



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
60/884,089	01/09/2007		200	16222U-024411US	5		

CONFIRMATION NO. 1975

66945
TOWNSEND AND TOWNSEND CREW LLP
TWO EMBARCADERO CENTER, 8TH FLOOR
SAN FRANCISCO, CA 94111

FILING RECEIPT

Date Mailed: 01/26/2007

Receipt is acknowledged of this provisional Patent Application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Ayman Hammad, Pleasanton, CA;

Power of Attorney: The patent practitioners associated with Customer Number 66945

If Required, Foreign Filing License Granted: 01/25/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US60/884,089**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

AUTHENTICATION USING MULTIPLE COMPONENTS

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant

to 37 CFR 5.15(b).

Application Data Sheet

Application Information

Application number::

Filing Date::

Application Type:: Provisional

Subject Matter:: Utility

Suggested classification::

Suggested Group Art Unit::

CD-ROM or CD-R??::

Number of CD disks::

Number of copies of CDs::

Sequence Submission::

Computer Readable Form (CRF)?::

Number of copies of CRF::

Title:: AUTHENTICATION USING MULTIPLE
COMPONENTS

Attorney Docket Number:: 16222U-024411US

Request for Early Publication:: No

Request for Non-Publication:: No

Suggested Drawing Figure::

Total Drawing Sheets:: 5

Small Entity?:: No

Latin name::

Variety denomination name::

Petition included?:: No

Petition Type::

Licensed US Govt. Agency::

Contract or Grant Numbers One::

Secrecy Order in Parent Appl.: No

Applicant Information

Applicant Authority Type:: Inventor
Primary Citizenship Country:: US
Status:: Full Capacity
Given Name:: Ayman
Middle Name::
Family Name:: Hammad
Name Suffix::
City of Residence:: Pleasanton
State or Province of Residence:: CA
Country of Residence:: US
Street of Mailing Address:: 6048 Corte Monatanas
City of Mailing Address:: Pleasanton
State or Province of mailing address:: CA
Country of mailing address:: US
Postal or Zip Code of mailing address:: 94566

Correspondence Information

Correspondence Customer Number:: 66945

Representative Information

Representative Customer Number:: 66945

Domestic Priority Information

Application:: Continuity Type:: Parent Application:: Parent Filing Date::

Foreign Priority Information

Country:: Application number:: Filing Date::

Assignee Information

Assignee Name::

Street of mailing address::

City of mailing address::

State or Province of mailing address::

Country of mailing address::

Postal or Zip Code of mailing address::

AUTHENTICATION USING MULTIPLE COMPONENTS

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] NOT APPLICABLE

BACKGROUND OF THE INVENTION

5 **[0002]** There are a number of ways to ensure that payment transactions are securely conducted. Embodiments of the invention are directed to improved payment transaction authentication processes and systems, as well as components thereof.

SUMMARY OF THE INVENTION

10 **[0003]** Systems and methods for improved consumer and portable consumer device authentication are disclosed. Embodiments of the invention include ways to authenticate a portable consumer device such as a payment card, authenticate a consumer using the portable consumer device, perform back end processing, and provide consumer notification of purchase transactions.

15 **[0004]** Embodiments of the invention are directed to specific combinations of these different aspects, as well as specific embodiments related to those specific aspects. Further details regarding embodiments of the invention are provided below in the Detailed Description, Claims, and Appendix.

BRIEF DESCRIPTION OF THE DRAWINGS

20 **[0005]** FIG. 1 shows a block diagram of a system according to an embodiment of the invention.

[0006] FIG. 2 shows a block diagram of aspects of a payment transaction authentication system according to an embodiment of the invention.

25 **[0007]** FIGS. 3(a)-3(c) show schematic views of batteryless cards according to embodiments of the invention.

[0008] FIG. 4 shows a portable security device.

[0009] FIG. 5 shows a representation of data fields associated with a portable consumer device such as a credit card.

[0010] FIG. 6 shows parts of a primary account number (PAN).

5

DETAILED DESCRIPTION

[0011] I. Exemplary Systems and Payment Transactions

[0012] Embodiments of the invention are directed to improved transaction authentication systems and methods. In a typical purchase transaction, a consumer uses a portable consumer device (e.g., a credit card) to purchase goods or services from a merchant.

[0013] FIG. 1 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 **30** may purchase goods or services at the merchant **22** using a portable consumer device **32**. The acquirer **24** can communicate with an issuer **28** via a payment processing system **26**.

[0014] The consumer **30** may be an individual, or an organization such as a business that is capable of purchasing goods or services.

[0015] The portable consumer device **32** may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, 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).

[0016] The payment processing system **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 system may include VisaNet™. Payment processing
5 systems such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

10 **[0017]** The payment processing system **26** may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing system **26**
15 may use any suitable wired or wireless network, including the Internet.

[0018] The merchant **22** may also have, or may receive communications from, an access device **34** that can interact with the portable consumer device **32**. The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular
20 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.

[0019] 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
25 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**.

[0020] In a typical purchase transaction, the consumer **30** purchases a good or service at the merchant **22** using a portable consumer device **32** such as a credit
30 card. The consumer's portable consumer device **32** can interact with an access device **34** such as a POS (point of sale) terminal at the merchant **22**. For example, the consumer **30** may take a credit card and may swipe it through an appropriate slot

in the POS terminal. Alternatively, the POS terminal may be a contactless reader, and the portable consumer device **32** may be a contactless device such as a contactless card.

[0021] An authorization request message is then forwarded to the acquirer **24**.

5 After receiving the authorization request message, the authorization request message is then sent to the payment processing system **26**. The payment processing system **26** then forwards the authorization request message to the issuer **28** of the portable consumer device **32**.

[0022] After the issuer **28** receives the authorization request message, the
10 issuer **28** sends an authorization response message back to the payment processing system **26** (step **56**) to indicate whether or not the current transaction is authorized (or not authorized). The transaction processing system **26** then forwards the authorization response message back to the acquirer **24**. The acquirer **24** then sends the response message back to the merchant **22**.

15 **[0023]** 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 POS terminal, or may be printed out on a receipt.

[0024] At the end of the day, a normal clearing and settlement process can be
20 conducted by the transaction processing system **26**. A clearing process is a process of exchanging financial details between an acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position. Clearing and settlement can occur simultaneously.

[0025] Embodiments of the invention are not limited to the above-described
25 embodiments. For example, although separate functional blocks are shown for an issuer, payment processing system, and acquirer, some entities perform (e.g., Discover, AMEX, etc.) all of these functions and may be included in embodiments of invention.

[0026] II. Transaction Authentication

[0027] Referring to FIG. 2, which shows a conceptual block diagram **100**, the authentication of a purchase transaction can have various aspects. Such aspects include portable consumer device authentication **100(a)**, consumer authentication **100(b)**, back end processing including real time risk analysis **100(c)**, and consumer notification of the purchase transaction **100(d)**.

[0028] Portable consumer device authentication relates to the authentication of the portable consumer device. That is, in a portable consumer device authentication process, a determination is made as to whether the portable consumer device that is being used in the purchase transaction is the authentic portable consumer device or a counterfeit portable consumer device. Specific exemplary techniques for improving the authentication of a portable consumer device include:

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

[0029] Consumer authentication relates to a determination as to whether or not the person conducting the transaction is in fact the owner or authorized user of the portable consumer device. Conventional consumer authentication processes are conducted by the merchants. For example, merchants may ask to see a credit card holder's driver's license, before conducting a business transaction with the credit card holder. Other ways to authenticate the consumer would be desirable, since consumer authentication at the merchant does not occur in every instance. Specific examples of possible ways to improve the consumer authentication process include at least the following:

- Knowledge-based challenge-responses
- Hardware tokens (multiple solution options)

- OTPs (one time password, limited use)
- AVSs (not as a stand alone solution)
- Signatures
- Software tokens

- 5
- PINs (online/offline)
 - User IDs/Passcodes
 - Two-channel authentication processes (e.g., via phone)
 - Biometrics

10 **[0030]** Back end processing relates to processing that may occur at the issuer or payment processing system, or other non-merchant location. As will be explained in detail below, various processes may be performed at the "back end" of the payment transaction to help ensure that any transactions being conducted are authentic. Back end processing may also prevent transactions that should not be authorized, and can allow transactions that should be authorized.

15 **[0031]** Lastly, consumer notification is another aspect of transaction authentication. In some cases, a consumer may be notified that a purchase transaction is occurring or has occurred. If the consumer is notified (e.g., via cell phone) that a transaction is occurring using his portable consumer device, and the consumer is in fact not conducting the transaction, then appropriate steps may be
20 taken to prevent the transaction from occurring. Specific examples of consumer notification processes include:

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

25 **[0032]** Specific details regarding some of the above-described aspects are provided below. The specific details of the specific aspects may be combined in any suitable manner without departing from the spirit and scope of embodiments of the invention. For example, portable consumer device authentication, consumer

authentication, back end processing, and consumer transaction notification may all be combined in some embodiments of the invention. However, other embodiments of the invention may be directed to specific embodiments relating to each individual aspects, or specific combinations these individual aspects.

5 **[0033] III. Portable Consumer Device Authentication**

[0034] Improvements can be made with respect to various portable consumer device authentication processes. Examples of such improvements are provided below.

[0035] A. *Dynamic card verification values (dCVVs)*

10 **[0036]** To help ensure that the portable consumer device being used in a payment transaction is in fact the authentic portable consumer device, "dynamic" data may be provided from the portable consumer device. Dynamic data is data that may change over time, and is therefore more secure than static data (e.g., a name). For example, a portable consumer device authentication process may include
15 "dynamic" verification data such as a dynamic CVV (or dynamic card verification value).

[0037] In comparison, "static" data may be data that does not change over time. For example, today, credit cards have card verification values (CVV values) printed on the back of the cards. These values can be used to verify that the
20 portable consumer device being used is authentic. For example, when conducting a purchase transaction over the telephone or the Internet using a credit card, a merchant may ask for the CVV value on the back of the credit card. The CVV value may be matched to the credit card number to ensure that the caller in fact possesses the authentic portable consumer device. One problem with current CVVs is that they
25 are static. They can be stolen and used.

[0038] Dynamic CVV ("dCVV") is described in U.S. Patent Application No. 10/642,878, which is herein incorporated by reference in its entirety for all purposes. A copy of this patent application is attached hereto in the attached Appendix. U.S. Patent Application No. 10/642,878 describes the generation of a verification value
30 using information including a PAN (primary account number), an expiration date, a

service code, and an automatic transaction counter. This verification value is transmitted from a merchant to an issuer where it is decoded and evaluated for possible approval. The automatic transaction counter keeps track of the number of times that a portable consumer device is used, and if there is a mismatch between a counter value that is received at the issuer and the counter at the issuer, then this may indicate possible data skimming or fraudulent use.

[0039] The dCVV or other dynamic data may be transmitted using any suitable secure data transmission process and may use DES (dynamic encryption standard), as well as ECC (elliptical curve cryptography), or AEC (advanced encryption cryptography). Any symmetric or asymmetric cryptographic elements may be used.

[0040] Other security enhancements of the dCVV process may include the use of a longer DES number and a longer counter.

[0041] B. *dCVVs created with specific input data*

[0042] It would be desirable to improve upon the dCVV processes by generating different dynamic verification values using different data or different types of variable information. For example, more transaction and/or user specific data could be dynamically changed to verify that the portable consumer device is the correct one. This would be more secure than using just a simple counter. For example, specific information could include the following: terminal ID, time of day, telephone number, SIM card number, transaction amount, account number, service code (two digits), expiration date, current date, random numbers from the terminal, etc. The specific information preferably includes at least one dynamic data element such as a counter, time of day, purchase amount, etc. In other embodiments, the specific information used to create the dynamic verification value includes dynamic, consumer specific or transaction specific information such as the time of day when the transaction is taking place, the purchase amount, prior transaction data, etc. Any, some, or all of these may be used to create a verification value or other specific pieces of information could be dynamically altered to create a new dCVV. The new dCVV could then be processed in a manner that is similar to, or different than, the general process scheme described in U.S. Patent Application No. 10/642,878. In

one specific example, data regarding a prior transaction (e.g., a prior purchase amount, the time of a prior purchase, etc.) may be a dynamic data element, which may be used to authenticate a portable consumer device for future transactions.

[0043] *C. Reducing the number of rejected dCVV transactions*

5 **[0044]** The above described dCVV processes are useful. There may, however, be a number of instances where the dynamic data (e.g., a counter value) transmitted from a portable consumer device and received at an issuer's server does not match the corresponding dynamic data (another corresponding counter value) that are generated at the issuer's server. For example, sometimes, a merchant
10 might not forward transaction data to the issuer in a timely manner. If this occurs, it is possible that future transactions conducted by the consumer could be inadvertently rejected. For instance, if the portable consumer device used by the consumer has a counter in it to count the number of transactions conducted, and if the counter in the issuer's server does not keep a corresponding transaction count,
15 because of the delayed receipt of transaction data from one or more merchants, some of the consumer's transactions may be inadvertently rejected.

[0045] The solution to this problem may include widening the range of the transaction counter (or widening the tolerance of some other variable data such as the time, date, etc.) so that there is some margin for potential error. For example, a
20 consumer's portable consumer device may have a counter in it that currently has a transaction total equal to 100. When the consumer conducts a transaction at a POS terminal, an authorization message may be sent from the POS terminal to the issuer's server. The authorization message may indicate that this is transaction number 100 for consumer A. The issuer's server may then check a corresponding
25 counter range. If the received transaction counter falls within the corresponding counter range determined by the issuer, then the transaction is approved. For example, the corresponding counter range may be between 98 and 102. Since the consumer's counter is 100 and falls between 98 and 102, the transaction is approved. Thus, if the issuer's server has a counter that has a value that is slightly
30 different than the counter on the consumer's portable consumer device, the transaction will not be inadvertently rejected. If actual data skimming is occurring or if a consumer's payment account number is being used without authorization, the

counter at the issuer's server would likely differ significantly from the actual counter on the consumer's portable consumer device.

