Portable Account Number for Consumer Payment Account

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority from United States Patent Application No. 12/893,834, entitled "Portable Account Number for Consumer Payment Account," filed September 29, 2010, which claims priority from United States Provisional Patent Application No. 61/310,161, entitled "Portable Account Number for Consumer Payment Account," filed March 3, 2010, the contents of each of which is hereby incorporated in its entirety by reference for all purposes.

BACKGROUND

[0002] Embodiments of the present invention are directed to systems, apparatuses and methods for conducting transactions such as payment transactions and for processing transaction data, and more specifically, to the use of an issuer independent primary account number (PAN) or other form of payment account or device identifier for conducting transactions. Embodiments of the invention implement a payment transaction using a payment account number or payment device identifier which does not include a bank identification number (BIN) or other identifier of the issuer of a payment device. The decoupling of the issuer identifier from the PAN provides a portable and customizable account number that enables greater freedom for consumers and provides the ability to deliver new and improved services to consumers who use payment cards (e.g., credit, debit or prepaid cards) with magnetic stripes or contactless elements embedded in other form factors as payment devices for conducting payment transactions.

[0003] Consumer payment devices such payment cards with magnetic stripes, or contactless chips embedded in other devices are used by millions of people worldwide to facilitate various types of commercial transactions. In a typical transaction involving the purchase of a product or service at a merchant location, the payment device is presented at a point of sale terminal ("POS terminal") located at a merchant's place of

business. A consumer may also initiate a payment transaction by providing payment data from a remote location to a merchant over a network such as the Internet. Transactions of this type are typically initiated using a computing device such as a personal computer or laptop computer. Transactions may also be initiated by using a mobile device such as a cell phone or personal digital assistant (PDA) that communicates with a merchant or service provider directly or indirectly over a wireless network. Transactions in which the consumer is not in the same physical location as a merchant, and hence where a payment device is not physically presented to the merchant, are termed "card not present" (CNP). Further, transactions may also include ones where a merchant or vendor automatically initiates a transaction based on a prior agreement with a customer for charging their payment card an amount at a agreed upon date or frequency. Such transactions may be termed "standing instruction" transactions.

[0004] A consumer's payment device is typically identified by, or associated with a string of alphanumeric characters that is unique to each payment device. The string, along with other associated payment transaction data, is submitted to a merchant, accessed from a payment device, or otherwise provided by a consumer when conducting a payment transaction. Typically, the string of characters is in a specified format, with one standard format being that of a bank identification number (BIN) as a prefix to an account identifier. In some cases, the combination of the BIN and the account identifier is termed a "primary account number" or PAN. The PAN may correspond to the number or alphanumeric string embossed on a credit card or debit card, for example. The BIN or its equivalent is a unique identifier for the bank or organization that acted as issuer for the payment device or for the payment account associated with the device. The BIN may be generated or assigned by a payment processing network, card association or network (such as Visa, MasterCard, or American Express), or other form of payment processor. The account identifier is an identifier for the consumer's individual payment account and may be generated by the issuer in accordance with its internal rules or processes. The combination of the BIN and account identifier represents a unique identifier for the consumer's payment

account or payment device, and as noted, includes information regarding the issuer of the payment account or payment device.

[0005] However, as recognized by the inventor of the present invention, the coupling of the BIN to the account identifier (typically as a prefix to the account identifier) to create a unique PAN does have some disadvantages. For example, a consumer's PAN is typically changed every time they move their payment account to a different issuer, or desire to use a new payment device product provided by the same issuer. In the case of a consumer who has instructed certain merchants or service providers to automatically deduct or charge a specified amount to the consumer's payment account on a regular basis (such as a monthly payment for a loan, etc.), the consumer must notify every such merchant or service provider each time the consumer changes issuers or products offered by the same issuer. This is inconvenient and may lead to errors in which a merchant attempts to charge an amount to, or deduct an amount from, a cancelled or otherwise improper payment account. This situation also creates extra work for the consumer and is an inefficient and wasteful use of data processing resources. Further, the need to use a different combination of BIN and account identifier for each payment device or account increases the data processing and data storage requirements on the payment processing networks used to process payment transactions. The use of a combined BIN and account identifier for payment devices or accounts may also act to limit the types of payment products or combined payment and non-payment products that may be offered by issuers or by other organizations that do not wish to be constrained by the existing system (such as by requiring the involvement of a typical issuer in order to offer the product).

[0006] What is desired are a system, apparatus and method for providing consumers and issuers with a payment account or payment device identifier that can be used to conduct payment transactions and which overcomes the noted disadvantages of current methods of identifying such devices or accounts. Embodiments of the invention address these problems and other problems individually and collectively.

SUMMARY

[0007] Embodiments of the present invention are directed to a system, apparatus, and method for generating a payment account number or payment device identifier for use in conducting a payment transaction, and for enabling a consumer to use that identifier to conduct a payment transaction. In some embodiments of the invention, the bank identification number (BIN) is decoupled from the account identifier when generating the payment account number or payment device identifier (such as the primary account number or PAN). The BIN or its equivalent data that is used to control the routing of payment transaction data or messages to an issuer may be provided in one or more suitable ways, including but not limited to, as a data string in a separate data field from the account identifier (for magnetic stripes on payment cards, for example), as data in a new field that is stored in a chip or data storage element (for smart cards and other types of contact or contactless payment devices), or as data stored in a lookup table or database that is accessed based on the consumer's account number or payment device identifier.

