for systems and methods, which can integrate such technologies and use them effectively.

[0005] Embodiments of the invention address the above problems and other problems individually and collectively.

SUMMARY OF THE INVENTION

[0006] Embodiments of the invention includes systems and methods for authenticating portable consumer devices such as payment cards.

[0007] One embodiment of the invention is directed to a method for verifying a portable consumer device. The method includes receiving an authorization request message associated with a transaction conducted using a portable consumer device. The portable consumer device includes a portable consumer device fingerprint. The authorization request message includes an altered portable consumer device fingerprint and an algorithm identifier. The method also includes selecting an algorithm from among a plurality of algorithms using the algorithm identifier, determining the portable consumer device fingerprint using selected algorithm and the altered portable consumer device fingerprint, determining if the portable consumer device fingerprint matches a stored portable consumer device fingerprint, and sending an authorization response message after determining if the portable consumer device fingerprint matches the stored portable consumer device fingerprint.

[0008] Another embodiment of the invention is directed to a method comprising sending an authorization request message associated with a transaction conducted using a portable consumer device, wherein the portable consumer device comprises a portable consumer device fingerprint, and wherein the authorization request message comprises an altered portable consumer device fingerprint and an algorithm identifier. An algorithm is selected from among a plurality of algorithms using the algorithm identifier, and the portable consumer device fingerprint is determined using selected algorithm and the altered portable consumer device fingerprint. A server computer determines if the portable consumer device fingerprint matches a stored portable consumer device fingerprint, and an authorization

response message is received. The authorization response message indicates whether or not the transaction is approved.

[0009] Another embodiment of the invention is directed to a method comprising receiving an authorization request message, wherein the authorization request message is generated after an interaction between a portable consumer device and an access device. The method also includes analyzing the authorization request message for one or more characteristics or the portable consumer device or the access device to determine if a confidence threshold is met or exceeded, and if the confidence threshold is not exceeded, performing additional authentication processing.

[0010] Other embodiments of the invention are directed to systems, computer readable media, access devices, etc. used in conjunction with such methods.

[0011] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 shows a block diagram of a system according to an embodiment of the invention.

[0013] FIG. 2 shows a schematic illustration of a portable consumer device in the form of a card.

[0014] FIG. 3 shows a block diagram of an access device.

[0015] FIG. 4 shows a block diagram of some software modules that may reside on a server computer.

[0016] FIG. 5 shows a block diagram of exemplary components in a computer apparatus.

[0017] FIG. 6 shows a flowchart illustrating steps in a method according to an embodiment of the invention.

[0018] FIG. 7 shows a flowchart of a confidence assessment method according to an embodiment of the invention.

[0019] FIG. 8 shows a block diagram of components in an authentication system.

DETAILED DESCRIPTION

[0020] I. Methods using algorithm identifiers

[0021] In embodiments of the invention, a payment processing organization or other entity may support different security technologies offered by different companies. The different security technologies may use portable consumer device fingerprints. For example, two magnetic stripes on two payment cards can store identical consumer data (e.g., account number information), but the magnetic structures of the two magnetic stripes may be different. A specific magnetic structure may be an example of a fingerprint or "DNA" that is associated with a payment card. If a thief copied the consumer data stored on a magnetic stripe to an unauthorized credit card, the magnetic stripe of the unauthorized credit card would have a different magnetic structure or fingerprint than the authorized credit card. A back end server computer receiving the authorization request message in response to the unauthorized card's use would determine that the unauthorized credit card is not real, because the fingerprint is not present in the authorization request message. Two companies that offer this type of technology are Magtek™ and Semtek™. Each company uses its own proprietary algorithm in a point of sale terminal to alter (e.g., encrypt) its own fingerprint before it is sent to an issuer or other entity in a subsequent authentication process.

[0022] In embodiments of the invention, a portable consumer device fingerprint may include any suitable identification mechanism that allows one to identify the portable consumer device, independent of static consumer data such as an account number or expiration date associated with the portable consumer device. Typically, unlike consumer data, portable consumer device fingerprint data is not known to the consumer. For instance, in some embodiments, the fingerprint data may relate to characteristics of the materials from which the portable consumer devices are made. For example, as noted above, a portable consumer device fingerprint can be embedded within the particular microscopic structure of the magnetic particles in the magnetic stripe in a payment card. In some cases, no two magnetic stripes will have same portable consumer device fingerprint.

[0023] Portable consumer device fingerprints can take other forms. For example, another card verification technology comes from a company called QSecure™. The technology offered by QSecure™ uses a dynamic CVV (card verification value) that can be generated by a chip in a payment card (the chip may be under a magnetic stripe and can write the dynamic CVV or a number related to the dynamic CVV to the magnetic stripe). In this case, the dynamic CVV may act as a portable consumer device fingerprint identifying the particular portable consumer device. The dynamic CVV may be sent to a point of sale device during a payment transaction. A specific algorithm in the point of sale device may alter (e.g., encrypt) the dynamic CVV before it is sent to the issuer of the payment card for authorization. The issuer, payment processing organization, or other entity, may receive the altered dynamic CVV and may restore it to its original form. The dynamic CVV can then be checked by the back end server computer to see if it corresponds to an independently derived dynamic CVV, thereby authenticating the portable consumer device. In this example, the dynamic CVV value could also be considered a portable consumer device fingerprint, even though it is dynamic in nature.

[0024] Embodiments of the invention allow for many different types of portable consumer device fingerprinting systems to be used together in a single payment processing system. In embodiments of the invention, a different identifier or ID is assigned to each type of algorithm in each type of POS terminal. For example, a back end entity such as an issuer or a payment processing organization might use algorithm identifiers like those in Table 1 below.

Table 1

Algorithm Identifier	Description of Algorithm
01	Company A magnetic stripe fingerprint encryption algorithm
02	Company B magnetic stripe fingerprint encryption algorithm
03	Company C dynamic CVV encryption algorithm

As shown in Table 1, the algorithm ID may take any suitable form. For example, the algorithm IDs may simply be one, two, or three digit numbers.

[0025] When the POS terminal sends an authorization request message to an issuer, the authorization request message may contain the particular algorithm ID associated with the POS terminal and an altered portable consumer device fingerprint. When the authorization request message is received by a back end server computer, it can determine which algorithm was used to encrypt the portable consumer device fingerprint. The back end server computer may then decrypt the encrypted portable consumer device fingerprint and may determine if the portable consumer device fingerprint corresponds to the portable consumer device fingerprint that is stored in a back end database. The portable consumer device fingerprint may have been previously stored in the back end database along with corresponding consumer data (e.g., an account number) as part of the process of issuing the portable consumer device to the consumer who will use it.

[0026] Using such algorithm identifiers, embodiments of the invention can effectively integrate different technologies into a single payment processing system. For example, a consumer can swipe a payment card through a POS (point of sale) terminal to pay $5.00 for office supplies. The POS terminal may contain an encryption algorithm produced by Company A. The encryption algorithm may encrypt a fingerprint that is embedded in the magnetic structure of the magnetic stripe of the payment card. The POS terminal may then send an authorization request message to a back end server computer. The authorization request message may contain information including the purchase amount, consumer data such as the consumer's account number, the encrypted fingerprint, and an algorithm identifier that is specifically associated with the encryption algorithm produced by company A. The back end server computer can receive the authorization request message from a POS (point of sale) terminal. It can then determine which algorithm was used to encrypt the fingerprint, and can subsequently decrypt the fingerprint. Once the fingerprint is determined, the back end server computer can determine if the received fingerprint corresponds to the stored fingerprint. If it does, then the payment card is authenticated.