[0046] These embodiments of the invention can help decrease the number of false transaction denials. As an alternative or additional authentication measure, the issuer may provide a challenge question (e.g., what is your birthday) to the consumer if the issuer's server finds that the transaction counter received from the POS terminal and the transaction counter at the issuer's server do not match, or if the counter is not within a predetermined counter range determined by the issuer's server computer. If the consumer answers the challenge question correctly, then the transaction is approved. If the question is not answered correctly, then it is not approved.

[0047] *D. Portable Consumer Devices That Can Produce dCVVs.*

[0048] A number of different portable consumer devices may be produced, which are capable of providing variable transaction data such as counters. An example of this kind of portable consumer device includes a magnetic-stripe card that can rewrite the data provided on its magnetic stripe. A re-writing device such as a magnetic write head may be used to rewrite the data on a magnetic stripe. A patent that discusses this type of card is U.S. Patent No. 7,044,394, which is herein incorporated by reference in its entirety for all purposes. A battery is within the card and can supply power for the re-writing device.

[0049] The use of batteries in payment cards is not particularly desirable. For example, batteries need to be replaced and disposed of in an environmentally friendly manner. Also, if a battery-powered card does not have sufficient power at a given moment, a particular transaction conducted with that card may not take place as intended. In addition, if a consumer has multiple battery-powered cards in his wallet, this can raise potential security issues when traveling on airlines. Thus, batteryless cards are preferred.

[0050] In some embodiments, the portable consumer devices are batteryless cards (or other batteryless form factors) which contain may contain chip which may comprise a counter. These batteryless cards are powered by some external power source, instead of an internal battery. Examples of external power sources include

access devices such as POS terminals and transaction calculators. In embodiments of the invention, each time a batteryless card is powered by an external power source such as a POS terminal, a counter value (or other variable data) may be produced by the batteryless card. A number of specific embodiments are shown in
5 FIGS. 3(a)-3(c).

[0051] FIG. 3(a) shows a magnetic stripe card **202** including a plastic body **202(a)**. A magnetic stripe **202(e)** is on the plastic body **202(a)**. The plastic body **202(a)** may include an embossed region, which may have information such as cardholder name, card number, and expiration date (not shown). A processor (e.g.,
10 a microprocessor) **202(b)** is on the plastic body **202(a)**, and a read-write device **202(d)** and an antenna **202(c)** are coupled to the processor **202(b)**. In this example, the antenna **202(c)** is a coil of wire which can receive power from a contactless card reader (not shown).

[0052] During use, the antenna **202(c)** may allow the magnetic stripe card **202**
15 to communicate with an external contactless reader (not shown) so that an account number and optionally counter information (or other variable data) may be obtained from magnetic stripe **202(e)** via the processor **202(b)** and the read-write device **202(d)**. At the same time, the antenna **202(c)** may also be used to power the processor **202(b)** and the read-write device **202(d)** temporarily so that the read-write
20 device **202(d)** can also change dynamic data (e.g., a counter) on the magnetic stripe **202(e)**. Thus, as illustrated by this example, embodiments of the invention can include the use of a batteryless magnetic-stripe card that can provide dynamic data that can be used in a portable consumer device authentication transaction.

[0053] Although the example in FIG. 3(a) includes a read-write device **202(d)**
25 for a magnetic stripe **202(e)**, in other embodiments, the read-write device may be embodied by logic which may read and/or write data to a volatile or semi-volatile solid-state memory device such as a flash memory chip or the like.

[0054] Another card embodiment **204** of the invention is shown in FIG. 3(b). In FIGS. 3(a) and 3(b), like numerals designate like elements. However, in FIG.
30 3(b), a conductive contact region **202(f)** is shown and the conductive contact is coupled to the processor **202(b)** instead of an antenna. In this example, the contact region **202(f)** may include multiple electrical contacts so that it may interface with

and electrically contact a corresponding contact region in a card reader (not shown). When the card **204** is used, power can be supplied to the processor **202(b)** via the conductive contact **204(f)**, and the read-write device **202(d)** can function as described above.

5 **[0055]** FIG. 3(c) shows another magnetic stripe card **206** according to an embodiment of the invention. It includes a portable consumer device reader interface region such as a interface region **202(g)**, which may take the form of the above-described antenna **202(c)** or electrically conductive contact **202(f)**. Power can be supplied to the processor **202(b)** and the read-write device **202(d)** via the
10 interface region **202(g)** as described above.

[0056] However, in this embodiment, a semi-static display **202(h)** is coupled to the processor **202(b)**. Each time the processor **202(b)** is powered by a card reader during a purchase transaction, the processor **202(b)** can cause the display **202(h)** to display a verification value such as a dynamic card verification value (dCVV). The
15 dCVV may be viewed by a consumer and used in a mail order, telephone, or Internet purchase transaction to help verify that the consumer has an authentic card. In this example, the same or different dCVV value (or other dynamic data) may be electronically transmitted to the card reader and subsequently transmitted in an authorization request message to the issuer for further verification.

20 **[0057]** FIG. 4 shows a security device **300** which can be used to power cards of the type shown in FIGS. 3(a)-3(c). The security device **300** may have a data input region **300(b)** (e.g., keys) on a housing **300(a)**. The housing **300(a)** may define a slot **300(d)** which can receive a batteryless card like those described above. A display **300(c)** is also present on the housing **300(a)**.

25 **[0058]** The security device **300** may contain a microprocessor, batteries, and a memory comprising computer code for producing a one-time transaction code or number for a consumer purchase transaction. The logic for producing the one-time transaction code may also reside on another server or computer (e.g., an issuer's server) so that the issuer, merchant, or other party, can verify that the person holding
30 the card is in fact the authorized cardholder. In this example, the security device **300** may be characterized as a hard security token and may be used to help authenticate the consumer.

[0059] During use, a consumer may insert a batteryless magnetic stripe card (as described above) into the slot **300(d)**. A one time transaction code may then be displayed on the screen **300(c)**. When the card is inserted into the security device **300**, power from the power source in the security device **300** powers a processor and read-write device in the card so that dynamic data (e.g., a counter) on the card can change. Thus, the security device **300** can produce a one time transaction number for a transaction, and also temporarily supply power to a batteryless card so that a counter (or other dynamic element) can change in the card. A system using both the security device **300** and a batteryless card that can have dynamic data can advantageously authenticate both the consumer as well as the portable consumer device.

[0060] F. *Masked primary account numbers (PANs)*

[0061] Another way to authenticate a portable consumer device is to use a masked PAN or primary account number. In this example, a partial portion of a transmitted PAN is masked and/or dynamically changed. The PAN includes an identification number portion such as a BIN number or bank identification number. Other examples of identification number portions include a merchant location, financial institution location, or even an IP address. The last four digits of the PAN and the BIN number will remain the same, while other numbers in the PAN change. These dynamically changing numbers are typically masked on a payment card receipt that is received by a consumer so that the consumer does not see anything unusual.

[0062] FIG. 5 shows a schematic diagram of data fields for data that is transmitted from a merchant to an issuer in a purchase transaction. The data fields include PAN, expiration date, service code, PIN CVV, and discretionary data fields.

[0063] An exemplary PAN **380** that might reside in memory (e.g., a magnetic stripe) in a portable consumer device is shown in FIG. 6. In this example, the first six digits (i.e., a first end portion) "123456" **380(a)** of the PAN **380** would correspond to the BIN number. The next 6 digits **380(b)** may be changed or different from the real PAN's 6 digits and are represented by "XXXXXX" in this example. The last four digits **380(c)** (i.e., a last end portion) are "9999" in this example, and would remain

the same. By keeping the BIN the same and the last four digits the same, the transaction will look like a real one to the merchant and the consumer. In a preferred embodiment, the middle six digits are dynamically changed using a counter or the like. This makes it more difficult for any unauthorized person to determine the real PAN.

[0064] In one embodiment, the middle portion of the PAN that resides in the memory of the portable consumer device may be different than the middle portion of the real PAN. The PAN that resides in memory may be referred to as a secondary PAN while the real PAN may be referred to as a primary PAN. An appropriate algorithm or look-up table (e.g., stored at the issuer or in an access device such as a POS device) may be used to link the primary and secondary PANs. For example, the middle six digits of the PAN number might be 666666 in a primary PAN (e.g., 1234566666669999), but the middle six digits might be 222222 in the secondary PAN (e.g., 1234562222229999) which is stored in the memory in a consumer's portable consumer device. In one embodiment, the secondary PAN may be received at a POS terminal and the POS terminal may convert the secondary PAN to the primary PAN and the primary PAN may be transmitted from the POS terminal to the issuer for processing and/or authorization. In another embodiment, the secondary PAN may be transmitted to the issuer and the issuer may convert the secondary PAN to the primary PAN, and may thereafter process and/or authorize the transaction.

[0065] In this embodiment, the issuer may receive both the primary PAN and the secondary PAN to verify that the portable consumer device being used is authentic. If an unauthorized person tries to use the primary PAN, then that unauthorized person will not know the secondary PAN and cannot fraudulently conduct a purchase transaction without knowing the secondary PAN. Alternatively, if an unauthorized person electronically intercepts or "skims" the secondary PAN, then the unauthorized person will not be able to conduct the purchase transaction without knowing the primary PAN.

[0066] In another embodiment, the middle portion of the PAN may be changed dynamically. For example, an appropriate algorithm or counter may be used to dynamically change the middle portion of the PAN each time the portable consumer

device is used. This way, even if the PAN is electronically intercepted by an unauthorized person, and knows the primary PAN, the secondary PAN will be dynamically changing. Even if the unauthorized person knows the primary PAN and intercepts the secondary PAN once, the intercepted secondary PAN would be
5 useless, since it is a dynamically changing secondary PAN. In this case, the unauthorized person would need to know the algorithm used to dynamically change the PAN in addition to the primary PAN and the secondary PAN. Thus, this embodiment is particularly useful for conducting secure transactions.

[0067] VI. Consumer authentication

10 **[0068]** As noted above, a number of consumer authentication processes can be used in embodiments of the invention. Specific examples of possible ways to improve the authentication of a consumer include:

- Knowledge-based challenge-responses
- Hardware tokens (multiple solution options)
- 15 • OTP (one time password, limited use)
- AVS (not as a stand alone solution)
- Signatures
- Software token
- PINs (online/offline)
- 20 • User IDs/Pascodes
- Two-channel authentication via phone
- Biometrics

[0069] As illustrated above, a variety of mechanisms may be used to authenticate the consumer and the mechanisms may use no user input (e.g., an
25 auto-software security token), limited user input (e.g., the user presses a button), or full user input (e.g., biometrics).

[0070] In addition, various "security tokens" may be used to help authenticate the user. A security token is an article or piece of information that can be used to verify real information or data. For example, a PIN may be a security token and may be used to verify the identity of the consumer when the consumer makes a
5 purchase. In another example, a challenge question and corresponding answer may be considered a security token that helps to authenticate the consumer. This latter example is an example of a token having a "bi-directional channel" whereby information flows to the consumer and the consumer sends information back to another party such as an issuer so that the user can authenticate himself.

10 **[0071]** 1. *Knowledge based challenges*

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

[0072] Thus, in embodiments of the invention, the payment processing
25 organization, the issuer, or any other non-merchant entity with information about the consumer may pose challenge questions to the consumer to authenticate the consumer. The challenge questions may be static where the same questions are asked for each purchase transaction or dynamic where different questions may be asked over time.

30 **[0073]** The questions asked may also have static or dynamic (semi-dynamic or fully dynamic) answers. For example, the question "What is your birthday?"

requires a static answer, since the answer does not change. The question "What is your zip-code?" requires a semi-dynamic answer, since it could change or can change infrequently. Lastly, the question "What did you purchase yesterday at 4 pm?" would require a dynamic answer since the answer changes frequently. Thus, in preferred embodiments, the challenge questions would preferably be based on "real time" information that the issuer would most likely possess. For example, the consumer might be asked a more specific question such as "Did you eat out at a Mexican restaurant last night?" By providing more specific knowledge based consumer challenges, the authentication of the consumer is ensured.

[0074] 2. *User account level authorization*

[0075] The consumer may also provide user-defined and user-modifiable input to assist in the authorization process. A consumer may determine the kinds and/or quantity of challenge questions to ask himself or herself. For example, the consumer may specify that the consumer wants to be asked three challenge questions if the consumer visits a jewelry store, but only one question if the consumer visits a fast food restaurant. The types of questions posed by the consumer may be based on the merchant type, frequency of purchasing, etc. Some concepts relating to user-defined authorization parameters are described in U.S. Patent Application No. 10/093,002, filed on March 5, 2002, which is herein incorporated by reference in its entirety for all purposes.

[0076] 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

[0077] 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.

5 **[0078]** 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
10 equivalents.

[0079] 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.

[0080] A recitation of "a", "an" or "the" is intended to mean "one or more"
15 unless specifically indicated to the contrary.

[0081] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

1 1. A method for authenticating a consumer transaction, the system
2 comprising:

3 authenticating a portable consumer device wherein the portable
4 consumer device includes dynamic data, wherein the portable consumer device is
5 associated with a consumer; and

6 authenticating the consumer, wherein the authentication is initiated by
7 a non-merchant entity, and wherein the non-merchant entity asks challenge
8 questions to the consumer, wherein the challenge questions are dynamic.

1 2. A method for authenticating a consumer transaction, the method
2 comprising:

3 authenticating a portable consumer device wherein the portable
4 consumer device includes dynamic data, wherein the portable consumer device is
5 associated with a consumer;

6 authenticating the consumer, wherein the authentication is initiated by
7 a non-merchant entity;

8 performing a back-end evaluation of the consumer transaction; and
9 optionally

10 notifying the consumer of the consumer transaction.