[0008] In one embodiment, the present invention is directed to an apparatus for processing a transaction, where the apparatus includes an electronic processor programmed to execute a set of instructions, a data storage device coupled to the processor, and the set of instructions contained in the data storage device, wherein when the set of instructions are executed by the processor, the apparatus processes the transaction by receiving an authorization request message for the transaction, processing the authorization request message to obtain an account identifier for an account used to conduct the transaction, the account identifier not including information identifying an issuer for the account, accessing a data storage element that includes information associating the account identifier with information identifying the issuer for the account, obtaining the information identifying the issuer for the account from the data storage element, providing the authorization request message to the issuer using the information identifying the issuer for the account obtained from the data storage element and receiving from the issuer for the account an authorization response

message containing a decision from the issuer whether to approve or deny the transaction.

[0009] In another embodiment, the present invention is directed to a method for processing a transaction, where the method includes receiving an authorization request message for the transaction, processing the authorization request message to obtain an account identifier for an account used to conduct the transaction, the account identifier not including information identifying an issuer for the account, using the identifier to determine an issuer for the account, providing the authorization request message to the issuer using the information identifying the issuer for the account, and receiving from the issuer for the account an authorization response message containing a decision from the issuer whether to approve or deny the transaction.

[0010] In yet another embodiment, the present invention is directed to a payment device for conducting a transaction, where the payment device includes a device substrate, a payment device identifier visibly located on the device substrate, the payment device identifier not including information identifying an issuer for the payment device, and a data storage region contained on or within the payment device, the data storage region further comprising a first data storage sub region containing data corresponding to the payment device identifier, and a second data storage sub region electronically isolated from the first data storage sub region and containing data identifying the issuer of the payment device.

[0011] Other objects and advantages of the present invention will be apparent to one of ordinary skill in the art upon review of the detailed description of the present invention and the included figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Fig. 1 is a functional block diagram illustrating the primary functional elements of an exemplary system for conducting an electronic payment transaction and processing payment transaction data that may be used in implementing an embodiment of the present invention;

[0013] Fig. 2 is a diagram illustrating the components of a typical primary account number (PAN) that is used in the processing of a payment transaction;

[0014] Fig. 3 is a diagram illustrating the components of a payment account or payment device identifier that may be used in implementing an embodiment of the present invention;

[0015] Fig. 4 is a flowchart illustrating a method of conducting a payment transaction in accordance with an embodiment of the present invention;

[0016] Fig. 5 is a functional block diagram illustrating a payment processing system including components of a payment processing network and elements that may interact with that network to enable a consumer to conduct a payment transaction using an embodiment of the inventive payment account number or payment device identifier;

[0017] Fig. 6 is a block diagram of elements that may be present in a computer apparatus configured to execute a method or process to conduct a payment transaction using a portable PAN or other form of payment account or payment device identifier, in accordance with some embodiments of the present invention;

[0018] Fig. 7 is a diagram illustrating the front (Figure 7(a)) and back (Figure 7(b)) of a payment device having a magnetic stripe that may be used to conduct a transaction and that functions in accordance with the first implementation of the present invention; and

[0019] Figure 8 is a diagram illustrating the front (Figure 8(a)) and back (Figure 8(b)) of a payment device in the form of a smart card having an embedded chip that may be used to conduct a transaction and that functions in accordance with the second implementation of the present invention.

DETAILED DESCRIPTION

[0020] Embodiments of the present invention are directed to a system, apparatus, and method for generating a payment account or payment device identifier for use in conducting a payment transaction, and for enabling a consumer to use that identifier to conduct a payment transaction. Embodiments of the present invention are also directed to methods of conducting a payment transaction using a payment account or payment device identifier. In some embodiments of the invention, the bank identification number (BIN) is decoupled from the account identifier when generating a payment account number or payment device identifier. This results in a payment account number or payment device identifier (e.g., a PAN or other account number such as is found on a credit or debit card) that does not have the BIN as a prefix. The BIN or its equivalent data that is used for routing of payment transaction data or messages to an issuer (and in some situations may be used to control the processing of payment transaction data in accordance with issuer instructions) may be provided in one or more suitable ways, including but not limited to, as a data string in a separate data field from the account identifier (for magnetic stripes on payment cards, for example), as data in a new field that is stored in a chip or data storage element (for smart cards, contact or contactless payment devices, etc.), or as data stored in a lookup table or database that is accessed based on the consumer's payment account number or payment device identifier.

[0021] Embodiments of the present invention may provide the ability to generate payment account numbers that are independent of an issuer. This enables a greater number of unique payment account numbers to be generated, enables a consumer to personalize or otherwise provide input into the structure of the payment account number (perhaps with the result of a consumer being able to have a single, more easily remembered number), and also enables the use of a payment account number that includes data that may be used to identify a market segment or provide another form of market differentiation in a payment product. Embodiments of the present invention may also increase the types of payment or identification products that are available, as well as increase the adoption of such products. For example, new types of combined payment and non-payment products (e.g., transit system use, loyalty and incentive redemption services, medical record data, etc.) that are not tied to a specific issuer

could be developed by businesses, governmental agencies, billing services, telecommunications service providers, etc. The present invention may permit easier development and distribution of such products and encourage innovation in this area.