[0027] Other details regarding methods and systems that utilize algorithm identifiers are provided below.

[0028] II. Confidence Assessment Methods

[0029] In some embodiments, the back end processor, or back end server computer, can also determine whether a transaction meets a desired confidence threshold of likely validity before it determines that a portable consumer device is authenticated. If the confidence threshold is not met, additional authentication processes can be performed. Such additional authentication processes may include the sending of one or more challenge questions and/or notification messages to the consumer.

[0030] Illustratively, a back end server computer may receive an authorization request message from a POS terminal after a consumer tries to pay for office supplies using a payment card. The back end server computer may determine that one of the three card verification technologies in Table I above is present, and that there have not been any recent suspicious transactions associated the payment card. The back end server computer may thereafter determine that the transaction is valid (i.e., a confidence threshold has been met) and can proceed if the transaction is otherwise authorized by the issuer of the payment card. Conversely, if a card and reader are used to conduct the transaction and none of the three card protection technologies in Table 1 (above) is used, and the profile of the transaction deemed to be risky, then the server computer may determine that a confidence threshold has not been met, and additional authentication processes can be initiated by the server computer. For example, a dynamic challenge (query) can be sent to the consumer before approval, and/or the consumer can be notified that a transaction is occurring.

[0031] Transaction confidence determinations can also take into account whether one algorithm could be more reliable than the other. The back end server computer can evaluate the algorithm that was used at the front end (e.g., at the POS terminal) and can determine whether or not the transaction should proceed. For example, the back end server computer may determine that the algorithm from company A may have 90% reliability and the algorithm from Company B may have 50% reliability.

[0032] There are a number of reasons why different algorithms may have different levels of reliability. For example, depending on the sensitivity of the terminal, depending on the way that the card is swiped, and depending on the aging

of the card, some algorithms may be able to handle data more precisely. In this example, if the server computer receives an authorization request message indicating that the algorithm from Company B is present and there has been recent suspicious activity associated with the payment card, then additional authentication processing may be initiated. On the other hand, if the server computer receives an authorization request message indicating that the algorithm from Company A is present and there has been recent suspicious activity, then the back end server computer may not initiate additional authentication processing.

[0033] Illustratively, Retailer 1 may have a relationship with Technology Provider A and Retailer 2 may have a relationship with Technology Provider B. They have may use different algorithms at their point of sale devices. Each one delivers two sets of data using two different algorithms. When they come back to a payment processing organization such as Visa, it may identify data as originating from a Technology Provider A algorithm, and/or from Technology Provider B algorithm. Weight can be put on the algorithms so that a confidence level can be determined. Additional authentication processing may then take place if a confidence level (or threshold) is not satisfied.

[0034] **III. Exemplary Systems**

[0035] FIG. 1 shows a system **20** that can be used in an embodiment of the invention. The system **20** includes a plurality of merchants **22(a)**, **22(b)**, **22(c)** and a plurality of acquirers **24(a)**, **24(b)**, **24(c)** associated with the merchants **22(a)**, **22(b)**, **22(c)**. In typical payment transactions, consumers **30(a)**, **30(b)**, **30(c)** may purchase goods or services at the merchants **22(a)**, **22(b)**, **22(c)** using their portable consumer devices **32(a)**, **32(b)**, **32(c)**. The consumers **30(a)**, **30(b)**, **30(c)** may be individuals, or organizations such as businesses. The acquirers **24(a)**, **24(b)**, **24(c)** can communicate with the issuers **28(a)**, **28(b)**, **28(c)** via a payment processing network **26**. The issuers **28(a)**, **28(b)**, **28(c)** may respectively issue portable consumer devices **30(a)**, **30(b)**, **30(c)** to the consumers **30(a)**, **30(b)**, **30(c)**.

[0036] For purposes of illustration, access device A **32(a)** may be produced by Company A, which may be associated with an algorithm with an algorithm identifier "01". Access device B **32(b)** may be produced by Company B and may be

associated with an algorithm with an algorithm identifier "02". Access device C **32(c)** may be associated with Company D and may have no algorithm associated with it.

[0037] The portable consumer devices **32(a)**, **32(b)**, **32(c)** may be in any suitable form. For example, suitable portable consumer devices **32(a)**, **32(b)**, **32(c)** 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, 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).

[0038] FIG. 2 shows a schematic illustration of a portable consumer device **32** in the form of a card. The portable consumer device **32** includes a contactless element **32(c)** comprising a memory device **32(c)-1** such as a chip, and an antenna **32(c)-2** operatively coupled to the memory device **32(c)-1**. FIG. 2 also shows consumer data **32(a)** comprising an account number (e.g., 1234 5678 1234 5678), an account name (e.g., Joe Consumer), and an expiration date (e.g., 10/10) associated with the portable consumer device **32**. The portable consumer device **32** may also comprise a magnetic stripe **32(b)**.

[0039] Information in the memory device **32(c)-1** or stripe **32(b)** may also be in the form of data tracks that are traditionally associated with credits cards. Such tracks include Track 1, Track 2 and other chip or account data . 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 number, encrypted PIN data, plus other discretionary or supplemental data.

[0040] The merchants **22(a)**, **22(b)**, **22(c)** may also have, or may receive communications from, respective access devices **34(a)**, **34(b)**, **34(c)** that can interact with the portable consumer devices **32(a)**, **32(b)**, **32(c)**. 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.

[0041] If the access device 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(a)**, **32(b)**, **32(c)**.

[0042] FIG. 3 shows a block diagram of an access device **32** according to an embodiment of the invention. The access device **32** comprises a processor **32(a)-1** operatively coupled to a computer readable medium **32(a)-2** (e.g., one or more memory chips, etc.), input elements **32(a)-3** such as buttons or the like, a reader **32(a)-4** (e.g., a contactless reader, a magnetic stripe reader, etc.), an output device **32(a)-5** (e.g., a display, a speaker, etc.) and a network interface **32(a)-6**.

[0043] The payment processing network **26** may include data processing subsystems, networks, and operations used to support and deliver authorization services, routing and switching, exception file services, and clearing and settlement services. An exemplary payment processing system may include VisaNet™. Payment processing systems 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.

[0044] The payment processing network **26** may include a server computer **26(a)**. 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 system **26** may use any suitable wired or wireless network, including the Internet. It may include a processor a computer readable medium comprising instructions (described herein) executable by the processor.

[0045] The server computer **26(a)** may comprise any suitable number of software modules and they may be of any suitable type. As shown in FIG. 4, the server computer **26(a)** may comprise an algorithm identification module **26(a)-1** and a confidence assessment module **26(a)-2**. It may also comprise a decryption module **26(a)-3**, as well as a data formatter module **26(a)-4**.

