Abstract: In order to make it more difficult to obtain numbers that can be used to conduct fraudulent transactions, a portion of a real account number is encrypted. The encrypted portion of the account number is used to generate a new account number, a new expiration date, and a new verification value. This information can be determined using processor that may reside in a point of sale terminal, a smart card, or a computer operated by a user. The new account number, the new expiration date, and the new verification value can be used in a payment transaction. A server computer in a central payment processing network may determine that the new account information is not the real account information, and may subsequently generate a modified authorization request message using the real account information and may send it to an issuer for approval. The transmission of data is more secure, since real account information is not sent from the merchant to the payment processing network.
DEVICE INCLUDING ENCRYPTED DATA FOR EXPIRATION DATE
AND VERIFICATION VALUE CREATION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a non-provisional of and claims the benefit of the filing date of U.S. Patent Application No. 61/179,970, filed on May 20, 2009, which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] There is a need for more secure data transfer when paying for goods and services using payment cards such as debit, credit, and stored value cards.

[0003] In a typical payment transaction, a user may use a credit card to purchase an item at a merchant. The user may swipe his credit card through a POS (point of sale) terminal, and the POS terminal may generate an authorization request message including the account number, expiration date, and card verification value (CW) associated with the credit card. The authorization request message may pass to the issuer of the credit card, and the issuer may approve or deny the request to authorize the transaction.

[0004] If information such as the account number, expiration date, and card verification value is obtained by an unauthorized person, the unauthorized person could potentially purchase goods and services using the obtained information. Such information could theoretically be intercepted by the unauthorized person during a transaction (e.g., as the account information passes from the merchant to the payment processing network) or it could be surreptitiously obtained from the card while it is with the authorized user.

[0005] There is a need for improved data security systems. Embodiments of the invention address these and other problems, individually and collectively.
[0006] Embodiments of the invention can alter account information such as an expiration date and/or verification value (e.g., CW or CW2) to protect account information.

[0007] In some embodiments, in order to make it more difficult to obtain numbers that can be used to conduct fraudulent transactions, a portion of a real account number associated with a payment card can be encrypted. Different segments of the encrypted portion of the real account number can be used to create a new expiration date, a new verification value (e.g., a CW2 value), and a new account number. The new expiration date, the new verification value, and the new account number can comprise new account information, which can be used instead of real account information to conduct payment transactions.

[0008] In some embodiments, when a payment transaction is conducted using the new account information and the payment card, an authorization request message may be generated and the new account information may be sent to a server computer in a payment processing network. The server computer can determine that the received new account information is not the real account information. It can subsequently determine the real account information (including the real account number, the real expiration date, and the real verification value) from the new account information. If the server computer does not make the authorization decision, a modified authorization request message may be generated and then sent to an issuer that issued the real account information. The issuer can then approve or deny the transaction authorization request.

[0009] One embodiment of the invention is directed to a method comprising encrypting, using a processor, a portion of a first account number to form an encrypted portion, the first account number being associated with a first expiration date and a first verification value. The method also includes determining a second expiration date or a second verification value using a segment of the encrypted portion.

[0010] Another embodiment of the invention is directed to a computer readable medium comprising code, executable by a processor, for implementing a
method comprising: encrypting, using a processor, a portion of a first account number to form an encrypted portion, the first account number being associated with a first expiration date and a first verification value; and determining a second expiration date or a second verification value using a segment of the encrypted portion.

[0011] Another embodiment of the invention is directed to a method comprising: receiving an initial authorization request message comprising a second account number, and at least one of a second expiration date and a second verification value. After the second account number and at least one of the second expiration date and the second verification value are received, a server computer can determine a first account number, a first expiration date, and a first verification value from the second account number. A modified authorization request message including the first account number, the first expiration date, and the first verification value can be sent to an issuer. The first verification value is different than the second verification value and the first expiration date is different than the second expiration date.

[0012] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] Fig. 1 shows a flowchart illustrating a method according to an embodiment of the invention.