[0022] Embodiments of the present invention are typically implemented in the context of a payment transaction, and specifically, in the context of the processing of transaction data as part of a transaction authorization process. In a typical payment transaction, a consumer provides a payment account number or payment device identifier to a merchant or service provider. The payment account number or payment device identifier may be provided in the form of a card (e.g., a magnetic stripe card or smart card with an embedded chip) accessed by a point of sale terminal or card reader, or payment account information may be provided by the consumer in a card not present situation (e.g., over a network as in an eCommerce transaction). Payment account or payment device identifier data may also be provided by a contactless element such as a chip embedded in a mobile phone, PDA, or other device that can function to make a payment for a transaction.

[0023] In order to provide a context in which the present invention may be implemented, a brief discussion of the entities involved in processing and authorizing a payment transaction and their roles in the processing of payment transaction data, will be presented. Figure 1 is a functional block diagram illustrating the primary functional elements of an exemplary system 20 for conducting an electronic payment transaction and processing payment transaction data that may be used in implementing an embodiment of the present invention. Typically, an electronic payment transaction is authorized if the consumer conducting the transaction is properly authenticated (i.e., their identity and their valid use of a payment account is verified) and has sufficient funds or credit to conduct the transaction. Conversely, if there are insufficient funds or credit in the consumer's account, or if the consumer's payment device is on a negative list (e.g., it is indicated as possibly having been stolen), then an electronic payment transaction may not be authorized. In the following description, an "acquirer" is typically a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant. An "issuer" is typically a business entity (e.g., a bank or credit

union) which issues a payment device such as a credit card, debit card, smart card, or contactless device to a consumer and which provides administrative and management functions for the consumer's payment account. Some entities may perform both issuer and acquirer functions.

[0024] As shown in Figure 1, in a typical transaction, a consumer 30 wishing to purchase a good or service from a merchant provides transaction data that may be used as part of a transaction authorization process, typically by means of a portable consumer device 32 that is capable of functioning as a payment device. Consumer 30 may utilize a portable payment device 32 such as a card having a magnetic stripe encoded with account data or other relevant data (e.g., a standard credit or debit card) to initiate the transaction. In an eCommerce (electronic commerce) transaction, the consumer may enter data into a consumer device capable of communicating with a merchant or other element of system 20, such as a laptop or personal computer. The consumer may also initiate the transaction using data stored in and provided from a suitable form of data storage device (such as a smart card, mobile phone or PDA containing a contactless element, or a transportable memory device). As examples, a card or similar payment device may be presented to a point of sale terminal which scans or reads data from that card. Similarly, a consumer may enter payment account data into a computing device as part of an eCommerce transaction. Further, a consumer may enter payment account data into a cell phone or other device capable of wireless communication (e.g., a laptop computer or personal digital assistant (PDA)) and have that data communicated by the device to the merchant, the merchant's data processing system, or a transaction authorization network. A wireless device may also be used to initiate a payment transaction by means of communication between a contactless element embedded within the device and a merchant device reader or point of sale terminal using a near field communications (NFC) or short range communications mechanism, such as RF, infra-red, optical, etc. Thus, in some cases an access device 34 may be used to read, scan, or otherwise interact with a consumer's portable payment device and thereby obtain data used in conducting a payment transaction.

[0025] The payment account data (and if needed for processing the transaction, other consumer data) is obtained from the consumer's device and provided to the merchant 22 or to the merchant's data processing system. The merchant or merchant's data processing system (which may include a point of service terminal or other type of access device) generates a transaction authorization request message that may include data obtained from the consumer's payment device as well as other data related to the transaction and the merchant. As part of generating the authorization request message, the merchant 22 or the merchant's transaction data processing system may access a database which stores data regarding the consumer, the consumer's payment device, or the consumer's transaction history with the merchant. The merchant transaction data processing system typically communicates with a merchant acquirer 24 (e.g., a commercial bank which manages the merchant's accounts) as part of the overall transaction authorization process. The merchant's transaction data processing system and/or merchant acquirer 24 provide data to Payment Processing Network 26, which among other functions, participates in the clearance and settlement processes which are part of the overall transaction processing. As part of the transaction authorization process, an element of Payment Processing Network 26 may access an account database which contains information regarding the consumer's payment history, chargeback or dispute history, credit worthiness, etc. Payment Processing Network 26 communicates with issuer 28 as part of the authorization process, where issuer 28 is the entity that issued the payment device to the consumer and provides administrative and management services for the consumer's payment account. Consumer account data is typically stored in a consumer database which is accessed by issuer 28 as part of the transaction authorization and account management processes.

[0026] In standard operation, an authorization request message is created during a consumer purchase (or proposed purchase) of a good or service at a point of sale (POS). The point of sale may be a merchant's physical location or a virtual point of sale such as a web-site that is part of an eCommerce transaction. In a typical transaction, the authorization request message is sent from the point of sale (e.g., the merchant or the merchant's transaction data processing system) to the merchant's acquirer 24, then to the Payment Processing Network 26, and then to the appropriate issuer 28. An

authorization request message can include a request for authorization to conduct an electronic payment transaction. It may include one or more of an account holder's primary account number (PAN; or, as will be described with reference to embodiments of the present invention, an account or payment device identifier), payment device expiration date, currency code, sale amount, merchant transaction stamp, acceptor city, acceptor state/country, etc. An authorization request message may be protected using a secure encryption method (e.g., 128-bit SSL or equivalent) in order to prevent data from being compromised.