[0046] The algorithm identification module **26(a)-1**, in conjunction with the decryption module **26(a)-3**, may review a received authorization request message including an algorithm ID and an altered portable consumer device fingerprint. From the received algorithm ID, it may then determine which algorithm was used to alter (e.g., encrypt) the portable consumer device fingerprint. A lookup table or the like may be used to identify correspondence between the algorithm ID, the algorithm(s) used to alter a portable consumer device fingerprint or restore an altered portable consumer device fingerprint, and consumer data (e.g., an account number). (In some cases, the algorithm may be a key in an encryption process.) The server computer **26(a)** may then be used to determine (e.g., by unencrypting) the portable consumer device fingerprint from the altered portable consumer device fingerprint in an authorization request message. Once the portable consumer device fingerprint is determined, this information may be analyzed to determine if it corresponds to a stored fingerprint linked to consumer data (e.g., account number) associated with the portable consumer device.

[0047] The confidence assessment module **26(a)-2** may generate a confidence assessment from various pieces of information. Such information may include the type of portable consumer device used (e.g., a phone may be more secure than a payment card), the type of algorithm used to encrypt the portable consumer device fingerprint (e.g., some encryption algorithms are more secure than others), etc. Using the confidence module **26(a)-2**, the server computer **26(a)** may subsequently determine if additional authentication processes need to take place.

Such additional authentication processes may comprise challenge questions and/or consumer notification that a transaction is occurring.

[0048] The confidence assessment module **26(a)-2** can "score" a transaction based on a number of transaction variables. If this score exceeds a predetermined threshold, then the transaction can be considered valid and additional authentication processing need not take place. Conversely, if the score does not exceed a predetermined threshold, then the transaction may be characterized as suspicious and additional authentication processes may be initiated.

[0049] The data formatter module **26(a)-4** may be used to format data so that it can be used by the confidence assessment module **26(a)-2**. In some cases, data that is from different POS terminals from different companies may be decrypted by the decryption module **26(a)-3** and may be in different formats. The data formatter can format any data so that it can be used by the confidence assessment module **26(a)-2**.

[0050] FIG. 5 shows typical components or subsystems of a computer apparatus. Such components (or subsystems) or any subset of such components may be present in various components shown in FIG. 1, including the access devices, server computer, etc. The subsystems shown in FIG. 5 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.

[0051] 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 system, and acquirer, some entities perform all of these functions and may be included in embodiments of invention.

[0052] IV. Exemplary methods

[0053] Various methods according to embodiments of the invention may be described with reference to FIGS. 1, 6 and 7. FIGS. 6-7 include flowcharts.

[0054] Some or all of the steps shown in FIG. 6 may be included in embodiments of the invention. For example, some embodiments of the invention may use algorithm identifiers to determine if a portable consumer device fingerprint in an authorization request message matches a portable consumer device fingerprint stored in a back end database, and may not perform transaction confidence processing before determining if the transaction is authorized. In other embodiments, a transaction confidence process may be performed without using portable consumer device fingerprints to authenticate portable consumer devices. In preferred embodiments, however, algorithm identifiers, portable consumer device fingerprints, and transaction confidence processing are used to authenticate the portable consumer devices and transactions as a whole.

[0055] Also, while the flowcharts shown in FIGS. 6 and 7 shows specific steps being performed in a specific order, embodiments of the invention can include methods which include such steps in a different order.

[0056] Referring to FIGS. 1 and 6, a consumer A **30(a)** may use a portable consumer device A **32(a)** to interact with an access device A **34(a)** at a merchant A **22(a)** (step **202**). For example, the portable consumer device **32(a)** may be a credit card, the access device A **34(a)** may be a point of sale terminal, and the merchant A **22(a)** may be a gas station. Consumer A **30(a)** may want to purchase gas from merchant A **22(a)** using the portable consumer device A **32(a)**.

[0057] After the portable consumer device A **32(a)** interfaces with the access device A **34(a)** at merchant A **22(a)**, the access device A **34(a)** reads consumer data and portable consumer device fingerprint data such as magnetic stripe fingerprint data from the portable consumer device A **32(a)** (step **204**). The consumer data may include information of which the consumer is typically aware. Examples of consumer

data include a consumer's account number, expiration date, and service code. As noted above, portable consumer device fingerprint data are data that are not typically known to the consumer, but are used to authenticate the portable consumer device. In this example, the portable consumer device fingerprint data may be magnetic stripe fingerprint data. The magnetic stripe fingerprint data may also comprise data that are embedded into the magnetic structure of the magnetic stripe and are only readable using an access device that is manufactured by a particular company.

[0058] Once the access device A **34(a)** obtains the consumer data from the portable consumer device A **34(a)**, an authorization request message including an algorithm identifier is created (step **206**). The authorization request message may also include consumer data (e.g., an account number), data relating to the amount of the purchase, and portable consumer device fingerprint data. The access device A **34(a)** may alter (e.g., encrypt) the received fingerprint data using an algorithm A that is stored in a memory in access device A **34(a)**, before it is incorporated into the authorization request message. In some embodiments, the portable consumer device fingerprint and the algorithm identifier may be stored in a supplementary data field called Field 55.

[0059] Different types and sizes of fingerprints may originate from different portable consumer devices offered by different manufacturers. These different fingerprints may be inserted into a data field of standard size so that transmission through the payment processing system is uniform regardless of the particular fingerprint being transmitted. For example, in some cases, it is desirable to pad the data field with characters such as zeros to fill up the data field. For example, a data field may have a size of 64 bytes. The fingerprint from one type of portable consumer device may be 54 bytes while the fingerprint from another type of portable consumer device may be 56 bytes. Additional padding characters may be present in the 64 byte field along with a two character algorithm identifier. The padding characters may be placed in the field in a predetermined manner. Equally a TLV (Tag Length Value) format can be used to deliver the payment and authentication data. This approach provides additional flexibility and usage of standard or new payment and authorization message fields.

[0060] In embodiments of the invention, the previously described algorithm identifier may not only identify the algorithm used to encrypt a portable consumer device fingerprint; the identified algorithm can also be used to restore the fingerprint to its original form so that it can be evaluated. For example, the algorithm identifier may be used to identify the algorithm that may be used to remove any padding characters to restore the received, but altered fingerprint to its original form so that it can be evaluated.

[0061] The authorization request message is then sent from access device **34(a)** to the payment processing network **26** directly or via the acquirer A **24(a)** associated with the merchant A **22(a)** (step **208**). In other embodiments, the access device **34(a)** could send the authorization request message to the payment processing network directly, instead of through the acquirer A **24(a)**.

[0062] After the authorization request message is received by the payment processing network **26**, the server computer **26(a)** in the payment processing network **26** analyzes the authorization request message and then selects an algorithm using an algorithm ID that is in the authorization request message (step **210**). The selected algorithm ID and the selected algorithm may be selected from the algorithm database **26(c)**. The algorithm database **26(c)** may contain a plurality of algorithm IDs and a plurality of algorithms which may be associated with various access devices (e.g., access device A **32(a)** and access device B **34(b)**).

[0063] After the algorithm is identified, the portable consumer device fingerprint is determined by the server computer **26(a)** in the payment processing network **26** (step **212**). The selected algorithm is then used to restore (e.g., decrypt) the altered portable consumer device fingerprint present in the authorization request message.