[0014] Fig. 2 shows schematic diagram illustrating how a second account number, a second date, and a second verification value can be formed in an embodiment of the invention.

[0015] Fig. 3 shows a block diagram of a system.

[0016] Fig. 4 shows a block diagram of parts of a payment processing system.

[0017] Fig. 5 shows a flowchart illustrating a process for using a second account number, a second expiration date, and a second verification value.

[0018] Fig. 6 shows a block diagram of components in a computer apparatus according to various embodiments.
Figs. 7 and 8 show block diagrams illustrating components in consumer devices according to various embodiments.

DETAILED DESCRIPTION

Embodiments of the invention provide for methods and systems for generating a verification value such as a CW or CW2 value, a new second account number, and a new second expiration date from first real account information including a real first account number. Embodiments of the invention can be used for both card present and card-not-present (CNP) transactions.

Embodiments of the invention have a number of advantages. Embodiments of the invention are able to maintain or improve existing user experiences, minimize the impact on merchant processes/systems, leverage existing network data transport mechanisms, utilize an existing issuer validation infrastructure, support multiple forms of implementation, and maintain consistency with a broader authentication strategy. Further, because authentication elements such as expiration dates and the verification values associated with a payment card can change in embodiments of the invention and otherwise appear to be normal to unauthorized persons and can use an encryption process that is not known to the general public, it is difficult, if not impossible, for an unauthorized person to obtain the real account information associated with the user's payment card.

Fig. 1 shows a flowchart illustrating a method according to an embodiment of the invention. The method may be performed by any suitable device (or processor therein), including a device that is located at the transaction site. The device may be operated by a merchant or a user (or consumer).

Referring to Fig. 1, a real first account number can be determined by a processor (step 102). The first account number could be a real first account number associated with a payment card such as a debit or credit card. It may include any suitable number of digits or characters (e.g., 12, 16, 18, etc.). The first account number may be associated with other first account information including an expiration date and a verification value.
The verification value may be a CW (card verification value) value. There can be two types of CW values. The first, called CVC1 or CW1, is encoded on the magnetic stripe of a payment card. The second, called CVC2 or CW2, is printed on the payment card.

The CW1 code is used for "in person" transactions, where the consumer using the payment device is physically present at the time of purchase. The consumer hands the merchant his payment card, and the merchant swipes it through a point of sale terminal. Information stored on the magnetic stripe, including the CW1 code, is read from the magnetic stripe and transmitted to an authenticating entity (e.g., an issuer or a payment processing organization such as Visa) in a purchase transaction for verification (authentication).

However, transactions over the Internet, by mail, fax or over the phone cannot be verified using the CW1 code. For these so-called "card not present" (CNP) transactions, the merchant will use the CW2 code to confirm that the consumer is in possession of the authentic card by asking the consumer to state the code over the phone (in a phone transaction) or enter it into a Web page (in an Internet transaction). The CW2 code is used to authenticate the purchase transaction by comparing the code supplied by the consumer against the code that is stored in a cardholder database at a payment processor facility. If the purchase transaction is authenticated, then an authorization request is sent to the issuer of the card to approve or deny the purchase.

A portion of the first account number can then be encrypted by the processor to form an encrypted portion (step 104). Any suitable number of digits in the first account number may be encrypted using any suitable encryption algorithm. For example, a middle portion of the first account number (e.g., digits 2-11 in a 16-digit account number) may be encrypted using an encryption algorithm such as DES or triple DES. Other types of encryption algorithms may be used in other embodiments of the invention.

A first segment of the encrypted portion of the first account number may then be selected by the processor (step 106). Any suitable number of digits may be present in the first segment, and any suitable portion of the encrypted portion may form the first segment.
Then, the first encrypted portion segment is then mapped to a second expiration date using the processor (step 108). The mapping of the second expiration date to the first encrypted portion segment may occur in any suitable manner. For example, if the first encrypted portion includes two digits, then the numbers from 0-99 in those two digits can be mapped to various expiration dates corresponding to a month (e.g., a number from zero to twelve) and a year (e.g., a two digit number representing a year).