1 3. The method of claim 2 wherein the portable consumer device is
2 a card.

1 4. The method of claim 2 wherein the non-merchant entity is at
2 least one of a payment processing organization and an issuer.

1 5. A computer readable medium comprising:

2 code for authenticating a portable consumer device wherein the
3 portable consumer device includes dynamic data, wherein the portable consumer
4 device is associated with a consumer;

5 code for authenticating the consumer, wherein the authentication is
6 initiated by a non-merchant entity;

7 code for performing a back-end evaluation of the consumer
8 transaction; and optionally

9 code for notifying the consumer of the consumer transaction.

1 6. A server computer comprising the computer readable medium of
2 claim 5.

1 7. A payment processing system comprising the server computer
2 of claim 6.

1 8. An authentication method comprising:
2 generating a verification value, wherein the verification value is unique
3 to a purchase transaction, wherein the verification value is generated using at least
4 one dynamic data element that is specifically associated with a consumer conducting
5 the purchase transaction or specifically relates to the purchase transaction; and
6 sending the verification value to an issuer so that the issuer can verify
7 that the transaction.

1 9. The authentication method of claim 8 wherein dynamic data
2 element includes at least one of the time of day, telephone number, SIM card
3 number, transaction amount, and the current date.

1 10. A computer readable medium comprising:
2 code for generating a verification value, wherein the verification value
3 is unique to a purchase transaction, wherein the verification value is generated using
4 at least one dynamic data element that is specifically associated with a consumer
5 conducting the purchase transaction or specifically relates to the purchase
6 transaction; and
7 code for sending the verification value to an issuer so that the issuer
8 can verify that the transaction can be conducted.

1 11. A portable consumer device comprising the computer readable
2 medium of claim 10.

1 12. A method comprising:
2 receiving from a portable consumer device, a verification value derived
3 from a dynamic data element;

4 determining if the dynamic data element is within a predetermined
5 range; and
6 approving a transaction if the dynamic data element is within the
7 predetermined range.

1 13. The method of claim 12 wherein the dynamic data element is a
2 counter value and wherein the predetermined range is a predetermined counter
3 range.

1 14. A computer readable medium comprising:
2 code for receiving from a portable consumer device, a verification value
3 derived from a dynamic data element;
4 code for determining if the dynamic data element is within a
5 predetermined range; and
6 code for approving a transaction if the dynamic data element is within
7 the predetermined range.

1 15. A server computer comprising the computer readable medium of
2 claim 14.

1 16. A batteryless portable consumer device comprising:
2 a processor;
3 a memory device coupled to the processor, wherein the memory
4 device comprises code for providing a dynamic verification value; and
5 an interface region coupled to the processor, wherein the interface
6 region is configured to receive power from an external source.

1 17. The batteryless portable consumer device of claim 16 wherein
2 the memory device is a magnetic stripe and wherein the batteryless portable
3 consumer device further includes a read-write device.

1 18. The batteryless portable consumer device of claim 17 wherein
2 the interface region is also adapted to transmit account information from the memory
3 device to the external source, and wherein the external source is a card reader.

1 19. The batteryless portable consumer device of claim 16 wherein
2 the interface region comprises an antenna or an electrically conductive contact.

1 20. The batteryless portable consumer device of claim 16 further
2 comprising a display screen coupled to the processor.

1 21. A system comprising:
2 the batteryless portable consumer device of claim 16; and
3 a portable security device configured to interact with the batteryless
4 portable consumer device.

1 22. An authentication method comprising:
2 receiving, at an issuer, an authorization request sent from an access
3 device; and
4 in response to receipt of the authorization request, providing one or
5 more dynamic challenge questions to the consumer before authorizing a transaction
6 conducted by a consumer.

1 23. The authentication method of claim 22 wherein the dynamic
2 challenge questions are generated by the issuer and are related to past transactions
3 conducted by the consumer.

1 24. A computer readable medium comprising:
2 code for receiving, at an issuer, an authorization request sent from an
3 access device at an issuer; and
4 code for providing one or more dynamic challenge questions to the
5 consumer before authorizing a transaction conducted by a consumer.

1 25. A method comprising:
2 providing a secondary PAN associated with a primary PAN using a
3 portable consumer device, wherein the secondary PAN has end portions that are the
4 same as the primary PAN, but has a middle portion of that is different than the
5 primary PAN; and
6 receiving approval for a payment transaction after providing the
7 secondary PAN.

1 26. The method of claim 25 wherein the end portions include a first
2 end portion comprising a BIN number and a second end portion including four digits.

1 27. The method of claim 25 wherein the secondary PAN is stored in
2 a memory device in a portable consumer device, and wherein the primary PAN is
3 generally known to an authentic consumer operating the portable consumer device,
4 but the secondary PAN is not known to the authentic consumer.

1 28. The method of claim 25 wherein the middle portion is dynamic,
2 but the end portions are static.

1 29. A portable consumer device comprising:
2 a memory device comprising code for a secondary PAN associated
3 with a primary PAN, wherein the secondary PAN has end portions that are the same
4 as the primary PAN, but has a middle portion of that is different than the primary
5 PAN.

AUTHENTICATION USING MULTIPLE COMPONENTS

ABSTRACT OF THE DISCLOSURE

Systems and method for improved consumer and portable consumer device authentication are disclosed.

60954584 v1

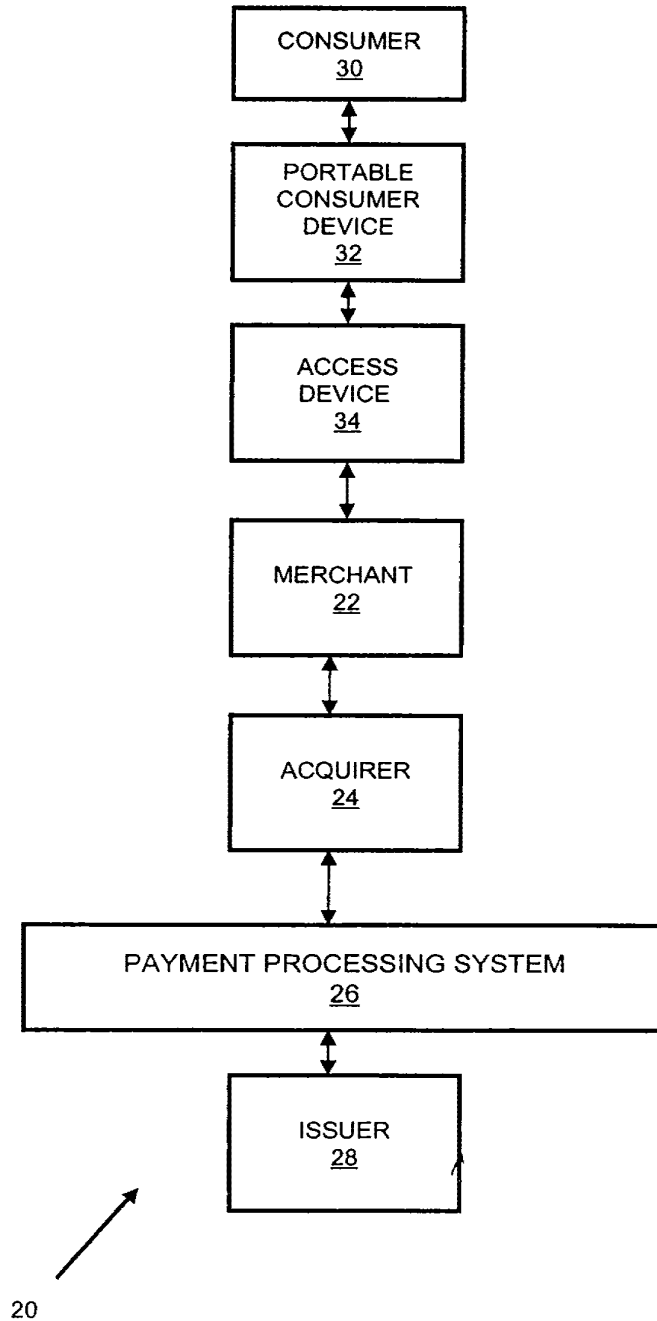


FIG. 1

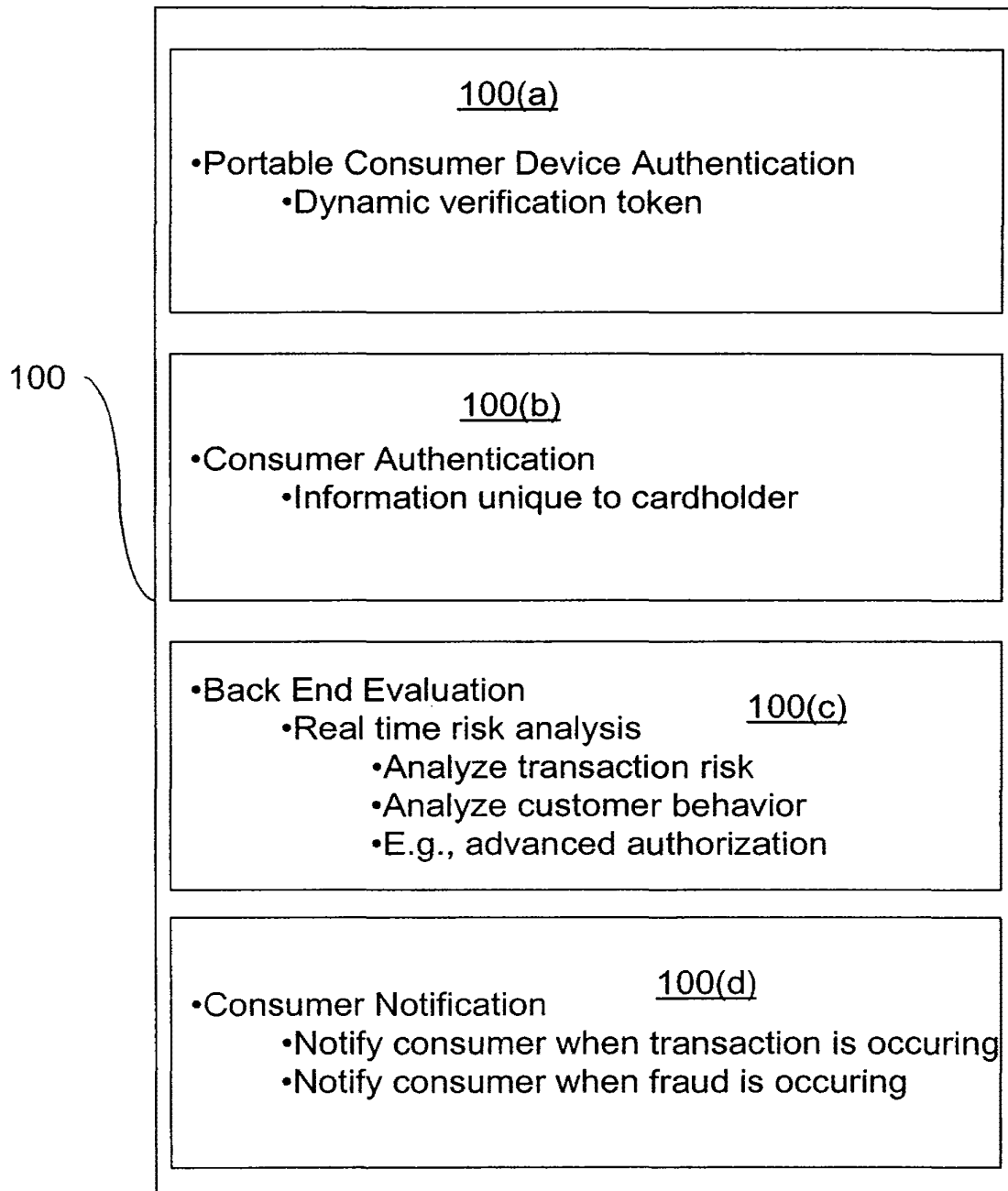
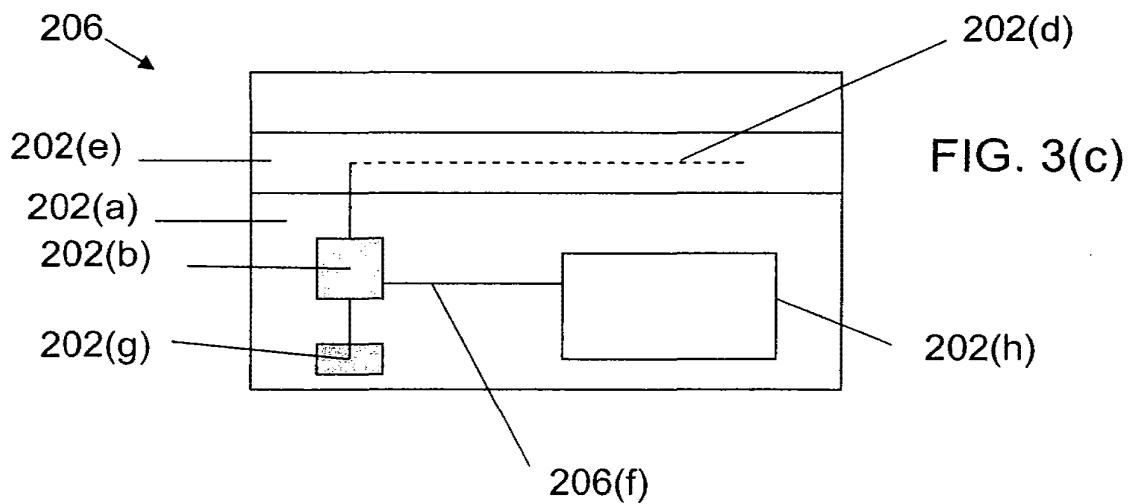
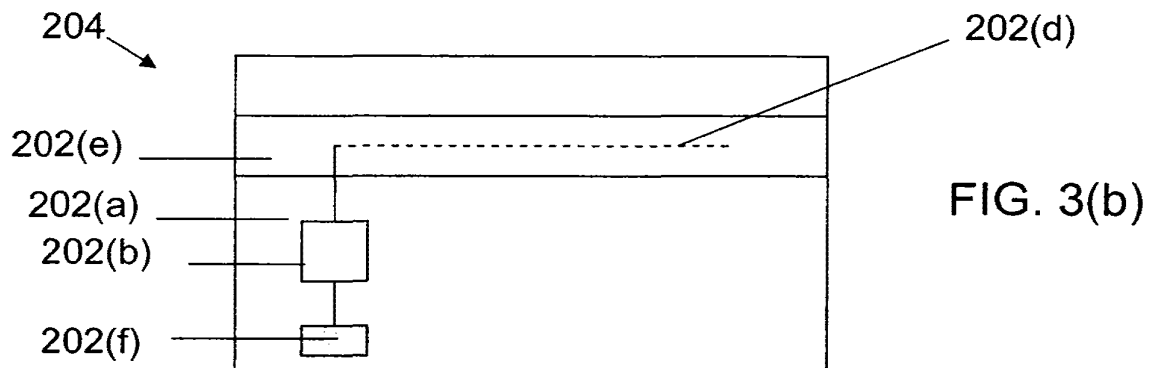
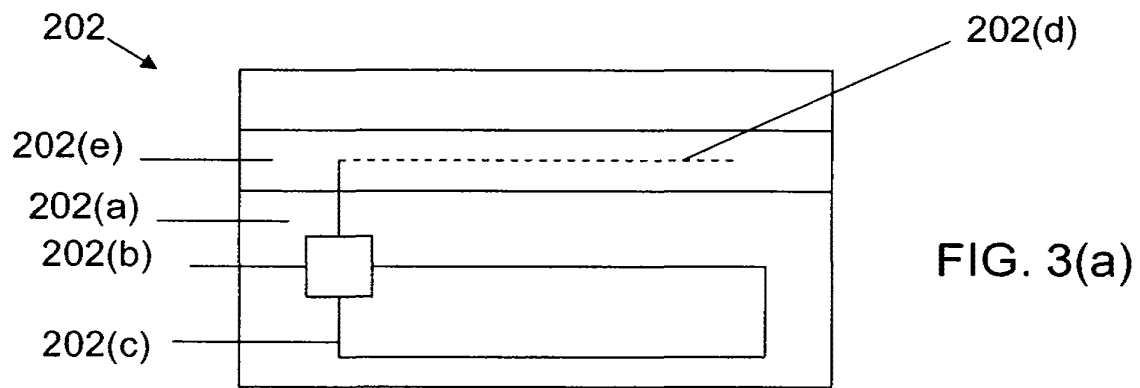