[0064] Then, the server computer **26(a)** determines if the determined portable consumer device fingerprint corresponds to a previously stored fingerprint in a database (step **214**). The server computer **26(a)** can first obtain consumer data such as the consumer's account number from the authorization request message and/or may obtain additional consumer data from the consumer database **26(b)** after analyzing the authorization request message. Once the consumer data are determined, the server computer **26(a)** can obtain the portable consumer device

fingerprint from the consumer database **26(b)**. The server computer **26(a)** then determines if the portable consumer device fingerprint in the authorization request message and the portable consumer device fingerprint in the consumer database **26(b)** match.

[0065] If the portable consumer device fingerprint obtained from the consumer database **26(b)** does not correspond to the previously restored portable consumer device fingerprint obtained from the authorization request message, then additional authentication processes may be performed and/or an authorization response message may be sent back to the consumer A **22(a)** indicating that the transaction is denied (step **222**). Additional authentication processing may include sending a transaction notification message to the consumer A **22(a)** (e.g., to the consumer's cell phone or the consumer's computer) notifying the consumer that a transaction is taking place. The notification message may request that the consumer A **22(a)** confirm that the transaction is authentic. Alternatively or additionally, other types of challenges, such as challenge questions, may be sent to consumer A **22(a)**. Challenges such as challenge questions are described in further detail in U.S. Patent Application No. 11/763,240, filed on June 14, 2007 (Attorney Docket No. 16222U-031600US), which is herein incorporated by reference in its entirety for all purposes.

[0066] In some embodiments, if a fingerprint obtained from the authorization request message and the fingerprint in the consumer database **26(b)** match, the server computer **26(a)** may also optionally determine if a transaction confidence threshold is satisfied (step **215**). If the confidence threshold is not satisfied, then additional authorization processing may be performed (step **223**). If, however, the confidence threshold is satisfied, the authorization may be processed on behalf of the issuer or an authorization request message may then be forwarded onto issuer A **28(a)** (step **216**) for final decisioning.

[0067] The transaction confidence threshold may take any number of transaction characteristics to score the transaction as being authentic or potentially suspicious. Such transaction characteristics may relate to the access device (e.g., whether the access device uses new or old technology, whether the access device uses a secure encryption algorithm to encrypt data, etc.), portable consumer device

(e.g., whether the portable consumer device is a phone, a magnetic stripe card with old technology, a magnetic stripe card with new technology, etc.), etc.

[0068] As noted above, in a payment processing system, there can be many different combinations of access devices and portable consumer devices interacting together at any given time. These different combinations of access devices and potable consumer devices may initiate transactions that may have different levels of potential authenticity. For example, referring to FIG. 1, access device A **34(a)** may use an encryption algorithm from company A to encrypt data in an authorization request message, access device B **34(b)** may use an encryption algorithm from company B, and access device C **34(c)** may not use any encryption technology. Encryption algorithm A may be considered a more reliable encryption algorithm than encryption algorithm B. Consequently, authorization request messages from access device A **34(a)** may have a higher level of potential authenticity than authorization request messages from access device B **34(b)** or access device C **34(c)**. Additional authentication processing may be performed when transactions are performed access devices B and C **34(b)**, **34(c)** rather than the access device A **34(a)**. In another example, if portable consumer devices A, B, and C **32(a)**, **32(b)**, **32(c)** are all highly secure portable consumer devices, then only authorization request messages coming from access device C **34(c)** may be require additional authentication processing, since only the access device C **34(c)** does not contain an encryption algorithm. As illustrated by this example, the threshold for determining whether or not additional authorization processing needs to be performed can be varied and can be set according to predetermined rules.

[0069] After the authorization request message is received by issuer A **28(a)**, issuer A may then determine if the transaction is authorized. If the transaction is not authorized (e.g., due to insufficient funds or credit in consumer A's account), then additional authorization processing may be performed and/or an authorization response message indicating that the transaction is declined may be sent to consumer A **30(a)** (step **224**).

[0070] If the transaction is approved by issuer A **28(a)**, then an authorization response message may be sent back to consumer A **30(a)** via the payment

processing network **26**, acquirer A **24(a)**, merchant A **22(a)**, and access device A **34(a)** (step **220**).

[0071] 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 an 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.

[0072] **IV. Authentication Systems**

[0073] The above-described portable authentication processes can be part of a larger overall transaction authentication process.

[0074] FIG. 8 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)**.

[0075] 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

[0076] 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

[0077] Back end processing relates to processing that may occur at the issuer or payment processing system, 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.

[0078] 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

[0079] 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.

[0080] 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

[0081] 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.

[0082] 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. For example, although algorithms for use in encrypting portable consumer device fingerprints are described in detail, the algorithms may be used for any other suitable end use in embodiments of the invention.

[0083] 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.

[0084] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving an authorization request message associated with a transaction conducted using a portable consumer device, wherein the portable consumer device comprises a portable consumer device fingerprint, and wherein the authorization request message comprises an altered portable consumer device fingerprint and an algorithm identifier;

selecting an algorithm from among a plurality of algorithms using the algorithm identifier;

determining the portable consumer device fingerprint using selected algorithm and the altered portable consumer device fingerprint;

determining if the portable consumer device fingerprint matches a stored portable consumer device fingerprint; and

sending an authorization response message after determining if the portable consumer device fingerprint matches the stored portable consumer device fingerprint.

2. The method of claim 1 wherein the altered portable consumer device fingerprint was formed an at access device at a merchant.

3. The method of claim 2 wherein the stored portable consumer device fingerprint is stored in a database, which also stores an account number associated with the portable consumer device.

4. The method of claim 1 wherein the portable consumer device is a payment card comprising a magnetic stripe, wherein the portable consumer device fingerprint is a magnetic stripe fingerprint.

5. The method of claim 1 wherein the algorithm is a key used in an encryption process.

6. The method of claim 1 wherein the authorization request message further comprises an account number associated with the portable consumer device and a transaction amount associated with the transaction.

7. The method of claim 1 further comprising receiving the authorization response message from an issuer of the portable consumer device before sending the authorization response message.

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

9. The computer readable medium of claim 8 wherein the portable consumer device is a payment card comprising a magnetic stripe, wherein the portable consumer device fingerprint is a magnetic stripe fingerprint

10. A server computer comprising the computer readable medium of claim 8.

11. A system comprising:

means for receiving an authorization request message associated with a transaction conducted using a portable consumer device, wherein the portable consumer device comprises a portable consumer device fingerprint, and wherein the authorization request message comprises an altered portable consumer device fingerprint and an algorithm identifier;

means for selecting an algorithm from among a plurality of algorithms using the algorithm identifier;

means for determining the portable consumer device fingerprint using selected algorithm and the altered portable consumer device fingerprint;

means for determining if the portable consumer device fingerprint matches a stored portable consumer device fingerprint; and

means for sending an authorization response message after determining if the portable consumer device fingerprint matches the stored portable consumer device fingerprint.