Before or after the first encrypted portion segment is determined by the processor, a second encrypted portion segment of the encrypted portion is used by the processor to determine a second verification value (step 110). The second encrypted portion could be mapped to different verification values stored in a local or remote database, or it could simply be a representation of a new verification value. In the latter case, for example, if the second encrypted portion is "191," then the new second verification value is also "191."

Before or after the first and second encrypted portion segments are determined and/or processed by the processor, a third encrypted portion segment can be determined by the processor. A second account number can then be formed from the third encrypted portion segment (step 112). In the formation of the new second account number, the third encrypted portion segment can be inserted into the middle of a new second account number. In addition to the middle portion comprising the third encrypted portion segment, the new second account number may comprise a signal segment and a segment that is from the real first account number. For example, the second account number may be "400001234569876." "40000" may be a signal segment, "123456" may be the third encrypted portion segment, and "9876" may be a segment that is unchanged from the real first account number.

The segment that is from the real first account number may be the last four digits of the real account number. It is desirable to keep the last four digits of the real first account number and the new second account number the same, so that the user does not sense that anything is different. For example, when the user receives a receipt for a purchase transaction, the receipt will include the last four digits of the real account number and also the new account number. Typically, only
the last four digits of an account number are shown on a purchase receipt, so the user does not see the change in account number and may not notice a difference.

[0033] As a result of steps 102, 104, 106, 108, 110, and 112, new second account information can be used by a consumer in a payment transaction. The use of the new second account information is described in further detail below.

[0034] In a detailed example illustrating steps 102, 104, 106, 108, 110, and 112, a processor in a smartcard or a POS terminal can determine an existing first account number associated with a payment card and can encrypt a portion of it. In some embodiments, the encryption process may not use dynamic data so the encrypted portion and the second account information derived from it may be used in all transactions conducted with the payment card. However, in other embodiments which are described below, the encrypted portion may be formed using dynamic data such as a date or counter, so that the encrypted portion and consequently the second account information changes periodically (e.g., with every transaction).

[0035] The processor can use the encrypted portion to create a new second account number, second expiration date, and second verification value such as a second CW2 value. For example, an exemplary real first account number could be "4234561234567890," and a new second account number can be generated. The second account number could take the form "40000xxxxxx7890," where the last 4 digits of the second account number are the same as the last four digits of the real first account number. The number "40000" can be a signal segment that can alert a server computer in a payment processing network that the account number is not the real account number and that a decryption process needs to be performed. To fill in the digits "xxxxxx," the processor can take the eleven digits "23456123456" from the real first account number and can apply a DES encryption algorithm (or any other suitable encryption algorithm) and decimalize it to obtain a new eleven digit number. The processor could then take six of these numbers and plug them into the digits "xxxxxx" in the new second account number above. Two of the numbers may be mapped to a four digit expiration date, and the remaining three numbers can be used as a new CW or CW2 value. If it is a CW2 value, then the new CW2 value would be displayed or otherwise provided to the user so that the user could provide this
information to the merchant in a transaction. The new CW2 value could be displayed on the user's phone, computer, or other device.

[0036] Fig. 2 shows a block diagram illustrating how data is transformed according to embodiments of the invention using other information. Some of the illustrated blocks in Fig. 2 represent blocks of data that may be stored and manipulated in a computer-readable medium, which may be embodied by one or more memory devices. Some of the blocks in Fig. 2 represent various transformations that may take place on the data. The embodiments described with respect to Fig. 2 also include the use of "other information" in the encryption process. The "other information" may include other information that is personal to the user, keys, or dynamic data such as dates, counters, and the like.

[0037] Referring to Fig. 2, first account information may include a first account number 210, and may be a primary account number (PAN) that is 16 digits in length. Account numbers of other sizes could be used in embodiments of the invention. The first account number may correspond to a real account number associated with a consumer's payment card. Other first account information may include a first verification value and a first expiration date associated with the payment card.