[0027] Portable consumer device 32 (an example of a payment device) may be in any suitable form that can function as a payment device or that may incorporate a contactless chip or other element to enable it to function as a payment device. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include contact or contactless smart cards, credit or debit cards (typically with a magnetic stripe and without an embedded microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), and depending upon the specific device, may incorporate a contactless element that is configured to enable the portable consumer device to function as a payment device. Other examples of suitable portable consumer devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like, where such devices may incorporate a contactless element. Depending upon the specific design, the portable consumer device may function as one or more of a debit device (*e.g.*, a debit card), a credit device (*e.g.*, a credit card), or a stored value device (*e.g.*, a stored value or prepaid card).

[0028] Payment Processing Network 26 may include data processing subsystems and networks, and be configured to implement 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 for transactions and a Base II system which performs clearing and settlement services for transactions.

[0029] Payment Processing Network 26 may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, a server computer may be a database server coupled to a Web server. Payment Processing Network 26 may use any suitable wired or wireless network, including the Internet, to facilitate communications and data transfer between its component system elements.

[0030] Figure 2 is a diagram illustrating the components of a typical primary account number (PAN) that is used in the processing of a payment transaction. The primary account number depicted in Figure 2 may be a data string (numerical or alphanumerical) that is embossed on a face of a credit or debit card (either a magnetic stripe card or a smart card with an embedded chip) and encoded in a data storage element of the card (such as a magnetic stripe), or may be a data string that is stored in a data storage element of a embedded chip or other form of contactless element. Such an embedded chip or other form of contactless element may be incorporated into a mobile phone, key fob, laptop computer, PDA, or other device that may function as a payment device. As shown in the figure, in a typical PAN, the data string may be comprised of two sub-strings or components; a first (depicted as BBBBBB) that represents the issuer of the payment device, and a second (depicted as NNNNNNNNN) that represents a payment account identifier. Note that although the BIN is depicted as being a prefix to an account identifier, in other implementations, the BIN may be a data string within the PAN and not at the front end of the PAN. The issuer identifier (sometimes termed a bank identification number or BIN) is a data string that identifies the issuer of the payment device and is used by a payment processor (such as Visa) to route the transaction authorization message(s) and/or transaction data to the appropriate issuer for approval of a proposed payment transaction. The BIN may also serve to control the data processing operations applied to the transaction data so

that such operations are performed in accordance with the desired procedures of the issuer. In a typical payment transaction, the generation of the PAN and processing of the transaction using the PAN may be performed as follows:

a payment processor (such as Visa) assigns a unique BIN to an issuing bank or other entity (e.g., a credit union);

the issuer generates a payment card or device for a consumer – the card or device identifier (e.g., the PAN) may use the issuer's BIN as a prefix to an account identifier, or the BIN may be placed within or at the end of a data string representing the account identifier;

the consumer conducts a payment transaction using the card or device, and the transaction data and card or device identifier are forwarded to the payment processor;

the payment processor uses the first 6 digits of the card or device identifier (i.e., the BIN) to identify the issuer;

the payment processor processes the transaction in accordance with any instructions defined by or for the issuer, and forwards an authorization request with the card or device identifier to the appropriate issuer; and

the issuer makes a decision whether to approve or deny the transaction and sends a response indicating this decision back to the payment processor.

[0031] Although the payment card or payment device identifier (or payment account number) format described with reference to Figure 2 has proven to be advantageous in enabling payment transactions, as recognized by the inventor of the present invention, it does have some disadvantages. These primarily arise because the format depicted in Figure 2 ties the payment card or device identifier (e.g., the PAN) to a specific issuer. This may have one or more of the following (or other) undesirable effects:

(1) if a consumer wishes to change issuers, then they are required to obtain a new payment device and hence a new PAN;

(2) if a consumer desires to maintain the same issuer, but change the type or category of payment account they use (e.g., move to an account with different benefits, pricing structure, incentive programs, etc.), then they typically are required to obtain a new PAN;

(3) the PAN is generated by procedures defined by a payment processor and an issuer, and hence is a random or pseudo-random data string as far as a consumer is concerned – this does not assist a consumer to easily remember the PAN even if they use the payment account on a regular basis (and it is even more difficult to remember the PAN that should be used for a transaction if a consumer changes their PAN);

(4) given that the first set of characters (typically six) of a PAN are fixed, the number of unique combinations of BIN and account identifier that may be generated may not be sufficient to satisfy the increasing demand for payment accounts and market segment differentiated account offerings desired by issuers and/or consumers;

(5) as payment accounts and payment devices become used for more and more types of transactions (e.g., credit, debit, prepaid, government benefits, dual or multiple use applications (such as transit), etc.) consumers may find it more convenient (as well as increasing their confidence in the security of the device) to have their payment account number or payment device identifier decoupled from an issuer so that they may take advantage of products and services offered by non-banking entities;

(6) in the present system of assigning payment account or payment device identifiers, it is not possible to decouple the issuer identifier from the payment account number and to provide a consumer with a personalized account number – doing so may permit a consumer to have (or even to select) a payment account number that is easier for them to remember and use since it is not changed when they change issuers, etc.;

(7) continued growth in unique account numbers or device identifiers may place stress on the data processing resources used to process payment transactions – actions may need to be taken to curtail the growth in account numbers by consolidating all payment and multi-use accounts of a consumer into one identification number; and

(8) issuers and payment processors may prefer to use the first (n) characters of a payment account number for purposes other than identifying an issuer, for example to segment a market by providing different characters for different levels of service, different incentive programs, etc.