12. A method comprising:

sending an authorization request message associated with a transaction conducted using a portable consumer device, wherein the portable consumer device comprises a portable consumer device fingerprint, and wherein the authorization request message comprises an altered portable consumer device fingerprint and an algorithm identifier, wherein an algorithm is selected from among a plurality of algorithms using the algorithm identifier, the portable consumer device fingerprint is determined using selected algorithm and the altered portable consumer device fingerprint, and a server computer determines if the portable consumer device fingerprint matches a stored portable consumer device fingerprint; and

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

13. The method of claim 12 wherein the authorization request message comprises an account number.

14. The method of claim 12 wherein the portable consumer device is a phone.

15. The method of claim 12 wherein the portable consumer device is a payment card comprising a magnetic stripe, wherein the portable consumer device fingerprint is a magnetic stripe fingerprint.

16. The method of claim 12 wherein the algorithm is a key associated with an encryption process.

17. The method of claim 12 wherein the transaction is a payment transaction.

18. A computer readable medium comprising code for performing the method of claim 12.

19. An access device comprising the computer readable medium of claim 18.

20. The access device of claim 19 wherein the access device is a point of sale terminal.

21. A method comprising:

receiving an authorization request message, wherein the authorization request message is generated after an interaction between a portable consumer device and an access device;

analyzing the authorization request message for one or more characteristics or the portable consumer device or the access device to determine if a confidence threshold is met or exceeded; and

if the confidence threshold is not exceeded, performing additional authentication processing.

22. The method of claim 21 wherein the one or more characteristics of the portable consumer device include a particular portable consumer device used.

23. The method of claim 21 wherein the one or more characteristics of the access device include a particular algorithm used to alter a portable consumer device fingerprint associated with the portable consumer device.

24. The method of claim 23 wherein analyzing the authorization request message comprises analyzing at least one characteristic of the access device and at least one characteristic of the portable consumer device to determine if the confidence threshold is met or exceeded.

25. The method of claim 24 wherein the one or more characteristics of the access device include a particular algorithm present in the access device

26. The method of claim 24 wherein the portable consumer device is a payment card.

27. The method of claim 24 wherein the portable consumer device is a phone.

28. The method of claim 24, wherein the method further comprises:

sending an authorization response message to the consumer without performing additional authentication processing if the confidence threshold is met.

29. The method of claim 21 wherein the additional authentication processing comprises sending the consumer a message to a phone operated by a consumer or to an access device used to conduct the transaction, wherein the message indicates that the transaction is occurring.

30. The method of claim 29 wherein the transaction is a payment transaction.

31. A system comprising:

means for receiving an authorization request message, wherein the authorization request message is generated after an interaction between a portable consumer device and an access device;

means for analyzing the authorization request message for one or more characteristics or the portable consumer device or the access device to determine if a confidence threshold is met or exceeded; and

means for performing additional authentication processing if the confidence threshold is not exceeded.

32. The system of claim 31 wherein the one or more characteristics of the portable consumer device include a particular portable consumer device.

33. The system of claim 31 wherein the one or more characteristics of the access device include a particular algorithm in the access device.

34. The system of claim 31 wherein the means for analyzing the authorization request message comprises means for analyzing at least one characteristic of the access device and at least one characteristic of the portable consumer device.

35. The system of claim 31 wherein the portable consumer device is a payment card.

36. A system comprising:

a server computer comprising a processor; and computer readable medium comprising code for receiving an authorization request message, wherein the authorization request message is generated after an interaction between a portable consumer device and an access device, code for analyzing the authentication request message for one or more characteristics of the portable consumer device or the access device to determine if a confidence threshold is met or exceeded, and code for performing additional authentication processing if the confidence threshold is not exceeded.

37. The system of claim 36 further comprising an access device in operative communication with the server computer.

38. The system of claim 37 wherein the access device is a POS terminal.

39. The system of claim 36 wherein the one or more characteristics of the access device includes a particular algorithm that is used by the access device to encrypt data from the portable consumer device.

40. The system of claim 36 wherein the one or more characteristics comprises of the portable consumer device includes a particular portable consumer device.