[0038] Other information 220 can represent other data that may be used in combination with first account information 210 according to various embodiments. According to some embodiments, other information 220 can include data that changes on a regular basis. For example, other information 220 might include the current date, counter, the price of a transaction, information that is specific to a merchant, etc. The "other information" may be time dependent in nature, or location or merchant specific.

[0039] The other information may also include suitable encryption keys, including symmetric and asymmetric keys, that may be used with the encryption function 230. Suitable symmetric keys may include UDKs ("unique derived keys"). Such keys may be derived from user information such as the user's account number, birthday, social security number, etc., so that each key is unique to a particular user or payment card. The key and encryption algorithm may be previously loaded into the user's portable consumer device (e.g., a smartcard, phone, etc.).
Encryption function 230 can be a function that can take inputs, such as the first account number 210 and the other information 220, and transform the inputs into another value. For example, a portion of the first account number 220 can be encrypted. The output of the encryption function 230 can be represented by an encrypted portion 240. Any suitable encryption function including a DES or triple DES encryption functions can be used in embodiments of the invention.

Segments of the encrypted portion 240 can be used to form the second account information. For instance, the mapping function 250 can map a first segment of the encrypted portion 240 to a month and year value. The month and year value might be used as an expiration date for a credit or debit account in a transaction. The expiration date may be a dynamic second expiration date 270.

Other second account information may be determined from the encrypted portion 240. For example, a new dynamic second verification value 260 can be formed from a second encrypted portion segment of the encrypted portion 240. In another example, a new dynamic second account number 280 can be formed with a third encrypted portion segment.

As illustrated in Fig. 2, the new dynamic second account number 280 can be been broken up into three distinct segments including a static signal segment 281, an encrypted account number segment 282, and actual account number digits 283.

According to one embodiment, a new dynamic second verification value 260, a second dynamic account number 280, and a second dynamic expiration date 270 are created from a consumer's first account number 210 by first selecting the digits from the consumer's account number 210 that can serve as the basis for the dynamic numbers. In Fig. 2, the first twelve numbers of the first account number 210 are selected. Other embodiments may use a different combination of numbers from the first account number 210.

Once digits from the first account number 210 have been selected, other information 220 is selected that will be used to help create the second dynamic card verification value 260, the second dynamic account number 280, and the second dynamic expiration date 270. According to one embodiment, at least a portion of the other information 220 is selected so that both the entity encoding the
data (e.g., a processor in a POS terminal, a smartcard, etc.) and the entity decoding the data (e.g., a processor in a server computer remotely located from the point of sale) will know the value of the other information 220 without explicitly transmitting the other information 220 between the entities. For example, the current date could be used as a part of the other information 220. The entities encoding and decoding the data can have a mutual understanding that the other information 220 will comprise at least the current date, and both parties can use this information appropriately. Alternatively or additionally, the other information 220 may use a mutually agreed upon piece of data that will be transmitted as a part of a transaction. For example, the other data might include the price of the transaction or a merchant ID number. Many other possibilities for the value of the other information 220 also exist.

Once portions of the account number 210 and the other information 220 are selected, the encryption function 230 can be used to encrypt the portions of the account number 210 using other information 220 to produce the encrypted portion 240. The encrypted portion 240 can then be used, potentially along with other data, to generate the dynamic second account number 280, the dynamic second expiration date 270, and the dynamic second verification value 260.

In the embodiment illustrated in Fig. 1, a second dynamic account number 280 is created as a combination of a number of pieces of data. A static signal segment 281 can be inserted into the second dynamic account number 280 and can be used to communicate information about how the data was encoded. For example, a static signal segment 281 comprising “11111” might indicate to an authenticating entity that the received account number is not the real first account number, but is a new second account number. Alternatively or additionally, the static signal 281 might indicate additional information about the information that is transmitted, such as the encryption function 230 that was used, the type of other information used 220, how the dynamic data 240 was used to populate the various dynamic fields, etc.