[0032] Thus the current system and method of generating a payment account or payment device number by using an issuer identifier as a prefix to an account identifier (or located within, or at the end of an account identifier data string) creates limitations on the range of payment account or payment device numbers that can be generated by parties other than the issuer that is assigned a specific BIN or other identifier. For example, this restricts other entities from issuing a payment device or creating a payment account for a consumer that uses a previously assigned BIN as a prefix for the data string that is associated with the account or device. It also acts to limit the uses to which the payment account number data can be used by consumers, issuers, and other entities that may seek to develop new products based on mixed use devices, market segmentation, etc.

[0033] In recognition of the noted (and other) limitations of the presently used format for a payment account number, such as that depicted in Figure 2, the inventor of the present invention developed the novel format depicted in Figure 3, which is a diagram illustrating the components of a payment account number or payment device identifier that may be used in implementing an embodiment of the present invention. As shown in the figure, the inventive payment account number or payment account identifier is a numeric or alphanumeric string (depicted as NNNNNNNNNNNNNNN in the figure), which in contrast to the format depicted in Figure 2, does not have the BIN or other issuer identifier as a prefix to, at the end of, or within the data string presenting the account identifier. As will be described, depending on the type of payment device being used by a consumer (e.g., a card with magnetic stripe, smart card, device with embedded chip) and the type of transaction involved (e.g., a card present or a card not present transaction), the inventive payment account number or payment device identifier may be implemented in one or more suitable ways, with a payment transaction that is conducted using that payment device being processed in a manner that depends upon that implementation.

[0034] Although in some embodiments the inventive payment account number or payment device identifier may be of the format described with reference to Figure 3, it should be noted that this is not the only possible format that may be used when

practicing the present invention. Other formats or arrangements of numeric or alphanumeric data are possible and fall within the underlying concepts of the present invention, with such formats or arrangements being understood as those in which the payment account number or device identifier does not include a BIN or similar form of issuer identifier.

[0035] In a first possible implementation, such as one suited for use with a payment card (e.g., credit card or debit card) having a magnetic stripe, the inventive payment account number or payment device identifier is encoded as data present on the magnetic stripe. However, in contrast to the format and data processing described with reference to Figure 2, in this implementation the payment account number (or in this case the card number, which is typically embossed on the card face) does not include the BIN or other issuer identifier data. Instead, the BIN, issuer identifier data, or its equivalent is encoded as a data string (typically numeric or alphanumeric) in a location, track or field on the magnetic stripe that differs from that of the payment account number. When a consumer conducts a transaction with the payment device, the payment account number and the issuer identifier are read from the payment device, typically by a second device such as a card reader or point of sale terminal. The issuer identifier is provided to the payment processor and used to route the transaction authorization request to the appropriate issuer and/or process the transaction in accordance with the desired data processing operations of the issuer. Thus, in this implementation, both a credit card or debit card number (such as that embossed on the face of the card) and a separate issuer identifier data string would be read from two different data storage locations, tracks or fields of the magnetic stripe and provided to a payment processor. The processing of a payment transaction using the payment device would then continue as was described with reference to the standard format depicted with reference to Figure 2; the payment processor processes the transaction in accordance with any instructions defined by or for the issuer, forwards an authorization request with the card or device identifier to the appropriate issuer, and the issuer makes a decision whether to approve or deny the transaction and sends a response indicating this decision back to the payment processor.

[0036] Figure 7 is a diagram illustrating the front (Figure 7(a)) and back (Figure 7(b)) of a payment device 700 having a magnetic stripe that may be used to conduct a transaction and that functions in accordance with the first implementation of the present invention. As shown in the figure, payment device 700 is implemented in the form of a device substrate 702 that provides the form factor for the device. Payment device 700 also includes a magnetic stripe 704 which is typically affixed to the back of substrate 702 (as shown in Figure 7(b), and as indicated by an outline in Figure 7(a)). As shown in Figure 7(a), the front of device 700 includes a visible identifier, such as payment account number 706 which is typically embossed onto substrate 702. As noted, in accordance with the present invention, payment account number 706 does not include data identifying the issuer of device 700. The front of device 700 also typically includes other data, such as the name 708 of the account holder and the expiration date 709 of the payment device. As shown in Figure 7(b), the back of device 700 includes magnetic stripe 704 which functions as a data storage region that is "read" or accessed by a card reader or other form of access device. Magnetic stripe 704 may include one or more distinct data storage sub-regions, such as "tracks" 710 and 712. As described with reference to the first implementation of the present invention, a first data storage sub-region such as track 710 (or a similar data storage region, location, etc.) contains the payment account number 706 shown on the front of device 700, while a second data storage sub-region such as track 712 (or a similar data storage region, location, etc.) contains the issuer identifier data.

[0037] In a second possible implementation, such as one suited for use with a payment device in the form of a smart card (i.e., a card form factor with an embedded chip that communicates using a contact or contactless interface) or in the form of a device with an embedded chip that communicates using a contactless interface and functions as a payment device (such as a mobile phone or PDA), the inventive payment account number or payment device identifier again does not include a BIN, issuer identifier data, or its equivalent. The payment account number or payment device identifier is stored in a first data storage element or memory location of the chip. The BIN, issuer identifier data, or its equivalent is encoded as a data string (typically numeric or alphanumeric) in a second and different data storage element or memory location of

the chip. When a consumer conducts a transaction with the payment device, the payment account number and the issuer identifier are read from the device. The issuer identifier is provided to the payment processor and used to route the transaction authorization request to the appropriate issuer and/or process the transaction in accordance with the desired data processing operations of the issuer. Thus, in this implementation, both a payment account number or payment device identifier and a separate issuer identifier data string would be read from two different memory locations or data storage regions (or sub-regions) of the chip and provided to a payment processor. The processing of a payment transaction using the payment device would then continue as was described with reference to the standard format depicted with reference to Figure 2; the payment processor processes the transaction in accordance with any instructions defined by or for the issuer, forwards an authorization request with the card or device identifier to the appropriate issuer, and the issuer makes a decision whether to approve or deny the transaction and sends a response indicating this decision back to the payment processor.