FIG. 2



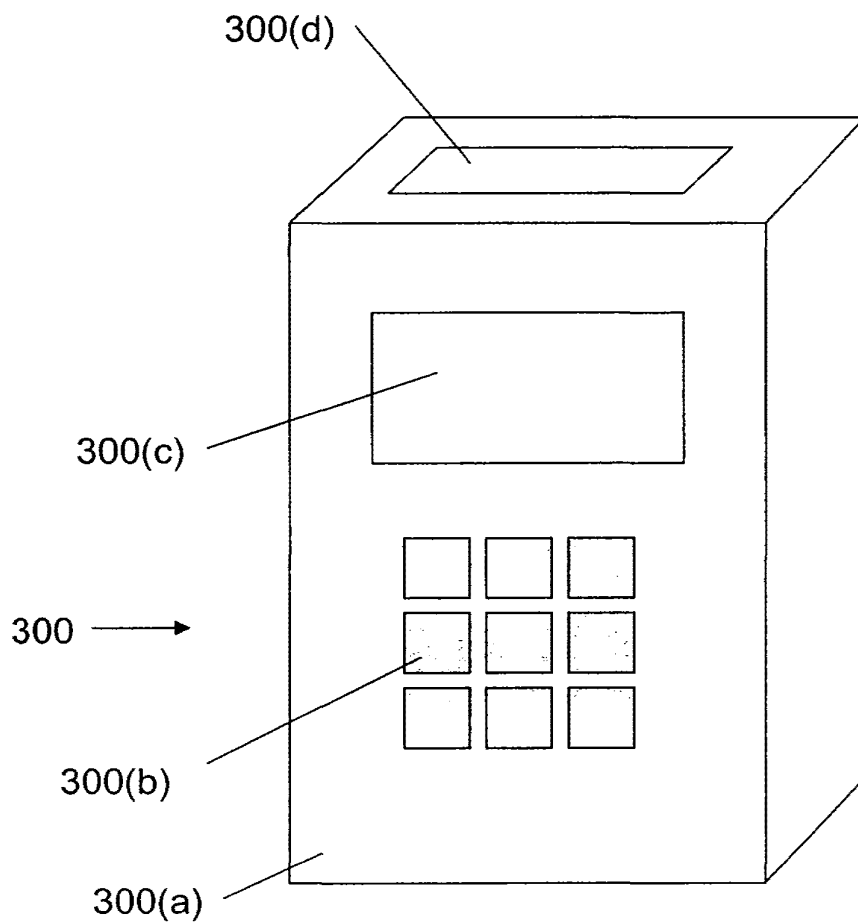


FIG. 4

PAN	EXP DATE	SERV CODE	PIN CVV	DISC DATA
-----	----------	-----------	---------	-----------

FIG. 5

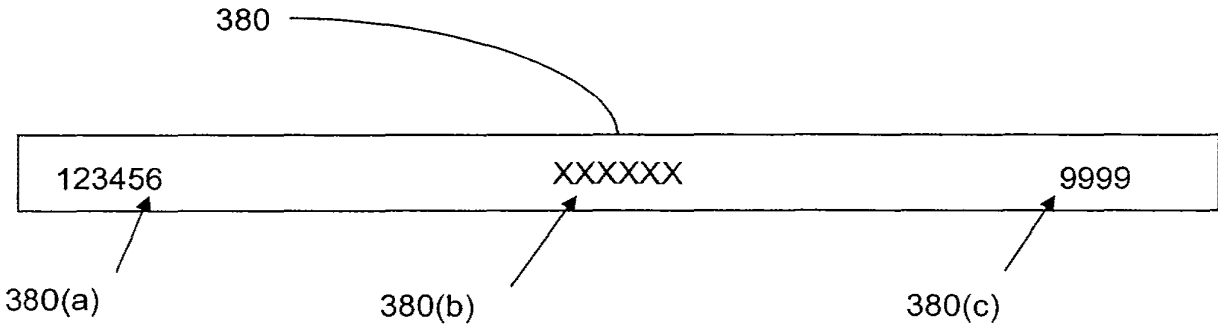


FIG. 6

)

)

APPENDIX



US 20050043997A1

(19) **United States**(12) **Patent Application Publication** (10) Pub. No.: **US 2005/0043997 A1**

Sahota et al.

(43) Pub. Date: **Feb. 24, 2005**(54) **METHOD AND SYSTEM FOR GENERATING A DYNAMIC VERIFICATION VALUE**

(52) U.S. Cl. 705/16

(76) Inventors: Jagdeep Singh Sahota, Rodeo, CA (US); Christian Aabye, Foster City, CA (US)

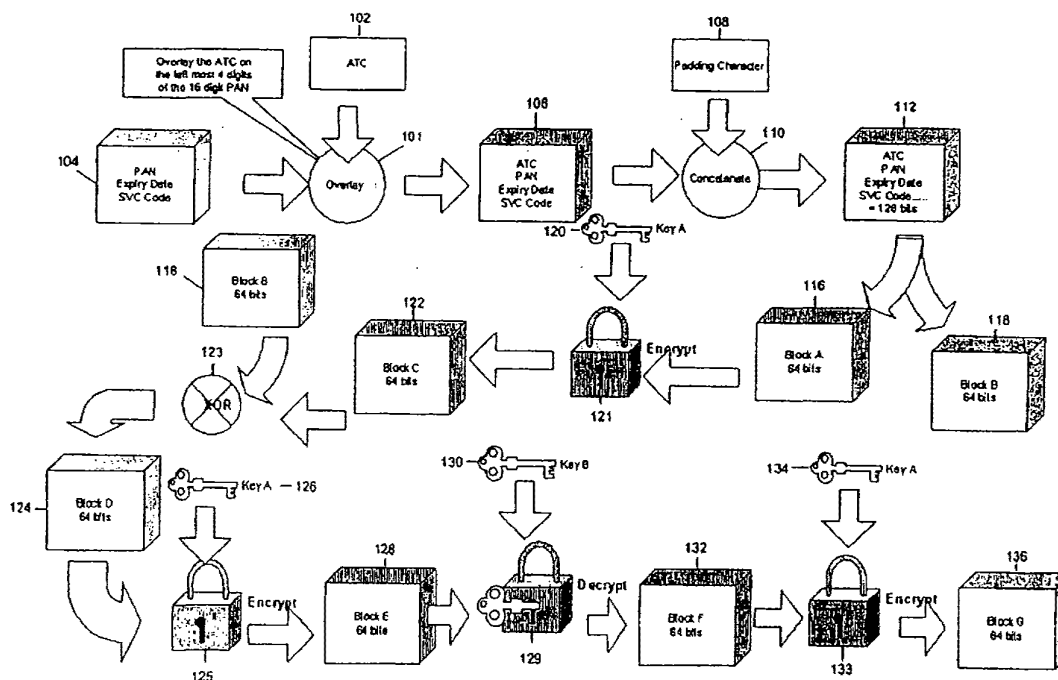
(57) **ABSTRACT**

Correspondence Address:
Pepper Hamilton LLP
50th Floor
One Mellon Center
500 Grant Street,
Pittsburgh, PA 15219 (US)

Methods and systems for dynamically generating a verification value for a transaction and for utilizing such value to verify the authenticity of the payment service application. The dynamically created verification value may be generated on a payment device, such as an integrated circuit credit card or smart card, embedded into the payment data, and transmitted to a point of sale terminal. Alternatively, payment data is sent by a payment device to a point of sale terminal, which generates a verification value and embeds it into the payment data. The embedded verification value is used by a service provider to verify the authenticity of the transaction. The methods and systems may be used in a contactless (wireless) environment or a non-wireless environment.