The second dynamic account number 280 can also use segments of the encrypted portion 240. In the embodiment illustrated in Fig. 2, the first seven digits of the encrypted portion 240 is inserted into the middle of the dynamic account.
number 282. In some embodiments, this insertion of data helps to insure that the dynamic account number 280 changes on a regular basis for a given account number 210.

[0049] The second dynamic account number 280 may also contain portions of the actual first account number 210. For example, in the embodiment illustrated in Fig. 2, the last four digits of the actual account number 210 are placed at the end of the dynamic account number 283.

[0050] Portions of the encrypted portion 240 can also be used to create a dynamic second expiration date 270. In the example shown in Fig. 2, the 8th and 9th digits of the encrypted portion 240 are used as the input into a function that maps the 8th and 9th digits to an expiration date. For example, the 8th and 9th digits, taken together, might correspond to a number range spanning "00" to "99." Each of these 100 different values can then be mapped to a specific month and year combination that might be used as an expiration date.

[0051] Portions of the encrypted portion 240 can also be used as a dynamic CW2 value 260 (or other verification value). As shown in Fig. 2, the last three digits of the encrypted portion 240 are used as the CW2 value 260.

[0052] Once the dynamic account number 280, dynamic expiration date 270, and dynamic CW2 260 have been created, this dynamically generated data can be used as the payment data used to conduct a transaction. The dynamically generated data can thus take the place of the actual first account number 210, first expiration date, or first CW2 value associated with the payment card of the consumer. Note that in some embodiments, the real account information such as the real account number may be displayed to the user (e.g., embossed on a card), but the second derived account information may not be visible or displayed to the user, but may be transmitted to the issuer instead of the real first account information.

[0053] An entity wishing to decode the actual first account number 210 for an account from the dynamically generated data (e.g., a server computer in a payment processing network or at an issuer), would typically need to know how the dynamic account number 280, dynamic expiration date 270, and dynamic CW2 field 260 were created in order to extract the actual information out of the dynamic fields. An
entity that knows precisely how the dynamic data is generated could undo the transformation to extract the actual first account number 210, but any entity that did not know how this information was assembled would not be able to extract useable account data out of the dynamic data. Furthermore, the dynamic data could regularly change for each use of the account number, based on how the other information 220 changed.

[0054] The embodiment illustrated in Fig. 2 can have many different variations as will be apparent to one skilled in the art. For example, the precise manner in which the encrypted portion 240 is used to populate the dynamic fields, or the precise digits from the first account number 210 used to create the encrypted portion 240 can all be varied according to various embodiments.

[0055] The processes described above may be implemented by a processor in a portable consumer device (e.g., a payment card), access device, or any other device involved in a transaction. The steps of the methods that are described above may be carried out by a processor executing computer-executable code residing on a computer-readable medium in any one of these devices.

[0056] I. Exemplary Systems

[0057] A system according to an embodiment of the invention is shown in Fig. 3.

[0058] Fig. 3 shows a system 20 that can be used in an embodiment of the invention. The system 20 includes a merchant 22 and an acquirer 24 associated with the merchant 22. In a typical payment transaction, a consumer such as user 30 may purchase goods or services at the merchant 22 using a portable consumer device such as portable consumer device B 32-2 (or portable consumer device A 32-1 or consumer device 32-3). The user 30 may be an individual, or an organization such as a business that is capable of purchasing goods or services. The acquirer 24 can communicate with an issuer 28 via a payment processing network 26.

[0035] As used herein, an "issuer" is typically a business entity (e.g., a bank) which maintains financial accounts for the user and often issues a portable consumer device such as a credit or debit card to the user. A "merchant" is typically
an entity that engages in transactions and can sell goods or services. An "acquirer" is typically a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Embodiments of the invention encompass such single entity issuer-acquirers.