[0038] Figure 8 is a diagram illustrating the front (Figure 8(a)) and back (Figure 8(b)) of a payment device 800 in the form of a smart card having an embedded chip that may be used to conduct a transaction and that functions in accordance with the second implementation of the present invention. As shown in the figure, payment device 800 is implemented in the form of a device substrate 802 that provides the form factor for the device. Payment device 800 also includes an embedded chip 820 (as shown in Figure 8(b)). As shown in Figure 8(a), the front of device 800 includes a visible identifier, such as payment account number 806 which is typically embossed onto substrate 802. As noted, in accordance with the present invention, payment account number 806 does not include data identifying the issuer of device 800. The front of device 800 also typically includes other data, such as the name 808 of the account holder and the expiration date 809 of the payment device. Embedded chip 820 includes a memory or data storage region 823, that may include one or more distinct data storage sub-regions, such as data storage locations 821 and 822. As described with reference to the second implementation of the present invention, a first data storage sub-region such as data storage location 821 (or a similar data storage region, location, etc.) contains the

payment account number 806 shown on the front of device 800, while a second data storage sub-region such as data storage location 822 (or a similar data storage region, location, etc.) contains the issuer identifier data.

[0039] Data stored in data storage region 823 of chip 820 may be accessed by a second device, such as a card reader or other from of access device. In some embodiments, the data may be accessed by means of a magnetic stripe 804 (as shown in Figure 8(b), and as indicated by an outline in Figure 8(a)) which provides an interface to chip 820. In some embodiments, the data may be accessed by a second device such as a card reader or point of sale terminal using a contactless data transfer mechanism. In such a situation, embedded chip 820 includes a contactless interface 824 that enables data transfer using a contactless mode of operation. Contactless interface 824 may include the capability to communicate and transfer data using a near field communications (NFC) technology or other short range communications technology. Note that although in Figure 8 embedded chip 820 is shown as being associated with a smart card form of payment device, in some embodiments embedded chip 820 (and contactless interface 824) may be embedded into a mobile phone, pager, laptop computer, or other suitable forms of devices that may be made to function as a payment device.

[0040] In a third possible implementation that is suited for use with credit cards, debit cards, smart cards, or devices with embedded chips in eCommerce or other forms of card not present transactions (in which the payment device is not physically present at the same location as the merchant), the inventive payment account number or payment device identifier again does not include a BIN, issuer identifier data, or its equivalent. In this embodiment, the payment account number or payment device identifier is obtained from the consumer or payment device using any suitable means, such as by the consumer providing data from the face of a credit card, debit card or smart card via a web-site, via a voice call, or by entering a command or data into a device (e.g., a mobile phone) that is capable of communicating with a merchant using a suitable communications network. The payment account number or payment device identifier data provided by the consumer is received by the payment processor and used to

access or otherwise obtain the BIN or other form of issuer or routing data appropriate for the payment device. The BIN or other form of issuer identifier may be maintained in a database, lookup table, or other suitable data storage mechanism, with the payment account number or payment device identifier being used to retrieve the issuer identifier by means of a mapping (or other form of association) between the payment account number or payment device identifier and the corresponding issuer data.

[0041] In a typical payment transaction conducted using this implementation, the generation of the payment account number or payment device identifier and the processing of a transaction using that data may be performed as follows, with reference to Figure 4 which is a flowchart illustrating a method of assigning account identifiers and conducting a payment transaction in accordance with an embodiment of the present invention (note that some or all of the following steps may be characteristic of embodiments of the invention and that all steps need not be present in all embodiments of the invention):

a payment processor (such as Visa) assigns a unique BIN to an issuing bank or other entity (e.g., a credit union);

the issuer generates a payment card or device for a consumer – the card or device identifier (e.g., the PAN) does not use the issuer's BIN as a prefix and does not contain data identifying the issuer (stage 402 of Figure 4);

the payment processor or another entity maintains a database or other form of data structure (e.g., a lookup table) that contains an association between the payment card or device identifier and the issuer (stages 404 and 406);

the issuer's data processing system updates the card or device number to issuer identifier (e.g., BIN) mapping maintained by the payment processor (or other entity) to reflect the issued payment card or payment device identifier (e.g., by means of real-time messages, pseudo real-time messages, or batch processing) (stage 406);

the consumer conducts a payment transaction using the payment card or device – the payment account number or payment device identifier is provided to a merchant in any suitable manner (e.g., data entry on a merchant's web-site, via a voice call from the consumer, via data entry at a merchant's location, etc.) and an element of the merchant's data processing system (e.g., a server or other computing device) generates and forwards an authorization request message including the payment account number or the payment device identifier over a communications network to a server computer in a payment processing network operated by the payment processor, (stages 408 and 410);