(21) Appl. No.: 10/642,878

(22) Filed: Aug. 18, 2003

Publication Classification(51) Int. Cl.⁷ G06F 17/60

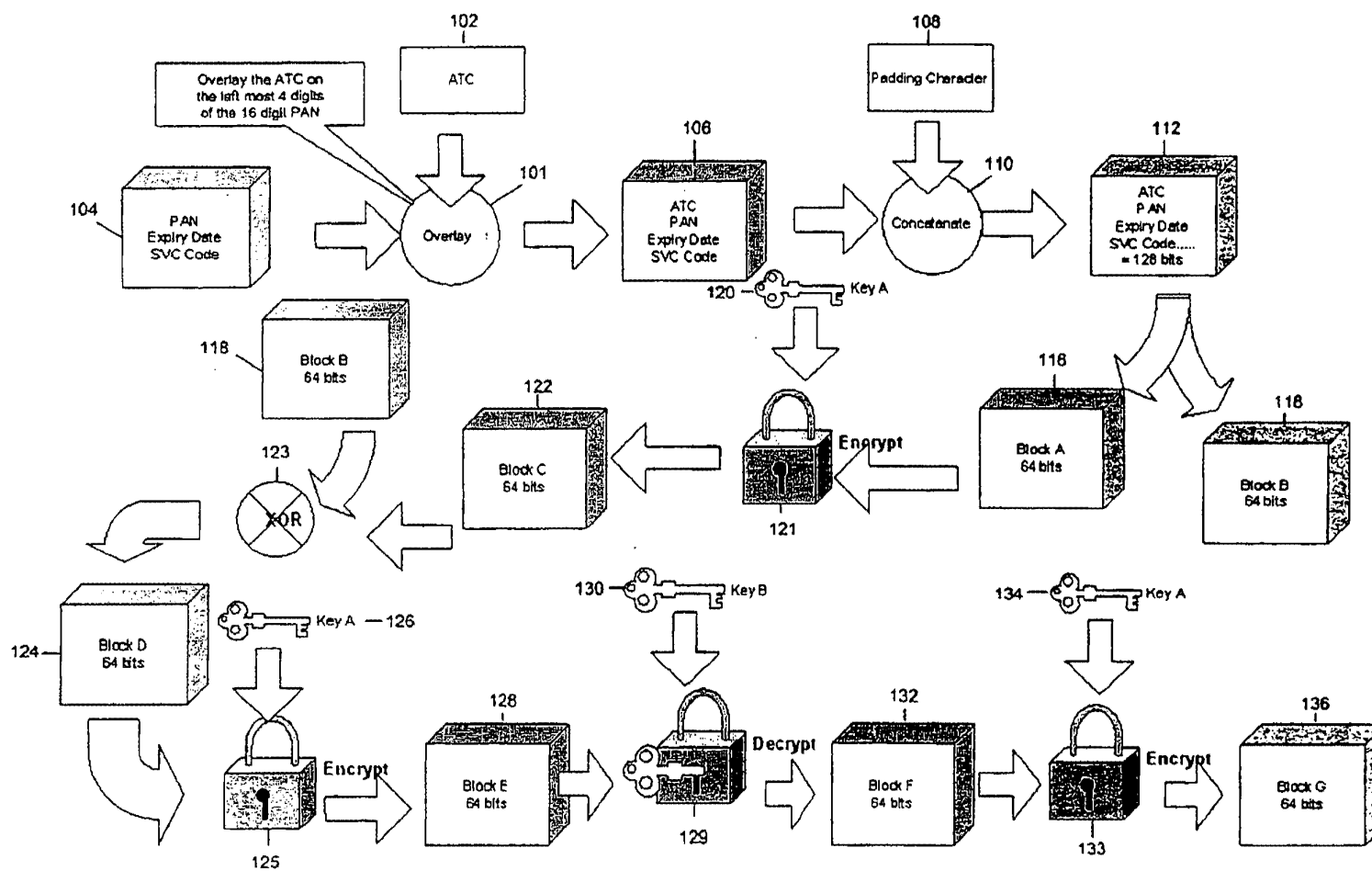


FIG. 1

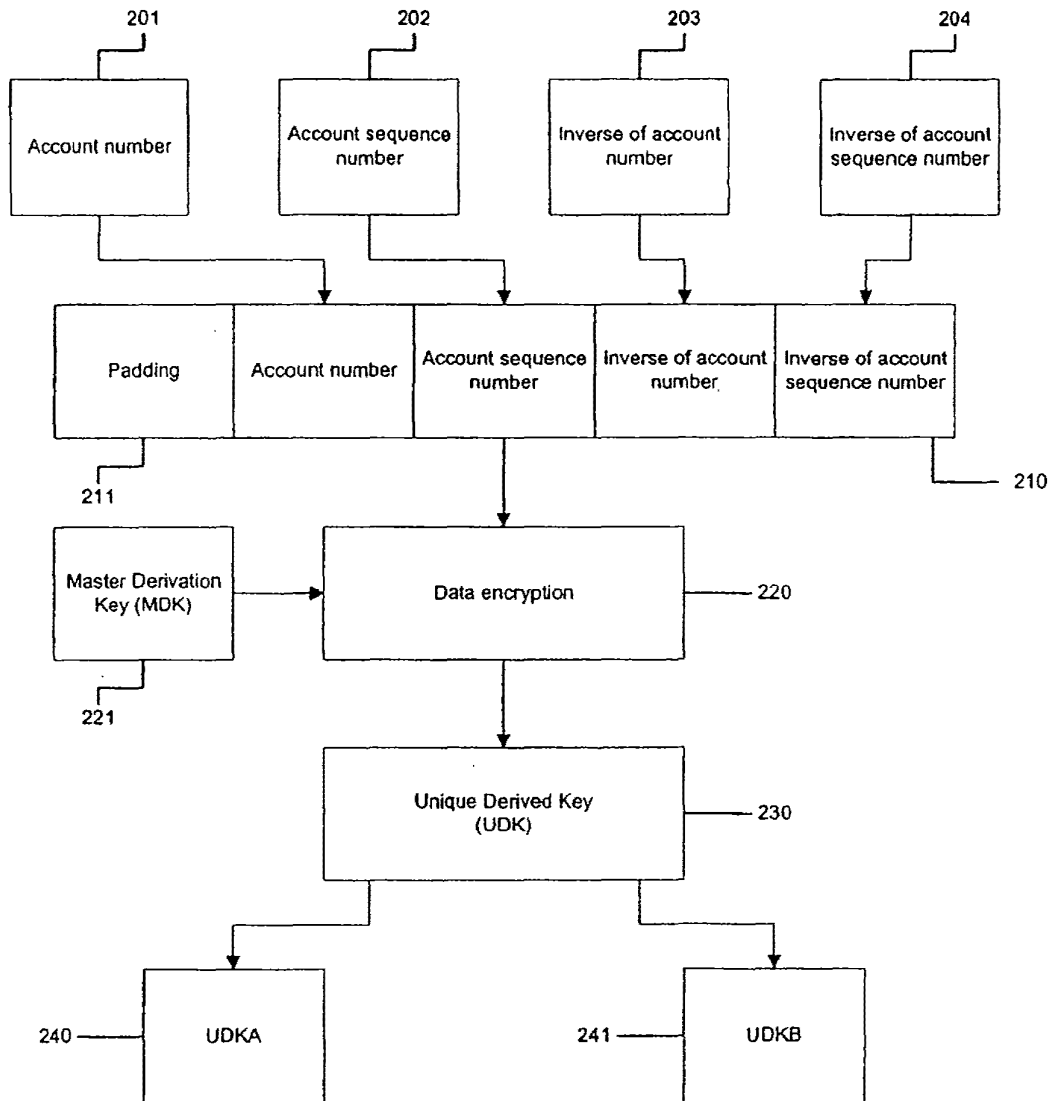


FIG. 2

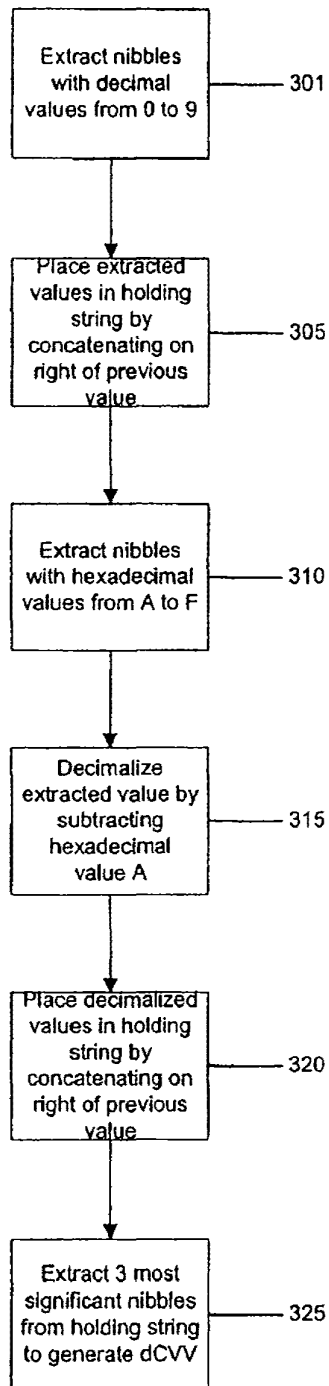


FIG. 3

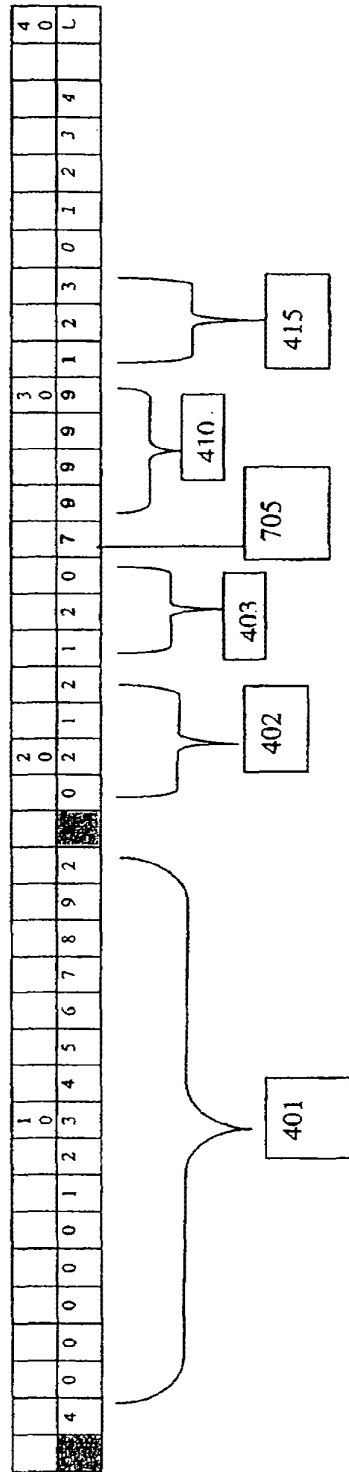


FIG. 4

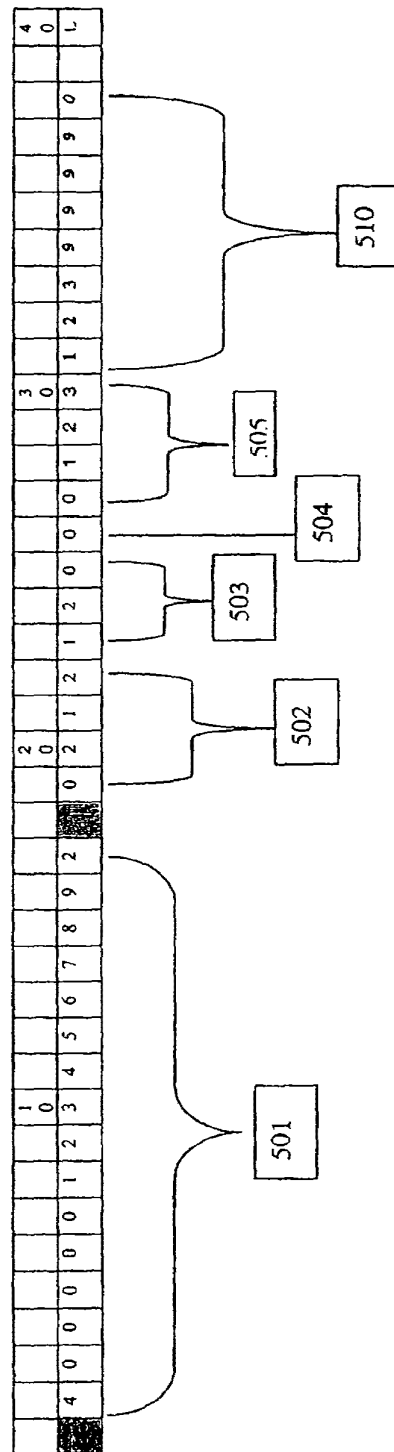


FIG. 5

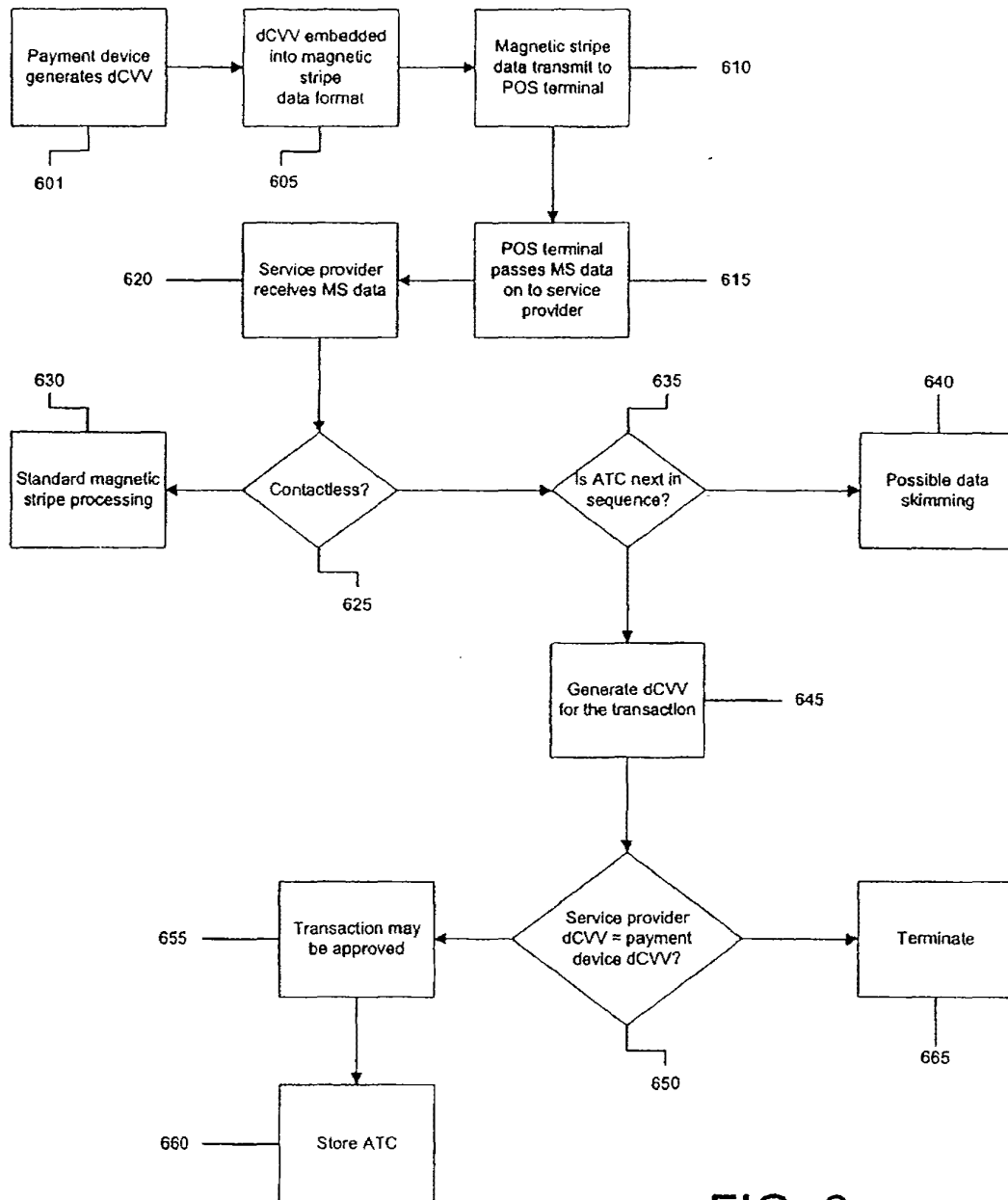


FIG. 6

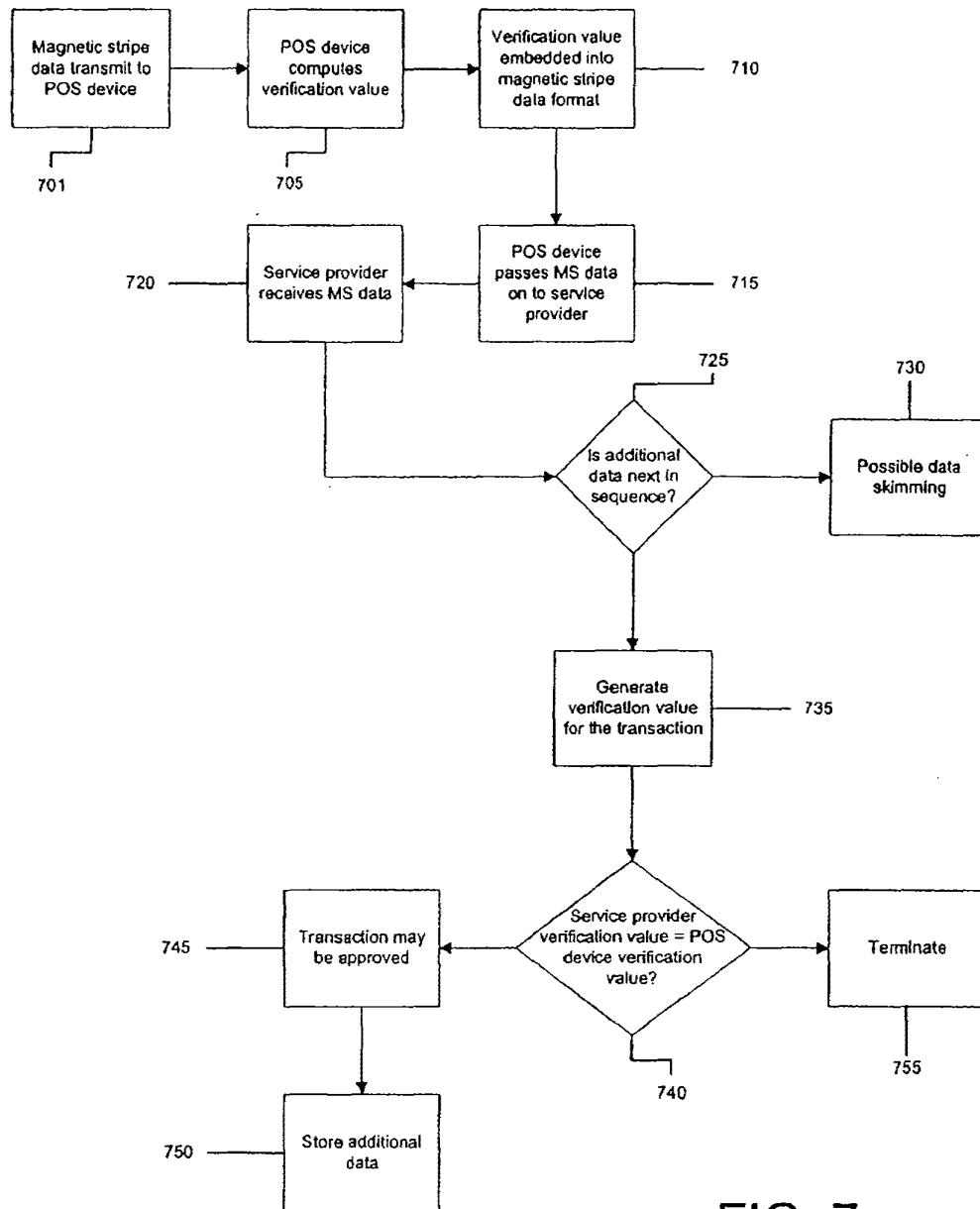


FIG. 7

METHOD AND SYSTEM FOR GENERATING A DYNAMIC VERIFICATION VALUE

BACKGROUND OF THE INVENTION

[0001] As methods and devices for engaging in financial transactions have increased and expanded into new horizons, age old problems such as fraud and counterfeiting persist. In fact, as applications and devices are developed which make credit or debit based transactions a more attractive and readily available alternative to cash, fraud and counterfeiting activities have seen a proportionate increase.

[0002] In order to protect financial institutions, consumers and merchants from the fraudulent use of transaction cards, the industry has developed and introduced many features designed to reduce fraud and counterfeiting such as holograms, special over-layers, and watermarks. Nonetheless, many of these features are proving to be less effective as financial transactions are increasingly being conducted in a wireless environment. Similarly, as financial instruments are increasingly being employed on electronic devices, rather than physical plastic cards, the ability to use techniques such as a customer signature or holograms to verify a party to a transaction is becoming less available.

[0003] One of the primary sources of fraud which is prevalent in the credit card industry is skimming, which refers to the electronic copying of the card's magnetic stripe data to create counterfeit cards. Early skimming was difficult to hide and required cumbersome equipment. As credit card technology has become more sophisticated, so has the technology used by skimmers.

[0004] In addition, new forms of skimming have appeared. For example, in one instance a small bug was implanted in a terminal, and left in place for weeks to collect hundreds of card numbers before being removed to harvest the collective card data. Also, one of the more insidious forms of skimming involved line tapping wherein the communication lines between the terminal and the credit card issuer is tapped and the card data extracted from the communications string. One of the most sophisticated examples of line tapping involved skimmers renting an office next to an issuers regional data center and tapping lines going to the issuer computers. The tapped lines were redirected through a computer on the skimmer's site. Compounding the problem, the skimmers were able to remotely access their computer thus permitting the skimmers to harvest the credit card numbers from a remote location. By some estimates, skimming costs financial institutions hundreds of billions of dollars annually. Furthermore, some industry analysts have estimated that each skimmed card will engage in at least \$2,000 in transactions before the fraud is uncovered.

[0005] Skimming is predominantly a phenomenon afflicting magnetic stripe based transactions. This is because the magnetic stripe, which is placed on the back of a transaction card and stores a variety of data on three separate tracks, is a passive media. In other words, the digital content of the magnetic stripe can be perfectly copied, without any difference between the copy and the original. Largely, this feature is relied upon in legitimate magnetic stripe transactions as a point of sale terminal is simply required to read the data present on the magnetic stripe.

[0006] One of the primary means by which skimming can be prevented is for the consumer to closely monitor the

whereabouts of their transaction card. This will allow the consumer to prevent the card from being swiped through inappropriate devices. However, as magnetic stripe contactless cards evolve and bring the promise of quick transactions to current payment environments, the classic skimming problem comes along with it. In fact, in a wireless environment the opportunity to skim magnetic stripe data is more prevalent. In a wireless environment, a potential skimmer need not physically possess the card to be skimmed nor have access to any of the physical equipment (e.g. POS terminal, communication lines, etc.) which is required for skimming in a wire based environment. A skimmer can simply, and without knowledge of the consumer or merchant, intercept the wireless transaction and copy the data being transmitted from the card to POS terminal.

[0007] Nonetheless, magnetic stripe data and magnetic stripe payment applications are increasingly being deployed on integrated circuit cards or similar devices which have processing capabilities. Accordingly, what is needed is to dynamically generate a verification value for each transaction which can be used to authenticate the transaction. Such an approach to authentication of the payment service will significantly reduce the opportunity for skimming since the verification value is different for each transaction. Therefore, even if the data utilized in a given transaction is skimmed, that data will not be useful in conducting further transactions since the skimmed verification value is not valid for subsequent transactions.

SUMMARY OF THE INVENTION

[0008] The present invention describes a system and method for dynamically generating a verification value for verifying the authenticity of a payment service deployed on a payment device, such as an integrated circuit credit card, each time the payment service is utilized in a transaction. With each transaction, a verification value is dynamically generated on the payment device from data specific to the payment service. The verification value is embedded into the payment data which is transmitted from the payment device to a point of sale terminal such as a credit card terminal. The point of sale terminal transmits the payment data, with the embedded verification data, which may be in the form of magnetic stripe credit card Track 1 and/or Track 2 data, to a payment network which transmits the payment data to a service provider computer. The service provider computer independently generates a verification value. The transaction is disapproved if the service provider generated verification value does not match the payment device generated verification value.

[0009] In an alternate embodiment, payment data generated with each transaction on the payment device is transmitted from the payment device on which the payment data was generated to a point of sale terminal such as a credit card terminal. A verification value may be generated by the point of sale terminal using the payment data and information contained within the point of sale device. The point of sale terminal transmits the payment data, with the verification data, which may be in the form of magnetic stripe credit card Track 1 and/or Track 2 data, to a payment network which transmits the payment data to a service provider computer. The service provider computer independently generates a verification value. The transaction is disapproved if the service provider generated verification value does not match the verification value generated on the point of sale terminal.