[0059] In Fig. 3, user 30 can use one or more different types of portable consumer devices including consumer device A 32-1 and portable consumer device B 32-2. In one example, consumer device A 32-1 may be in the form of a phone, while portable consumer device B 32-2 may be in the form of a card. The consumer device A 32-1 may consequently be used to communicate with the issuer 28 via a telecommunications gateway 60, a telecommunications network 70, and a payment processing network 26. The different consumer devices A 32-1 and B 32-2 could be linked to the same issuer account number, or could be linked to respectively different issuer account numbers. User 30 may also use a consumer device 32-3 such as a personal computer to communicate with the payment processing network 26 and/or the merchant 22 via the Internet 72.

[0060] The consumer devices according to embodiments of the invention may be in any suitable form. In some embodiments, the consumer devices are portable in nature and may be portable consumer devices. Suitable portable consumer devices can be hand-held and compact so that they can fit into a user'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).

[0061] Each consumer device may comprise a body, and a memory comprising a computer readable medium disposed on or within the body. In addition, the consumer device may also include a processor coupled to the memory, where greater functionality and/or security are desired. The computer readable
medium may comprise code, executable by a processor, for implementing a method comprising: encrypting, using a processor, a portion of a first account number to form an encrypted portion, the first account number being associated with a first expiration date and a first verification value; and determining a second expiration date or a second verification value using a segment of the encrypted portion.

[0062] 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.

[0063] Referring to Fig. 4, the payment processing network 26 may include a server computer 26(a), and a database 26(b) operatively coupled to the 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 network 26 may use any suitable wired or wireless network, including the Internet.

[0064] The server computer 26(a) in the payment processing network 26 may comprise code, executable by a processor, for implementing a method comprising: receiving an initial authorization request message comprising a second account number, and at least one of a second expiration date and a second verification value; determining, using a server computer, a first account number, a first expiration date, and a first verification value from the second account number; and sending a modified authorization request message to an issuer, wherein the modified authorization request message comprises the first account number, the first expiration date, and the first verification value, wherein the first verification value is
different than the second verification value and the first expiration date is different than the second expiration date.

[0065] The database 26(b) may store any suitable type of information. Suitable information that may be stored in the database 26(b) may include a lookup table linking first expiration dates with first encrypted portion segments, as well as other information.

[0066] The server computer 26(a) may also comprise a number of functional modules and data elements. They may include encryption keys 26(a)-1, a decryption module 26(a)-2, and a payment processing module 26(a)-3. Each of these modules may comprise any suitable combination of hardware and/or software to accomplish the functions described herein.

[0067] The payment processing module 26(a)-3 may comprise appropriate logic to process electronic payments. For example, the payment processing module 26(a)-3 may include an authorization sub-module for receiving and passing authorization request messages to appropriate issuers for approval. It may also include a clearing and settlement sub-module for clearing and settling transactions between different issuers and acquirers.

[0068] Referring again to Fig. 3, the merchant 22 may also have, or may receive communications from, an access device 34 that can interact with the portable consumer devices 32-1, 32-2. 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.

[0069] 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.

[0070] II. Exemplary Methods
Methods according to embodiments of the invention can be described with reference to Figs. 3-5. Although specific sequences of steps are described, it is understood that embodiments of the invention are not limited to the order of the specific steps described, and that any suitable combination of steps may be included in embodiments of the invention.

Referring to Fig. 3, the user 30 may conduct a transaction with a merchant 22. The transaction may be conducted in person, or may be conducted via the Internet 72.

In a typical in person purchase transaction, the user 30 purchases a good or service at the merchant 22 using a portable consumer device such as portable consumer device A 32-1, which may be in the form of a credit card, or portable consumer device B 32-2, which may be in the form of a phone. For instance, the user's portable consumer device A 32-a can interact with an access device 34 such as a POS (point of sale) terminal at the merchant 22. For example, the user 30 may take the 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 B 32-2 may be a contactless device such as a contactless card.

In a typical Internet transaction, the user 30 may use his consumer device C 32-3 and may contact the Web site of the merchant 22 via the Internet 72. The user 30 may select goods for purchase and may enter information onto the Web site including payment card information. As described above, the merchant 22 may then request authorization of the transaction from the issuer 28, and a clearing and settlement process may be performed after the authorization process is performed.