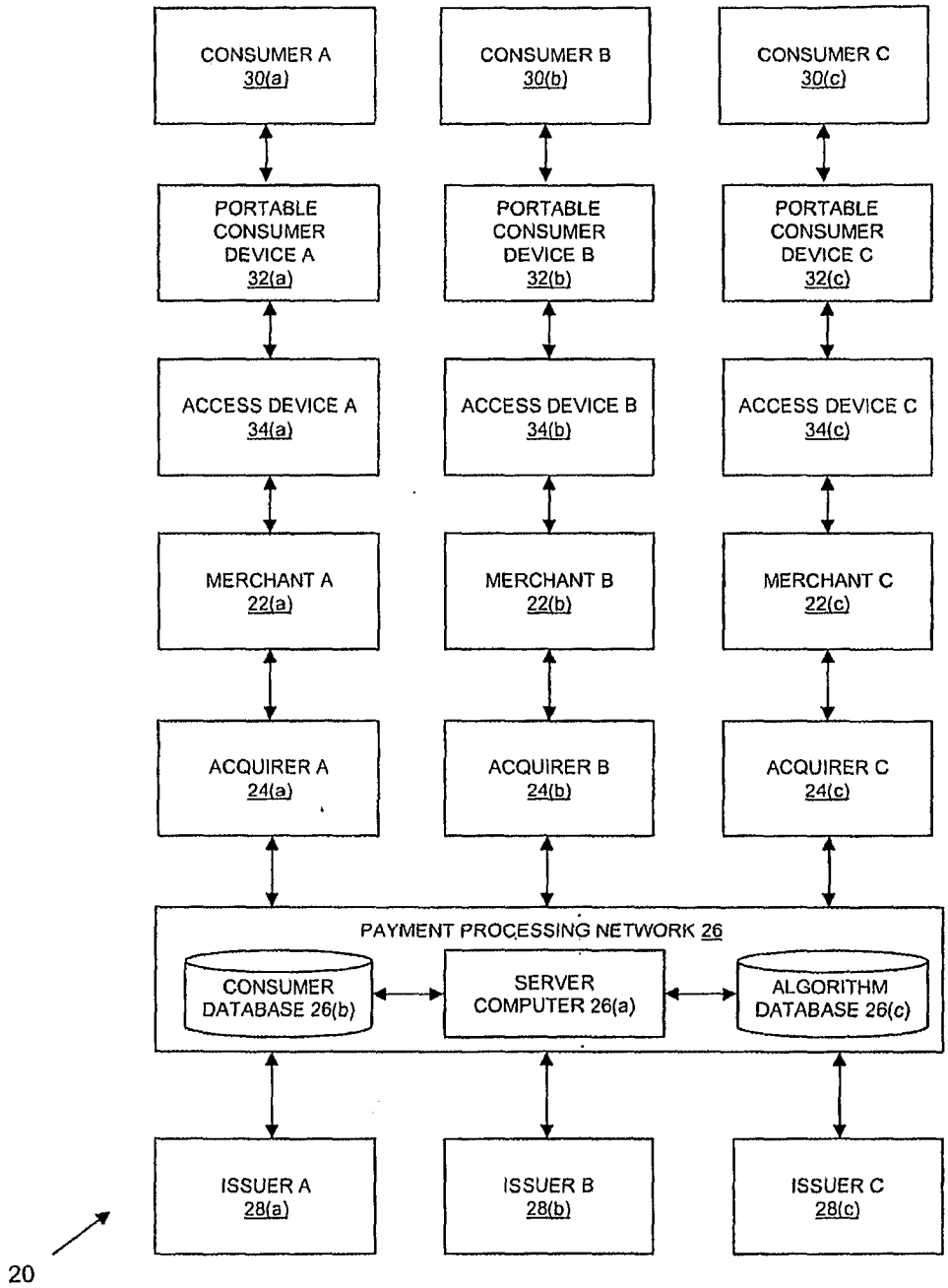

CONSUMER A
30(a)
CONSUMER B
30(b)
CONSUMER C
30(c)
PORTABLE CONSUMER DEVICE A
32(a)
PORTABLE CONSUMER DEVICE B
32(b)
PORTABLE CONSUMER DEVICE C
32(c)
ACCESS DEVICE A
34(a)
ACCESS DEVICE B
34(b)
ACCESS DEVICE C
34(c)
MERCHANT A
22(a)
MERCHANT B
22(b)
MERCHANT C
22(c)
ACQUIRER A
24(a)
ACQUIRER B
24(b)
ACQUIRER C
24(c)
PAYMENT PROCESSING NETWORK 26
CONSUMER DATABASE 26(b)
SERVER COMPUTER 26(a)
ALGORITHM DATABASE 26(c)
ISSUER A
28(a)
ISSUER B
28(b)
ISSUER C
28(c)
20

FIG. 1

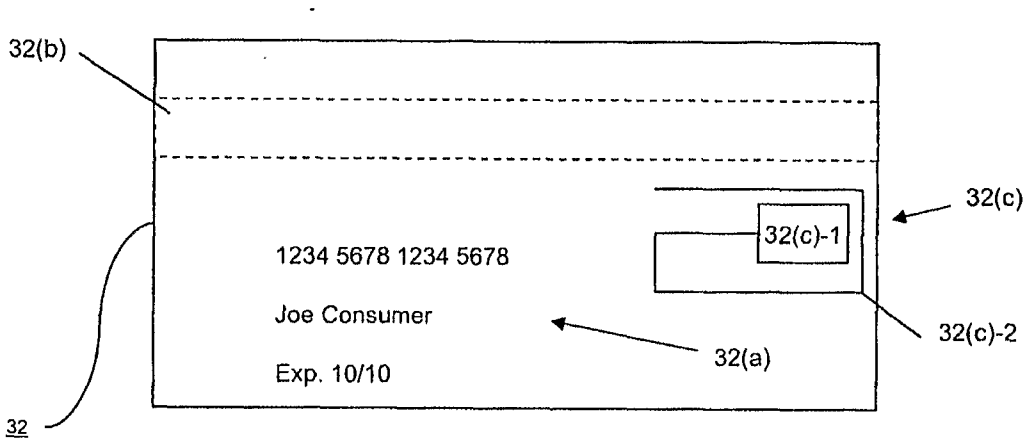

32(b)
32(c)
32(c)-1
1234 5678 1234 5678
Joe Consumer
Exp. 10/10
32(a)
32(c)-2
32

FIG. 2

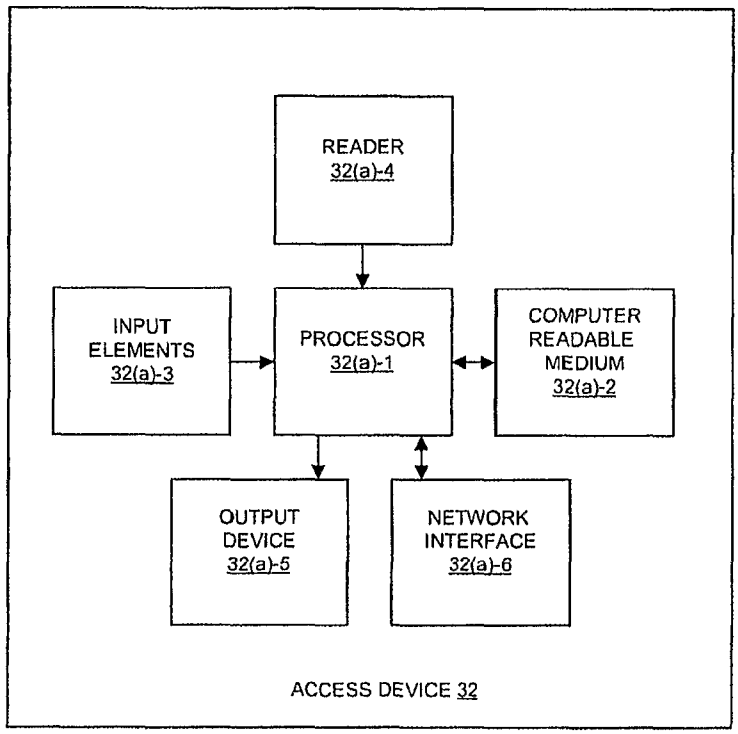

READER
32(a)-4
INPUT
ELEMENTS
32(a)-3
PROCESSOR
32(a)-1
COMPUTER
READABLE
MEDIUM
32(a)-2
OUTPUT
DEVICE
32(a)-5
NETWORK
INTERFACE
32(a)-6
ACCESS DEVICE 32

FIG. 3

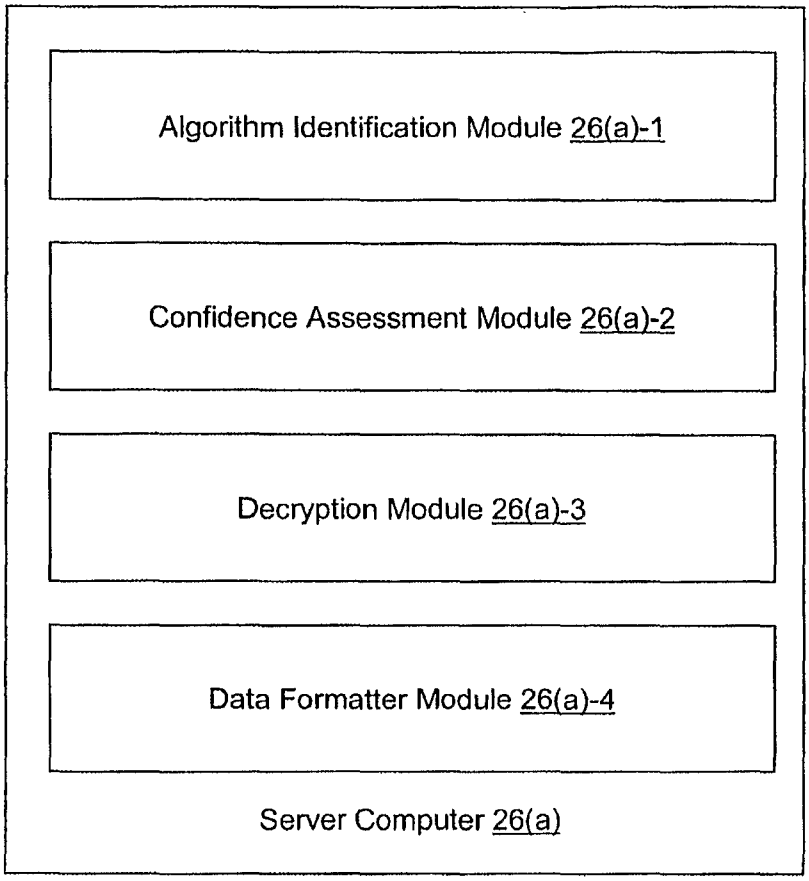

Algorithm Identification Module 26(a)-1
Confidence Assessment Module 26(a)-2
Decryption Module 26(a)-3
Data Formatter Module 26(a)-4
Server Computer 26(a)