[0010] The present invention may be used in any transaction in which magnetic stripe Track 1 and/or Track 2 data will be exchanged over any type of interface including contact-based interfaces and wireless interfaces.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Aspects, features, benefits and advantages of the embodiments of the present invention will be apparent with regard to the following description, appended claims and accompanying drawings where:

[0012] FIG. 1 depicts the method of creating an encrypted data block for use in the present invention.

[0013] FIG. 2 depicts a method for generating unique derived keys from data residing on a payment device.

[0014] FIG. 3 depicts a method for extracting portions of an encrypted data block for creating a dynamic card verification value according to the present invention.

[0015] FIG. 4 depicts an exemplary record format for use in an embodiment of the present invention.

[0016] FIG. 5 depicts an alternative exemplary format for use in an embodiment of the present invention.

[0017] FIG. 6 is a flowchart of a preferred method of utilizing a dynamically created verification value to authenticate a transaction.

[0018] FIG. 7 is a flowchart of an alternate method of utilizing a dynamically created verification value to authenticate a transaction.

DETAILED DESCRIPTION OF THE INVENTION

[0019] Before the present methods are described, it is to be understood that this invention is not limited to the particular methodologies, devices or protocols described, as these may vary. It is also to be understood that the terminology used in the description is for the purpose of describing the particular versions or embodiments only, and is not intended to limit the scope of the present invention which will be limited only by the appended claims. In particular, although the present invention is described in conjunction with financial transactions, it will be appreciated that the present invention may find use in any electronic exchange of data.

[0020] It must also be noted that as used herein and in the appended claims, the singular forms "a", "an", and "the" include plural reference unless the context clearly dictates otherwise. Thus, for example, reference to a "key" is a reference to one or more keys and equivalents thereof known to those skilled in the art, and so forth. Unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art. Although any methods similar or equivalent to those described herein can be used in the practice or testing of embodiments of the present invention, the preferred methods are now described. All publications mentioned herein are incorporated by reference. Nothing herein is to be construed as an admission that the invention is not entitled to antedate such disclosure by virtue of prior invention.

[0021] Generally, the present invention provides methods and systems for dynamically generating a card verification

value for each transaction and for utilizing such value to verify that the payment service is authentic and has not been skimmed. The dynamically generated Card Verification Value (referred to herein as the "dCVV") is generated on the payment device, embedded into the payment data, and transmitted to a point of sale terminal. In an alternate embodiment, payment data is received from a payment device, a verification value is generated by a point of sale terminal, and the verification value is embedded into the payment data.

[0022] In an embodiment, data received by the point of sale terminal is interpreted as simply payment data (e.g. standard magnetic stripe Track 1 and/or Track 2 data without an embedded dCVV) by the point of sale terminal. The point of sale terminal passes on the received data to a payment network which, in turn, passes the data on to the service provider. If the service provider determines the transaction is one for which a dCVV is required, the service provider independently generates a verification value. If the verification value generated by the service provider does not match the dCVV received from the payment device, the transaction is identified as potentially fraudulent and disapproved.

[0023] In an alternate embodiment, data is received by the point of sale terminal and is used by the point of sale terminal to generate a verification value. The point of sale terminal passes on the received data to a payment network which, in turn, passes the data on to the service provider. The service provider independently generates a verification value. If the verification value generated by the service provider does not match the dCVV received from the point of sale terminal, the transaction is identified as potentially fraudulent and disapproved.

[0024] For purposes of this application, the term "payment device" shall mean any device comprising a microprocessor which may be used in a transaction or data exchange as described herein. Without limiting the generality of the foregoing, "payment device" shall include an integrated circuit card (also commonly known as a smartcard), a memory card, a cellular telephone, a personal digital assistant, a mobile electronic device, or a computer.

[0025] For purposes of this application, "contactless" or "wireless" shall mean any communications method or protocol, including proprietary protocols, in which data is exchanged between two devices without the need for the devices to be physically coupled. Without limiting the generality of the foregoing, "contactless" or "wireless" shall include data transmissions by laser, radio frequency, infrared communications, Bluetooth, or wireless local area network.

[0026] For purposes of this application, the term "payment service" shall mean any application deployed on a payment device which causes the exchange of data between the payment device and any other device or location. It should be appreciated that "payment service" is not limited to financial applications.

[0027] For purposes of this application, "payment data" shall mean, with respect to financial applications those data elements used by the payment service to execute a transaction, and with respect to non-financial transactions any necessary data elements exclusive of the present invention. For example, when the payment service is a magnetic stripe

credit card transaction, "payment data" would comprise Track 1 and/or Track 2 data, as that is understood by one of ordinary skill in the credit card industry, such as the primary account number, expiration date, service codes, and discretionary data. "Payment data" may also comprise a unique card identification number or a unique identification number for a service provider.

[0028] In an embodiment, the payment data will reside on memory located on the payment device. The payment device will also maintain an application transaction counter (ATC). The ATC will initially be set by the service provider to a predetermined value. Thereafter, the ATC will be incremented with each transaction. Alternately, the ATC may be decremented from its initial predetermined value with each transaction. The ATC may be a value of any length. In addition, the service provider which deployed the payment service will maintain a corresponding ATC accessible to the service provider's computer. As discussed in more detail below, this corresponding ATC is used to identify payment services which may have been skimmed. In an alternate embodiment, a cryptogram, digital signature, or hash value based on transaction data may be used in place of or in conjunction with the ATC.