Before an authorization request message is forwarded to the acquirer 24, a processor in any of the consumer devices A 32-1, B 32-2, or C 32-3, or in the access device 34, can determine the second account information from the real first account information (as described above). This second account information may include a second account number, a second expiration date, and a second verification value such as a second CW2 value. This second account information may be derived from a real first account number (step 502).
[0076] After the second account information is determined, an authorization request message is then forwarded to the acquirer 24 (step 504).

[0077] After receiving the authorization request message (step 506), the authorization request message is then sent to the payment processing network 26. The server computer 26(a) in the payment processing network 26 then determines that the received second account number is not the user’s real account information after analyzing the signal segment in the second account number. It then determines the first account number, the expiration date, and the verification value associated with the received second account information. It can use the decryption module 26(a)-2 and an appropriate key or keys 26(a)-1 to do this (step 508). After the server computer 26(a) determines the real first account information, the payment processing network 26 (or the server computer located therein) then generates a modified authorization request message including the first account information and then forwards it to the issuer 28 for approval if it does not make the authorization decision (step 510).

[0078] After the issuer 28 receives the authorization request message, the issuer 28 then responds with an authorization response message indicating whether or not the transaction is authorized, and the authorization response message is received at the payment processing network 26 and is forwarded back to the acquirer 24 (steps 512 and 514). The acquirer 24 then sends the response message back to the merchant 22.

[0079] After the merchant 22 receives the authorization response message, the access device 34 at the merchant 22 may then provide the authorization response message for the consumer 30. The response message may be displayed by the access device 34, or may be printed out on a receipt.

[0080] 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.
FIGS. 6, 7, and 8 show block diagrams of consumer devices, computer devices and subsystems that may be present in computer apparatuses in systems according to embodiments of the invention.

The various participants and elements may operate one or more computer apparatuses to facilitate the functions described herein. Examples of such subsystems or components are shown in Fig. 6. The subsystems shown in Fig. 6 are interconnected via a system bus 775. Additional subsystems such as a printer 774, keyboard 778, fixed disk 779 (or other memory comprising computer readable media), 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 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.

A consumer device may be in any suitable form. For example, suitable 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 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 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). Other consumer devices may include personal computers, laptops, or other devices capable of communicating over the internet.

An exemplary consumer device 32' in the form of a phone may comprise a computer readable medium and a body as shown in Fig. 7. (Fig. 7
shows a number of components, and the consumer devices according to embodiments of the invention may comprise any suitable combination or subset of such components.) The computer readable medium 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, uniquely derived keys (such as those described above), encryption algorithms, etc. The memory also 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 consumer device 32.

[0085] 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, plus other discretionary data.

[0086] The 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) 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).

[0087] 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 consumer device 32 and an interrogation device. Thus, the consumer device 32 is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0088] The consumer device 32 may also include a processor 32(c) (e.g., a microprocessor) for processing the functions of the consumer device 32 and a display 32(d) to allow a consumer to see phone numbers and other information and messages. The 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 consumer device 32. The consumer device 32 may also include an antenna 32(a) for wireless data transfer (e.g., data transmission).

[0089] If the consumer device is in the form of a debit, credit, or smartcard, the consumer device may also optionally have features such as magnetic strips. Such devices can operate in either a contact or contactless mode.

[0090] An example of a consumer device 32" in the form of a card is shown in Fig. 2B. Fig. 2B 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).

[0091] As shown in Fig. 8, the 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 consumer
device 32". In other embodiments, either the magnetic stripe 32(n) or the contactless element 32(o) may be present in the consumer device 32".

[0092] 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.

[0093] 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.

[0094] 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.

[0095] 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.

[0096] 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.
[0097] A recitation of "a", "an" or "the" is intended to mean "one or more"
unless specifically indicated to the contrary.

[0098] All patents, patent applications, publications, appendixes, 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:
   - encrypting, using a processor, a portion of a first account number to
     form an encrypted portion, the first account number being associated with a first
     expiration date and a first verification value; and
   - determining a second expiration date or a second verification value
     using a segment of the encrypted portion.