the server computer in the payment processing network operated by the payment processor receives the authorization request message and accesses a database or other form of data structure (e.g., a lookup table) that contains an association between the payment card or payment device identifier and the issuer to retrieve data identifying the issuer (stages 412 and 414);

the server computer in the payment processing network operated by the payment processor processes the transaction in accordance with any instructions defined by or for the issuer, and re-formats and forwards an authorization request with the payment card or payment device identifier to the appropriate issuer (stage 416). Note that the message forwarded to the appropriate issuer need not contain the issuer identifier (e.g., the BIN or its equivalent) since that information is determined by the payment processor from the database and used to route the message; however, for purposes of quality control and to assure the issuer who receives the message that it is intended for that issuer, the payment processor may modify the incoming message so that the outgoing message provided to the issuer contains the issuer identifier; and

the issuer makes a decision whether to approve or deny the transaction and sends an authorization response message indicating this decision back to the server computer in the payment processing network operated by the payment processor (stages 418 and 420); the authorization response message is then forwarded to the merchant via an acquirer's computer apparatus and a suitable communications network.

[0042] Figure 5 is a functional block diagram illustrating a payment processing system including components of a payment processing network 504 and elements that may interact with that network to enable a consumer to conduct a payment transaction using an embodiment of the inventive payment account number or payment device identifier. As shown in the figure, elements that interact with network 504 include an acquirer 502 which provides an authorization request message 520 for a payment transaction to payment processing network 504 (note that the authorization request message may have been generated in whole or in part by a data processing element of the merchant's data processing system). Payment processing network 504 may provide a processed authorization request message 522 to issuer 510 to assist issuer 510 in deciding whether to authorize or deny a transaction. Issuer 510 provides payment processing network 504 with an authorization response message 524 containing an indication of whether the transaction has been approved or denied. Authorization response message 526 (which may be the same as message 524, or may contain other

information) is provided to acquirer 502 to inform acquirer 502 (and ultimately the merchant and consumer) if the transaction has been approved or denied.

[0043] In processing one or more of the transaction authorization messages, where such messages include transaction authorization request messages 520 and transaction authorization response messages 524, payment processing network 504 may utilize one or more of the components or elements depicted in Figure 5. Such components or elements include a processor or central processing unit 503 that is programmed to execute a set of instructions, where some or all of those instructions may be stored in data storage device or memory 506. The instructions may include instructions which when executed, cause payment processing network 504 to perform one or more transaction authorization processing functions or operations (as suggested by instructions or instruction set 508) and/or operations to identify the issuer (or other entity) associated with the payment account or payment device being used to conduct a payment transaction (as suggested by instructions or instruction set 507). In performing these operations, processor or central processing unit 503 may access one or more databases 509 containing payment account, cardholder, or other relevant data, including, but not limited to, a database or lookup table that includes the previously described association between a payment device identifier and the issuer for that device (note that this information may also be part of a separate data storage element that is accessed when executing instruction set 507). Payment processing network 504 may utilize network interface 505 to enable communication with other elements depicted in Figure 5 by means of a suitable communications network or channel.

[0044] There are many new or improved products and services that may be provided to consumers using an embodiment of the present invention. For example, use of a payment account number or payment device identifier in which the issuer identifier is decoupled from the account number or device identifier may enable an issuer, governmental agency, telecommunications carrier, payment processor, or other entity to provide one or more of the following:

- customized or personalized products for consumers such as a PAN (or its equivalent) that is generated from a consumer's favorite numbers or a more easily remembered string of numeric or alphanumeric characters;
- a PAN having a prefix that allows for market segmentation, tracking of the activities of market segments, and the provision of grades of service to consumers in different segments;
- a PAN that is disassociated from any particular issuer, thereby allowing other entities (such as a payment processing network) to work directly with service providers (such as a telecommunications carrier) to provide new services to consumers that may be billed through channels other than a traditional issuer;
- an integration of a payment account with other personal data or functions (such as identification cards, medical data cards, membership cards, government benefit cards, multi-use cards for a payment function and another function) in a manner that maintains a desired level of privacy and isolation of data for the consumer, while using a static account or device identifier that may be required for provision of those services (e.g., a governmental benefit card may necessitate a static account number so that the government entity can maintain proper administrative control and management of the benefit program);
- a static PAN that can be implemented as part of a payment device embedded in another device (such as a mobile phone), thereby eliminating the need to issue or alter the phone or other device if a consumer changes banking institutions, etc.; and
- a combination of a static PAN and other information regarding a consumer (e.g., location) may enable the provision of additional services or provide added functionality for payment transactions.

[0045] In implementing embodiments of the present invention, it may be desirable to alter or modify elements or processes of a typical payment processing network in order to most effectively implement the invention. For example, implementation of the present invention may involve modifications to the payment device issuing process, the process

used to generate the payment account identifiers, and the processing of transaction data (such as authorization request messages), among others.

[0046] Note that although certain embodiments of the present invention have been described with reference to using an account identifier and an issuer identifier to process a transaction, other implementations of the inventive concept of decoupling the issuer identifier from an account identifier are possible and are within the scope of the present invention. For example, in some embodiments, the identification of the issuer may be obtained from the account identifier and other account data (that may be accessed based on the account identifier), or from data contained in a transaction authorization message. In such embodiments, issuer identifier data is not used, although the issuer is inferred from other sources of data.