[0029] Each time the payment service is initiated, a dCVV is generated on the payment device for authentication purposes. FIG. 1 depicts the method of generating a dCVV for each transaction according to the present invention. Initially, a numeric string of predetermined length is created. This numeric string is created by overlaying 101 the ATC 102 over the corresponding leftmost digits of the account number for the payment service or PAN 104. This numeric string is concatenated on the right with the expiration date for the payment service and the service code to produce a concatenated value 106. If necessary, padding characters 108 are concatenated 110 on the right of the concatenated value 106 to form a numeric string 112 with a predetermined fixed length. In a preferred embodiment, this numeric string 112 is 128-bits in length, although a numeric string of any length may be used. The padding characters 108 may consist of a stream of 0's, 1's, or any other numeric value that is known both to the payment device and the service provider. The numeric string 112 is bisected into two blocks of equal length, Block A 116 and Block B 118. Block A 116 is then encrypted 121 with a first encryption key 120. The result of the encryption step 121 is Block C 122 of length equal to Block A 116. Block C 122 is then exclusively OR'ed (XOR) 123 with Block B 118 resulting in Block D 124. Block D 124 is then encrypted 125 with a second encryption key 126 to produce Block E 128. Block E 128 is then decrypted 129 using a decryption key 130 to produce Block F 132. Block F 132 is then encrypted 133 using a fourth encryption key 134 to produce Block G 136.

[0030] It will be apparent to one of ordinary skill in the art that the first encryption key 120, the second encryption key 126, the third encryption key 130 and the fourth encryption key 134 may take any preselected value. In an embodiment of the present invention, the first encryption key 120, the second encryption key 126, and the fourth encryption key 134 are equivalent and of a different value from the third encryption key 130. Other permutations of the encryption key values utilized in the methodology of FIG. 1 are within the scope of the present invention.

[0031] In a preferred embodiment, the first encryption key 120, the second encryption key 126, the third encryption key 130, and the fourth encryption key 134 take the value of unique keys derived from data existing on the payment device. Upon deployment, each payment service is personalized by the service provider with a master derivation key. The master derived key may be deployed with payment services in batches (i.e. multiple payment services receive the same master derived key) or individually. Each payment device will be personalized with the functionality to derive keys unique to the payment service. FIG. 2 shows the methodology for deriving two unique keys which are utilized in the preferred embodiment. The account number 201, the account sequence number 202, the inverse of the account number 203, and the inverse of the account sequence number 204 are concatenated together to create a concatenated value 210. If necessary, the concatenated value 210 may be padded with zeroes, or some other value 211, to create a string of a predetermined fixed length. In a preferred embodiment, the concatenated value 210 may be 128 bits in length, although the concatenated value is not limited to being this length. The concatenated value 210 is then encrypted 220 using the master derivation key 221 as the encryption key for each encryption stage. The encryption utilized may include any type of encryption methodology. For example, this encryption step may utilize Triple-DES encryption. The value resulting from the encryption step 220 is a unique derived key or UDK 230 for the application identified by the account number. Two additional keys, UDKA 240 and UDKB 241, are derived from the UDK. The derivation of UDKA 240 and UDKB 241 from the UDK 230 may take any form, including assigning the value of the leftmost half of the UDK 230 to UDKA 240, and assigning the value of the rightmost half of the UDK 230 to UDKB 241. Alternatively, the UDKA 240 may be derived by selecting alternating or other predetermined bit sequences from the UDK 230 while the remaining bits are assigned to UDKB 241. Furthermore, there is no requirement that UDKA 240 and UDKB 241 are of equal length.

[0032] Returning now to the result of the methodology set forth in FIG. 1. FIG. 3 describes the further processing required to generate the dCVV. Each nibble (4-bit grouping) of the value stored in Block G 136 is subjected to two separate iterative processes to evaluate the value of each nibble. As shown in FIG. 3, beginning with the most significant (i.e. left most) digit of Block G 136 and examining each sequential nibble, if a nibble contains a value ranging from zero to nine, inclusive, that value is extracted 301 and placed in a new numeric string 305, referred to herein as a holding string, by concatenating the extracted value to the right of the previously extracted value, if any. The result will be that the holding string contains a series of values ranging from zero to nine, inclusive, which appear from left to right in the holding string in the same sequence in which they appear in Block G 136.

[0033] A second evaluation is then performed again beginning with the most significant digit of Block G 136 and examining each sequential nibble. If a nibble contains a hexadecimal value ranging from ten (A) to fifteen (F), inclusive, that value is extracted 310. The extracted value is then decimalized by subtracting the hexadecimal value A from the extracted value resulting in a decimalized value

ranging from zero to five 315. This decimalized value is then concatenated on the right to the right most value of the holding string 320.

[0034] Once all nibbles in Block G have been twice examined as described, the three most-significant (i.e. left-most) nibbles of the holding string are extracted 325. This 3-digit value is the dCVV for the transaction. Other numbers of bits may be extracted from the twice-examined nibble string to generate the dCVV for a transaction. Furthermore, different nibbles, such as the rightmost nibbles, may be used as the dCVV for a transaction. The three leftmost nibbles, however, represent a preferred embodiment.

[0035] Once generated, the dCVV is embedded into the payment data transmitted from the payment device to the point of sale terminal. The data received by the point of sale terminal will appear to the point of sale terminal as standard payment data. In other words, the point of sale terminal will not be able to determine if a dCVV is embedded and where such dCVV may be located. There is no indication to the point of sale terminal that a dCVV is embedded into the data received from the payment device.

[0036] FIG. 4 depicts an exemplary record format for transmitting payment data, with the dCVV embedded therein, from the payment device to the point of sale terminal. The record format of FIG. 4 is created by concatenating a primary account number 401 for the payment service, with an expiration date 402, and a service code 403. In a preferred embodiment, the primary account number 401 is 16 digits long, the expiration date 402 is four digits long, and the service code 403 is three digits long. However, the primary account number 401, the expiration date 402, and the service code 403 are not limited to being these lengths. Next, in a field typically reserved for other uses, a value is placed as an indicator 405 that a dCVV has been embedded in this record. The value of this indicator is known by the service provider which deployed the application on the payment device. Next, the ATC 410 is placed in the field which may typically be reserved for PIN verification data. Finally, the dCVV 415 is concatenated on the right of the record. The remainder of the record may comprise additional discretionary data.

[0037] Alternately, FIG. 5 depicts a second exemplary format for transmitting payment information with the dCVV embedded thereon from the payment device to the point of sale terminal. The format in FIG. 5 is created by concatenating a primary account number 501 for the payment service, with an expiration date 502, a service code 503, a PVKI 504, and a field for PIN verification data 505. In a preferred embodiment, the primary account number 501 is sixteen digits long, the expiration date 502 is four digits long, the service code 503 is three digits long, the PVKI 504 is one digit long, and the PIN verification data 505 is four digits long. However, the primary account number 501, the expiration date 502, the service code 503, the PVKI 504, and the PIN verification data 505 are not limited to being these lengths. Next, in a single data field 510 each of the dynamically created CVV, the ATC and the indicator to be used by the service provider to identify that a dynamic CVV has been embedded are stored in sequence. The remainder of the record may comprise additional discretionary data.

[0038] An important aspect of the present invention is that the system of utilizing the dynamically created CVV allows

the service provider to make a determination of the authenticity of the payment service being utilized. This authentication step is not left to merchants, individual point of sale terminals, or other third parties or devices. FIG. 6 shows how the dCVV is used in a contactless environment to permit the service provider to evaluate the authenticity of the payment application deployed on the payment device to make a determination of whether the payment application has been skimmed. Although shown in the embodiment of a contactless environment in FIG. 6, the present invention is not limited to such an environment and may be used for any transaction where magnetic stripe Track 1 and/or Track 2 data is exchanged using any method or means for communicating such data. As shown in FIG. 6, the payment device generates the dCVV 601, preferably using the methodology described above. The dCVV is embedded into the payment data 605. In this respect, the exemplary record formats shown in FIG. 4 or FIG. 5 may be utilized. The payment data with the embedded dCVV is transmitted by data communication to the point of sale terminal 610. The point of sale terminal recognizes the received data as in the standard format of payment data and passes the data stream on to the service provider computer 615, likely via a payment network (not shown). The service provider computer receives 620 the payment data with the embedded dCVV and interrogates the appropriate indicator to determine if the transaction was a contactless transaction or not 625. If the service provider computer determines that the transaction was not a contactless transaction, the transaction is processed in its normal manner 630. If the service provider computer determines that the transaction was contactless, the service provider computer compares the ATC received from the payment device to the corresponding ATC stored on the service provider computer to determine if the received ATC is the expected next ATC 635. If the ATC received from the payment device is not the expected next ATC, the payment service deployed on the payment device has potentially been skimmed 640. If the expected next ATC is received, the service provider computer will independently re-generate the dCVV for the given transaction 645 utilizing the same process as described above. If the service provider generated dCVV matches the dCVV received from the payment device 650, the service provider deems the payment application to be authentic 655. The service provider computer then replaces the ATC which was previously stored on the service provider computer with the ATC received from the payment device 660 for subsequent authentications. If the service provider generated dCVV does not match the dCVV received from the payment device, the transaction is potentially fraudulent and is terminated 665.

[0039] The methodology of FIG. 6 discussed in conjunction with contactless transactions, is not limited thereto. For example, the methodology may be utilized with respect to transactions above a certain threshold value. In such an instance, the service provider, upon deploying the application, would configure the application to generate a dCVV for transactions above the threshold. The indicator interrogated in Step 625 would then be set for transactions above the threshold value. Similarly, the methodology may be utilized with respect to any other transaction criteria including, but not limited to, geographic location, use patterns, or any other criteria.

[0040] In an alternate embodiment, the payment device transmits payment data to a point of sale terminal such as a

credit card terminal 701. The point of sale terminal receives the data and computes a verification value for the transaction 705. The verification value may be computed in a number of different ways including, without limitation, using a unique transaction number provided by the point of sale terminal, a timestamp, or a transaction amount added to a timestamp. The point of sale terminal may then embed and/or append the verification value and additional data to the payment data 710. The additional data may be required for the service provider computer to verify the transaction. The point of sale terminal then passes the data stream on to the service provider computer 715, likely via a payment network (not shown). The service provider computer receives the payment data with the verification value 720. The service provider computer may optionally compare at least a portion of the additional data embedded or appended by the point of sale terminal to corresponding data stored on the service provider computer to determine if the received data is proper 725. If the received data from the point of sale terminal is improper, the transaction data may potentially have been skimmed 730. If proper data is received, the service provider computer will independently re-generate the verification value for the given transaction utilizing the same process as used by the point of sale terminal 735. If the service provider generated verification value matches the verification value received from the point of sale terminal 740, the service provider deems the payment application to be authentic 745. The service provider computer may then optionally update the additional data which was previously stored on the service provider computer with the additional data received from the payment device for subsequent authentications 750. If the service provider generated verification value does not match the verification value received from the point of sale terminal, the transaction is potentially fraudulent and is terminated 755.

[0041] The foregoing is considered as illustrative only of the principles of the invention. Further, since numerous modifications and changes will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation shown and described, and accordingly, all suitable modifications and equivalents may be resorted to, falling within the scope of the invention.

What is claimed is:

1. A method for authenticating a payment service being used in a transaction comprising:

generating on a payment device a first verification value unique to the transaction wherein said first verification value is derived from data comprising a first data value and a second data value;

communicating a payment record from the payment device to a point of sale terminal, wherein the payment record comprising the first verification value and payment data;

communicating the payment record from the point of sale terminal to a service provider computer;

generating a second verification value on the service provider computer, wherein the second verification value is generated solely from data residing on the service provider computer; and

disapproving the transaction when the first verification value does not equal the second verification value.

2. The method of claim 1 wherein said first data value comprises:

a primary account number for the payment service.

3. The method of claim 1 wherein said first data value comprises:

a unique identification number for the payment device.

4. The method of claim 1 wherein said first data value comprises:

a unique identification number for the service provider.

5. The method of claim 1 wherein said second data value comprises:

an application transaction counter.

6. The method of claim 1 wherein said second data value comprises:

a cryptogram.

7. The method of claim 1 wherein said second data value comprises:

a digital signature.

8. The method of claim 1 wherein said second data value comprises:

a value derived from the payment data.

9. The method of claim 1 wherein said first verification value is derived from data further comprising:

a service code which identifies the payment service; and

an expiration date for the payment service.

10. The method of claim 1 wherein the application transaction counter is incremented with any non-zero value with each executed transaction.

11. The method of claim 1 wherein the payment record further comprises an application transaction counter.

12. The method of claim 11 further comprising:

storing the application transaction counter in memory accessible by the service provider computer.

13. The method of claim 1 wherein the payment device communicates the payment record to the point of sale terminal via wireless communications.

14. A method of dynamically creating a verification value for a transaction comprising:

creating a base record comprising a first data value and a second data value for a payment service being used in the transaction;

splitting the base record into a first field and a second field;

encrypting the first field using a first encryption key;

performing an exclusive-OR (XOR) operation on the encrypted first field and the second field to produce a first result;

encrypting the first result using a second encryption key to produce a second result;

decrypting the second result using a decryption key to produce a third result;

encrypting the third result using a third encryption key to produce a fourth result;

sequentially extracting each value between 0 and 9 from the most-significant digit to the least-significant digit of the fourth result to produce a fifth result;

sequentially extracting and subtracting hexadecimal A from each value between hexadecimal A and hexadecimal F from the most-significant digit to the least-significant digit of the fourth result to produce the sixth result;

concatenating the fifth result and the sixth result to produce a seventh result; and

selecting one or more values from the seventh result as the card verification value.

15. The method of claim 14 wherein the first encryption key, the second encryption key, and the third encryption key are equivalent.

16. The method of claim 14 wherein the decryption key differs from the first encryption key.

17. The method of claim 14 wherein the decryption key differs from each of the first encryption key, the second encryption key, and the third encryption key.

18. The method of claim 14 wherein the base record is 128-bits in length.

19. The method of claim 14 wherein said first data value comprises:

a primary account number for the payment service.

20. The method of claim 14 wherein said first data value comprises:

a unique identification number for the payment device.