FIG. 4

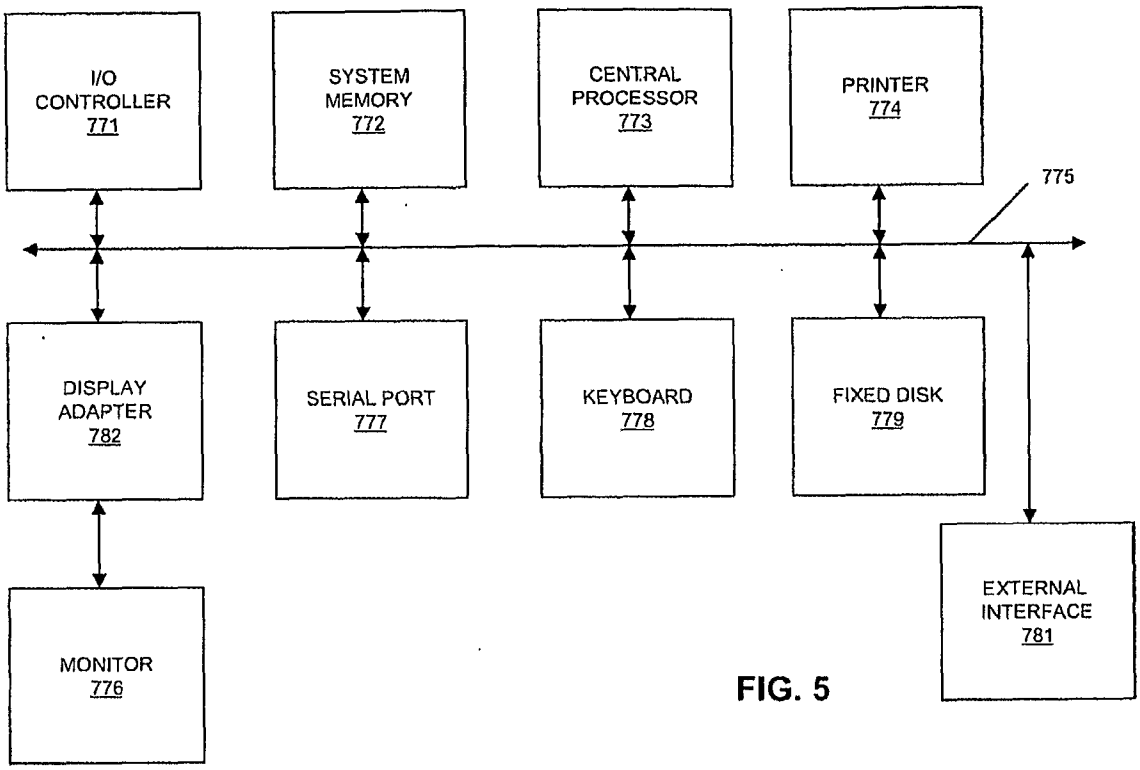

I/O CONTROLLER 771
SYSTEM MEMORY 772
CENTRAL PROCESSOR 773
PRINTER 774
775
DISPLAY ADAPTER 782
SERIAL PORT 777
KEYBOARD 778
FIXED DISK 779
EXTERNAL INTERFACE 781
MONITOR 776