[0047] As discussed, in some embodiments, the inventive methods, processes or operations for conducting a payment transaction using a portable PAN may be wholly or partially implemented in the form of a set of instructions executed by a programmed central processing unit (CPU) or microprocessor. The CPU or microprocessor may be incorporated in an apparatus, server or other computing device operated by, or in communication with, a node of the authorization network. As an example, Figure 6 is a block diagram of elements that may be present in a computer apparatus configured to execute a method or process to conduct a payment transaction using a portable PAN or other form of payment account or payment device identifier, in accordance with some embodiments of the present invention. The computer apparatus may be used in any of the components shown, for example, in Figures 1 and 5. The subsystems shown in Figure 6 are interconnected via a system bus 600. Additional subsystems such as a printer 610, a keyboard 620, a fixed disk 630, a monitor 640, which is coupled to a display adapter 650, and others are shown. Peripherals and input/output (I/O) devices, which couple to an I/O controller 660, can be connected to the computer system by any number of means known in the art, such as a serial port 670. For example, the serial port 670 or an external interface 680 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 the system bus 600 allows a central processor 690 to communicate

with each subsystem and to control the execution of instructions that may be stored in a system memory 695 or the fixed disk 630, as well as the exchange of information between subsystems. The system memory 695 and/or the fixed disk 630 may embody a computer readable medium.

[0048] 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.

[0049] 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.

[0050] While certain exemplary embodiments have been described in detail and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not intended to be restrictive of the broad invention, and that this invention is not to be limited to the specific arrangements and constructions shown and described, since various other modifications may occur to those with ordinary skill in the art. For example, although the specific embodiments of the invention refer to payment transactions, it is also possible for embodiments of the invention to be used in non-payment transactions such as money transfer transactions.

[0051] As used herein, the use of "a", "an" or "the" is intended to mean "at least one", unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. An apparatus for processing a transaction, comprising:

an electronic processor programmed to execute a set of instructions;

a data storage device coupled to the processor; and

the set of instructions contained in the data storage device, wherein when the set of instructions are executed by the processor, the apparatus processes the transaction by

receiving an authorization request message for the transaction;

processing the authorization request message to obtain an account identifier for an account used to conduct the transaction, the account identifier not including information identifying an issuer for the account;

accessing a data storage element that includes information associating the account identifier with information identifying the issuer for the account;

obtaining the information identifying the issuer for the account from the data storage element;

providing the authorization request message to the issuer using the information identifying the issuer for the account obtained from the data storage element; and

receiving from the issuer for the account an authorization response message containing a decision from the issuer whether to approve or deny the transaction.

2. The apparatus of claim 1, wherein the account identifier is a payment account identifier comprising a string of numeric or alphanumeric data.

3. The apparatus of claim 2, wherein the string of numeric or alphanumeric data corresponds to a payment account number or payment device identifier associated with a credit card, debit card, or smart card.

4. The apparatus of claim 1, wherein the data storage element is a database and the account identifier is used to retrieve the information identifying the issuer for the account from the database.

5. The apparatus of claim 1, wherein the data storage element is a table containing data and the account identifier is used to retrieve the information identifying the issuer for the account from the table.

6. A method for processing a transaction, comprising:

receiving an authorization request message for the transaction;

processing the authorization request message to obtain an account identifier for an account used to conduct the transaction, the account identifier not including information identifying an issuer for the account;

determining, based on the account identifier, an issuer for the account;

providing the authorization request message to the issuer using the information identifying the issuer for the account; and

receiving from the issuer for the account an authorization response message containing a decision from the issuer whether to approve or deny the transaction.

7. The method of claim 6, wherein determining, based on the account identifier, an issuer for the account further comprises:

accessing a data storage element that includes information associating the account identifier with information identifying the issuer for the account; and

obtaining the information identifying the issuer for the account from the data storage element.

8. The method of claim 6, wherein the account identifier is a string of numeric or alphanumeric data.

9. The method of claim 8, wherein the string of numeric or alphanumeric data corresponds to an account number or payment device identifier associated with a credit card, debit card, or smart card.

10. The method of claim 7, wherein the data storage element is a database and the account identifier is used to retrieve the information identifying the issuer for the account from the database.

11. The method of claim 7, wherein the data storage element is a table containing data and the account identifier is used to retrieve the information identifying the issuer for the account from the table.

12. A payment device for conducting a transaction, comprising:

a device substrate;

a payment device identifier visibly located on the device substrate, the payment device identifier not including information identifying an issuer for the payment device; and

a data storage region contained on or within the payment device, the data storage region further comprising

a first data storage sub-region containing data corresponding to the payment device identifier; and

a second data storage sub-region electronically isolated from the first data storage sub region and containing data identifying the issuer of the payment device.

13. The payment device of claim 12, wherein the data storage region is a magnetic stripe.

14. The payment device of claim 12, wherein the data storage region is located in an embedded chip.

15. The payment device of claim 13, wherein the first data storage sub-region is a first track of the magnetic stripe and the second data storage sub-region is a second data track of the magnetic stripe.

16. The payment device of claim 14, wherein the first data storage sub-region is a first memory location of the embedded chip and the second data storage sub-region is a second memory location of the embedded chip.

17. The payment device of claim 12, wherein the payment device identifier is a numeric or alphanumeric string.

18. The payment device of claim 14, further comprising a contactless interface operative to enable communication and data transfer between the payment device and a second device.

19. The payment device of claim 18, wherein the second device is a point of sale terminal.

20. The payment device of claim 18, wherein the second device is a device reader.