2. The method of claim 1 wherein the segment is a first encrypted
   portion segment, and wherein determining the second expiration date using the first
   encrypted portion comprises determining the second expiration date using the first
   encrypted portion segment.

3. The method of claim 2 wherein determining the second
   expiration date using the first encrypted portion segment comprises mapping the first
   encrypted portion to the second expiration date.

4. The method of claim 3 further comprising determining the
   second verification value using a second encrypted portion segment of the encrypted
   portion.

5. The method of claim 4 further comprising forming a second
   account number using a third encrypted portion segment of the encrypted portion.

6. The method of claim 5 wherein the second account number
   comprises a signal segment, the third encrypted portion segment, and an
   unencrypted portion of the first account number.

7. The method of claim 5 wherein the third encrypted portion
   segment consists of exactly four digits.

8. A computer readable medium comprising code, executable by a
   processor, for implementing a method comprising:
   - encrypting, using a processor, a portion of a first account number to
     form an encrypted portion, the first account number being associated with a first
     expiration date and a first verification value; and
determining a second expiration date or a second verification value using a segment of the encrypted portion.

9. The computer readable medium of claim 8 wherein the segment is a first encrypted portion segment, and wherein determining the second expiration date or the second verification value using the first encrypted portion comprises determining the second expiration date using the first encrypted portion segment.

10. The computer readable medium of claim 9 wherein determining the second expiration date using the first encrypted portion segment comprises mapping the first encrypted portion to the second expiration date.

11. The computer readable medium of claim 10 further comprising determining the second verification value using a second encrypted portion segment of the encrypted portion.

12. The computer readable medium of claim 11 further comprising forming a second account number using a third encrypted portion segment of the encrypted portion.

13. The computer readable medium of claim 12 wherein the second account number comprises a signal segment, the third encrypted portion segment, and an unencrypted portion of the first account number.

14. The computer readable medium of claim 13 wherein the third encrypted portion segment consists of exactly for digits.

15. A computer apparatus comprising the computer readable medium of claim 8, and the processor, coupled to the computer readable medium.

16. A method comprising:

   receiving an initial authorization request message comprising a second account number, and at least one of a second expiration date and a second verification value;
   
   determining, using a server computer, a first account number, a first expiration date, and a first verification value from the second account number; and
sending a modified authorization request message to an issuer,

wherein the modified authorization request message comprises the first account number, the first expiration date, and the first verification value,

wherein the first verification value is different than the second verification value and the first expiration date is different than the second expiration date.

17. The method of claim 16 wherein the initial authorization request message comprises the second account number, the second expiration date, and the second verification value.

18. The method of claim 16 wherein the second account number comprises a signal segment, which informs the server computer to generate the modified authorization request message.

19. The method of claim 16 wherein the first account number, the first expiration date, and the first verification value are associated with a debit or credit card.

20. A computer readable medium comprising code, executable by a processor, for implementing the method of claim 16.

21. A server computer comprising the computer readable medium and the processor coupled to the computer readable medium.
FIG. 1

1. Determine first account number 102.

2. Encrypt a portion of the first account number 104.

3. Select first segment of encrypted portion 106.

4. Map first encrypted portion segment to second exp date 108.

5. Determine second verification value using second encrypted segment 110.

6. Form second account number with third encrypted segment 112.
FIG. 4
DETERMINE SECOND ACCOUNT NUMBER 502

SEND AUTH REQUEST MESSAGE 504

RECEIVE AUTH REQUEST MESSAGE 506

DETERMINE FIRST ACCOUNT NUMBER, EXP DATE AND VERIFICATION VALUE 508

SEND MODIFIED AUTH REQUEST MESSAGE TO ISSUER 510

RECEIVE AUTH RESPONSE MESSAGE 512

SEND AUTH RESPONSE MESSAGE 514

FIG. 5
FIG. 6
FIG. 7

FIG. 8