FIG. 5

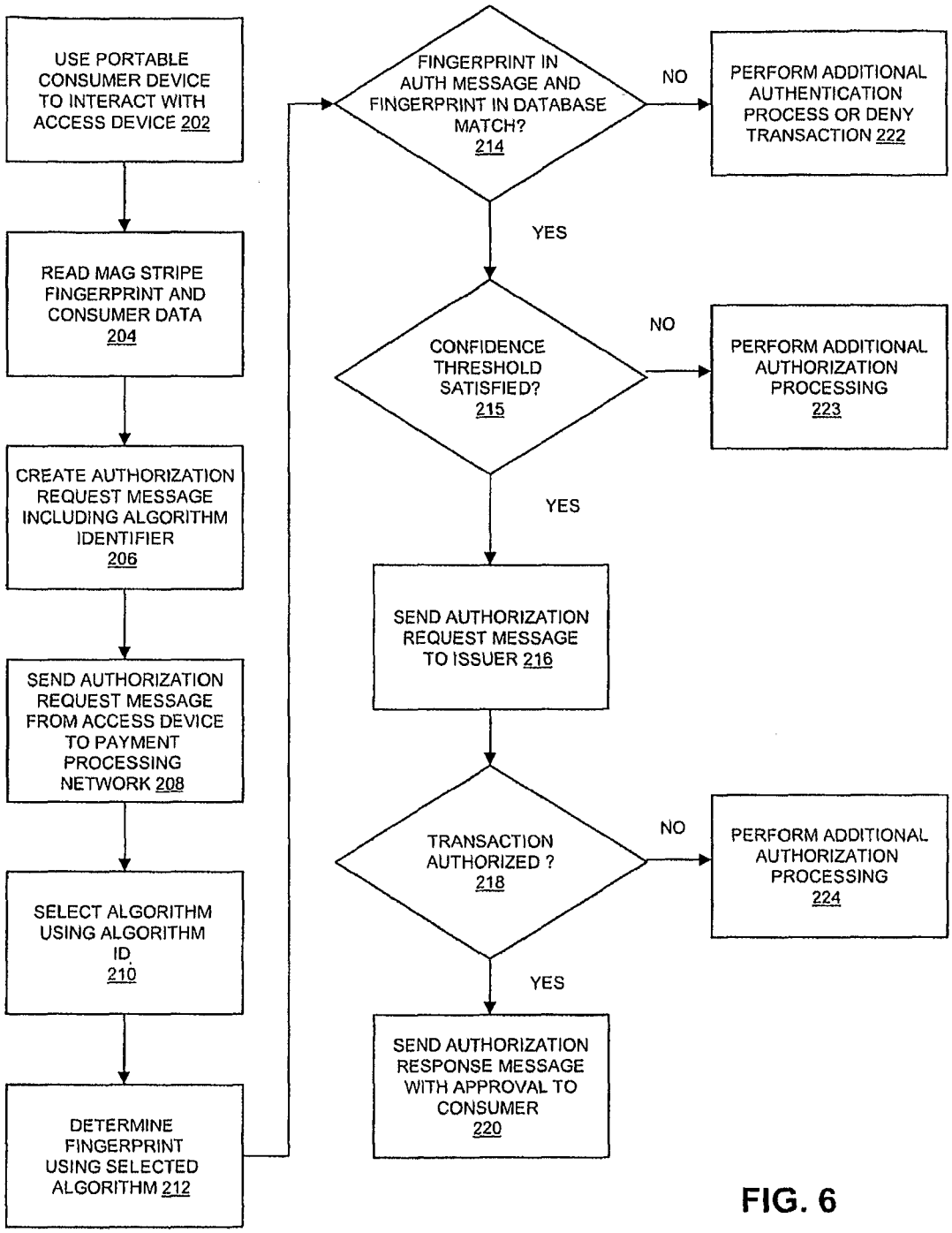

USE PORTABLE CONSUMER DEVICE TO INTERACT WITH ACCESS DEVICE 202
READ MAG STRIPE FINGERPRINT AND CONSUMER DATA 204
CREATE AUTHORIZATION REQUEST MESSAGE INCLUDING ALGORITHM IDENTIFIER 206
SEND AUTHORIZATION REQUEST MESSAGE FROM ACCESS DEVICE TO PAYMENT PROCESSING NETWORK 208
SELECT ALGORITHM USING ALGORITHM ID 210
DETERMINE FINGERPRINT USING SELECTED ALGORITHM 212
FINGERPRINT IN AUTH MESSAGE AND FINGERPRINT IN DATABASE MATCH? 214
NO
PERFORM ADDITIONAL AUTHENTICATION PROCESS OR DENY TRANSACTION 222
YES
CONFIDENCE THRESHOLD SATISFIED? 215
NO
PERFORM ADDITIONAL AUTHORIZATION PROCESSING 223
YES
SEND AUTHORIZATION REQUEST MESSAGE TO ISSUER 216
TRANSACTION AUTHORIZED ? 218
NO
PERFORM ADDITIONAL AUTHORIZATION PROCESSING 224
YES
SEND AUTHORIZATION RESPONSE MESSAGE WITH APPROVAL TO CONSUMER 220

FIG. 6

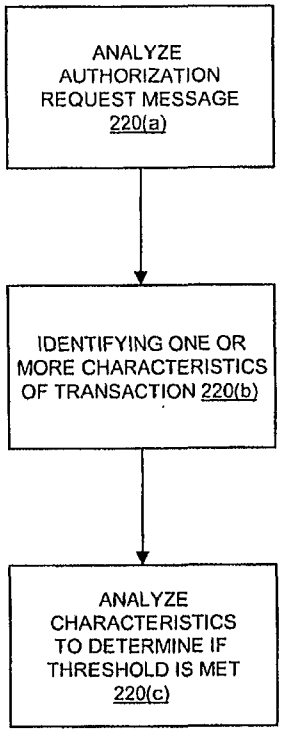

ANALYZE AUTHORIZATION REQUEST MESSAGE 220(a)
IDENTIFYING ONE OR MORE CHARACTERISTICS OF TRANSACTION 220(b)
ANALYZE CHARACTERISTICS TO DETERMINE IF THRESHOLD IS MET 220(c)

FIG. 7

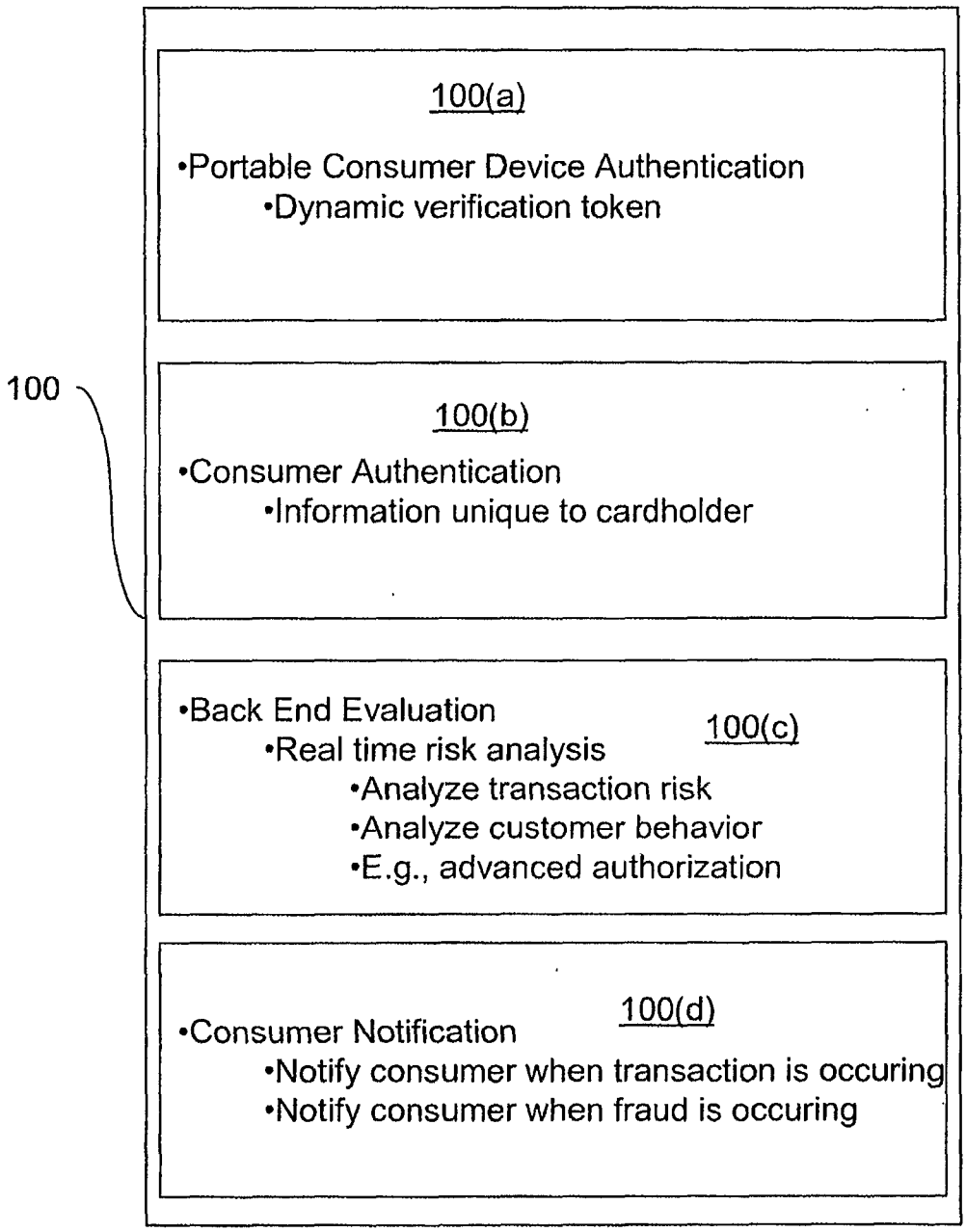

100
100(a)
•Portable Consumer Device Authentication
•Dynamic verification token
100(b)
•Consumer Authentication
•Information unique to cardholder
•Back End Evaluation
100(c)
•Real time risk analysis
•Analyze transaction risk
•Analyze customer behavior
•E.g., advanced authorization
100(d)
•Consumer Notification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

FIG. 8