21. The method of claim 14 wherein said first data value comprises:

a unique identification number for the service provider.

22. The method of claim 14 wherein said second data value comprises:

an application transaction counter.

23. The method of claim 14 wherein said second data value comprises:

a cryptogram.

24. The method of claim 14 wherein said second data value comprises:

a digital signature.

25. The method of claim 14 wherein said second data value comprises:

a value derived from the payment data.

26. The method of claim 14 wherein said first verification value is derived from data further comprising:

a service code which identifies the payment service; and

an expiration date for the payment service.

27. The method of claim 14 wherein the base record further comprises padding characters to extend the base record to a predetermined length.

28. The method of claim 14 wherein the first encryption key, the second encryption key, the decryption key, and the third encryption key are derived from data residing on the payment device.

29. A system for verifying a transaction comprising:

a first electronic device with a payment service deployed thereon;

a second electronic device in communication with the first electronic device wherein the second electronic device receives a payment record from the first electronic device, the payment record comprising an account number for the payment service and a first verification value generated on the first electronic device;

a service provider system in communication with the second electronic device wherein the service provider computer independently generates a second verification value and disapproves the transaction where the first verification value and the second verification value are not equal.

30. The system of claim 29 wherein the first electronic device is an integrated circuit card.

31. The system of claim 29 wherein the first electronic device is a personal digital assistant.

32. The system of claim 29 wherein the first electronic device is a cell phone.

33. The system of claim 29 wherein the first electronic device is a device comprising:

a microprocessor; and

means for communicating with the second electronic device.

34. The system of claim 29 wherein the first electronic device communicates with the second electronic device via radio frequency waves.

35. The system of claim 29 wherein the electronic device communicates with the second electronic device via infrared frequency waves.

36. The system of claim 29 wherein the electronic device communicates with the second electronic device via laser communication.

37. The system of claim 29 wherein the second electronic device is comprised of:

means for communicating with the first electronic device; and

a terminal.

38. The system of claim 37 wherein the second electronic device is further comprised of a hardware security key.

* * * * *

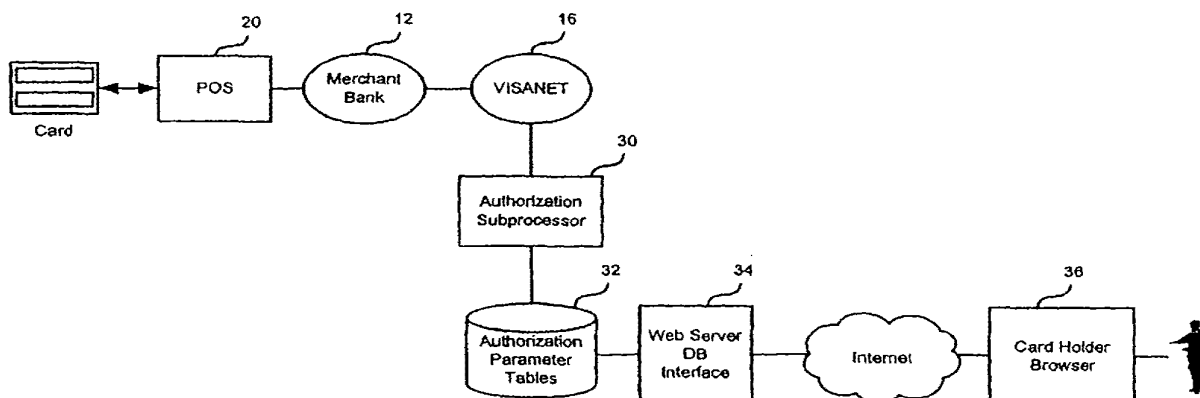


US 20030172040A1

(19) **United States**(12) **Patent Application Publication**
Kemper et al.(10) **Pub. No.: US 2003/0172040 A1**(43) **Pub. Date: Sep. 11, 2003**(54) **SYSTEM FOR PERSONAL AUTHORIZATION
CONTROL FOR CARD TRANSACTIONS****Publication Classification**(51) **Int. Cl.⁷** **G06F 17/60; H04K 1/00;****H04L 9/00**(52) **U.S. Cl.** **705/75**(75) **Inventors:** **Lynn Kemper**, San Carlos, CA (US);
Akshey Shawn Vij, Mountain View,
CA (US); **Robin O'Connell**, San
Francisco, CA (US)(57) **ABSTRACT**

An authorization system allows for cardholder-provided parameters to a personal authorization subsystem. The parameters can be selected by the cardholder to limit the authorizations that would otherwise be granted on the card. The parameters can indicate limits by frequency, dollar amount, merchant, geographic location, time of day, combinations thereof, or the like. Authorization for a given transaction, even where authorized by an issuer and a network operator, might be denied based on self-constraints set by the cardholder. In some variations, messages are sent to the cardholder based on constraints set by the cardholder and transactions might be approved and messaged, or denied and messaged.

Correspondence Address:

**TOWNSEND AND TOWNSEND AND CREW,
LLP****TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)**(73) **Assignee:** **Visa U.S.A.**, San Mateo, CA(21) **Appl. No.:** **10/093,002**(22) **Filed:** **Mar. 5, 2002**

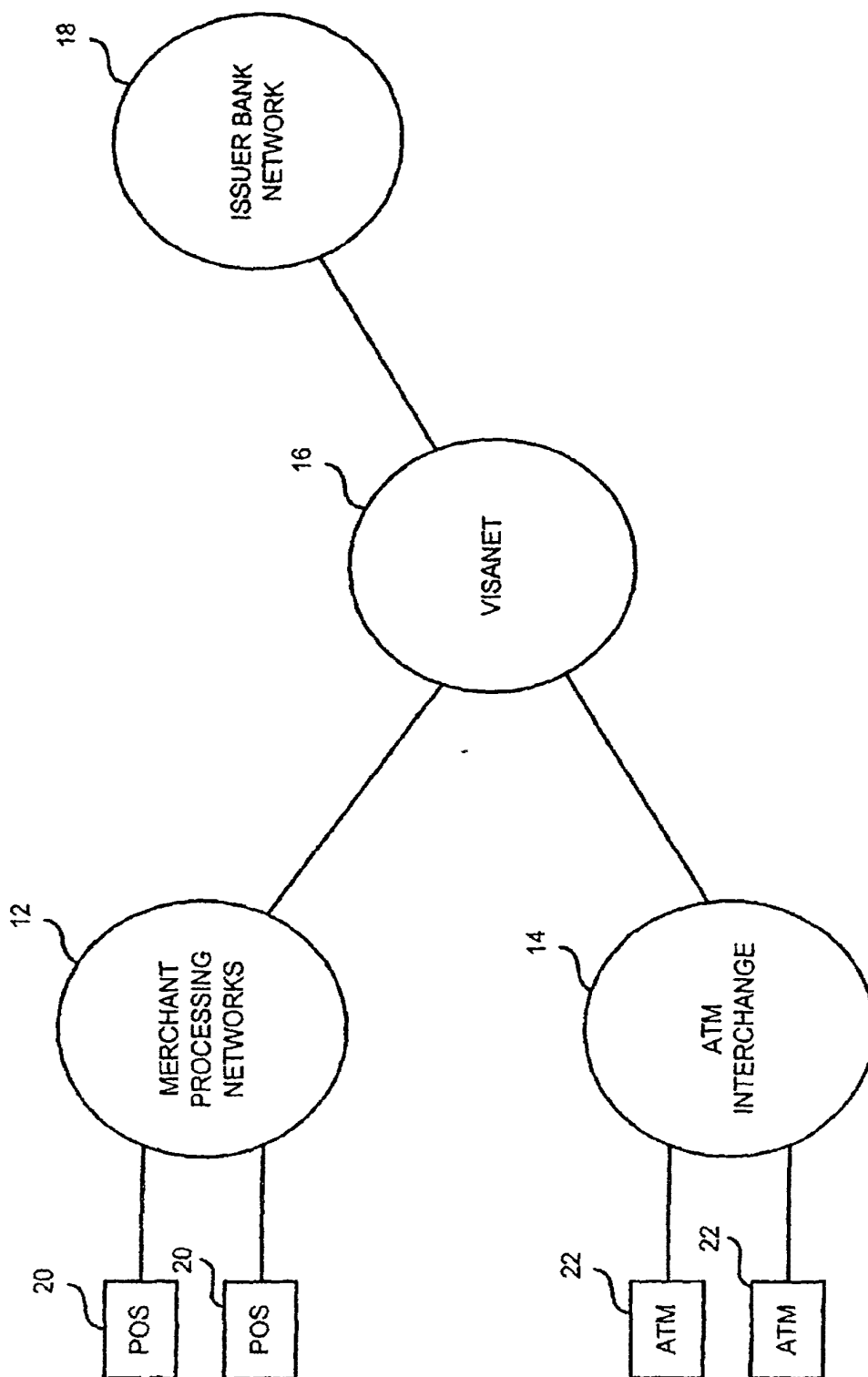


Fig. 1

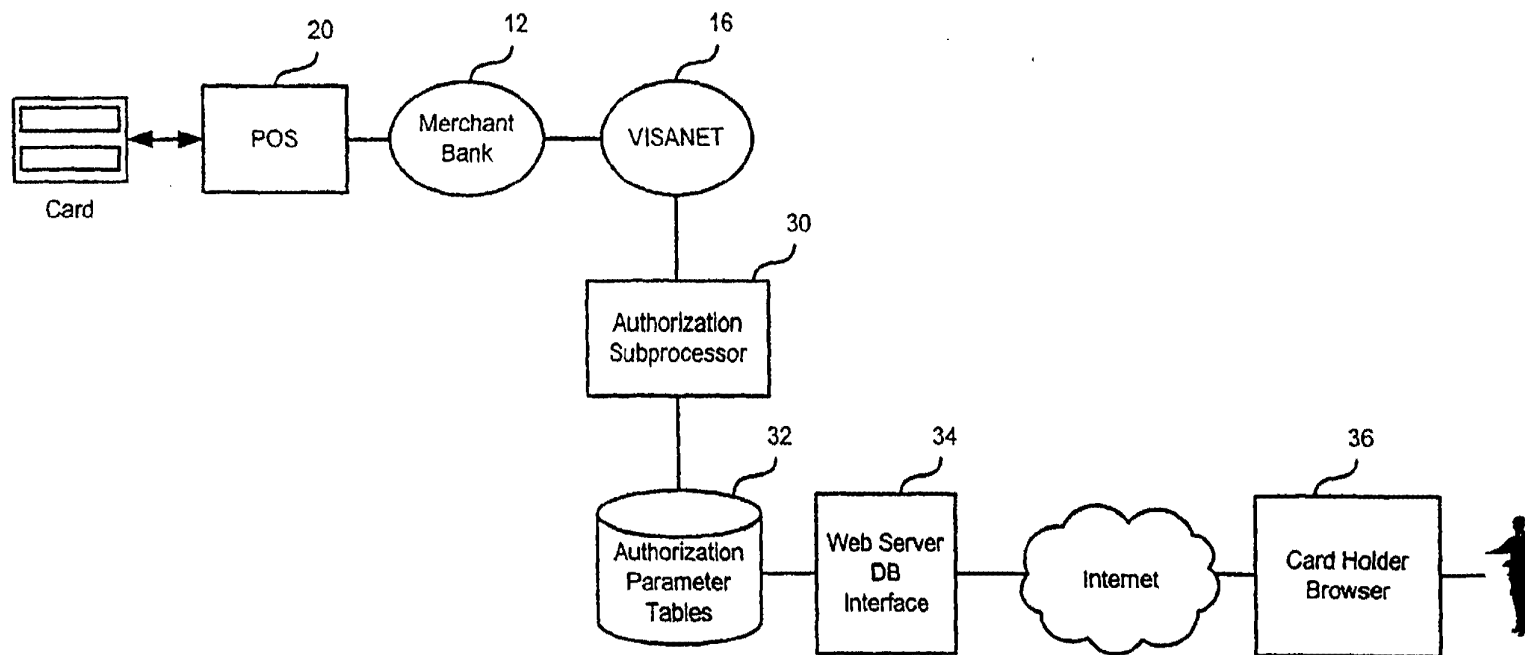


Fig. 2

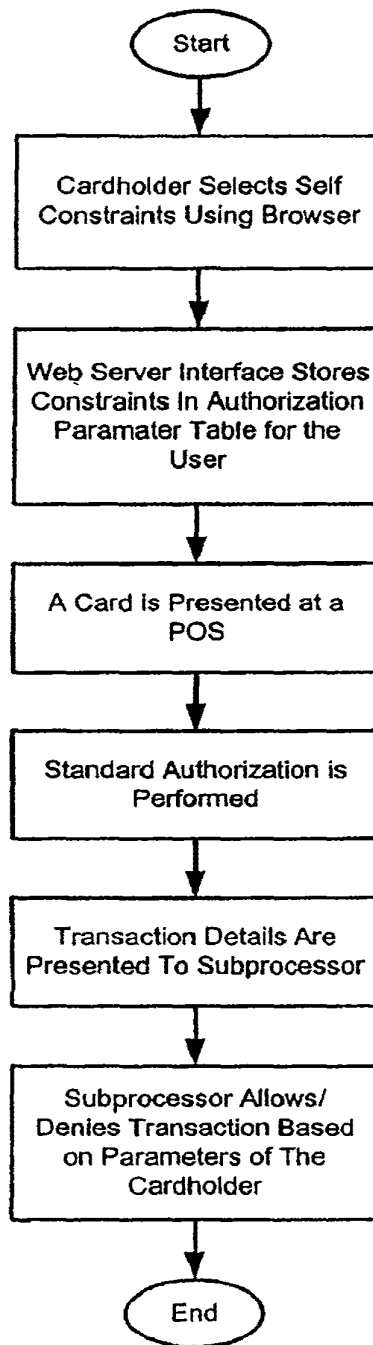
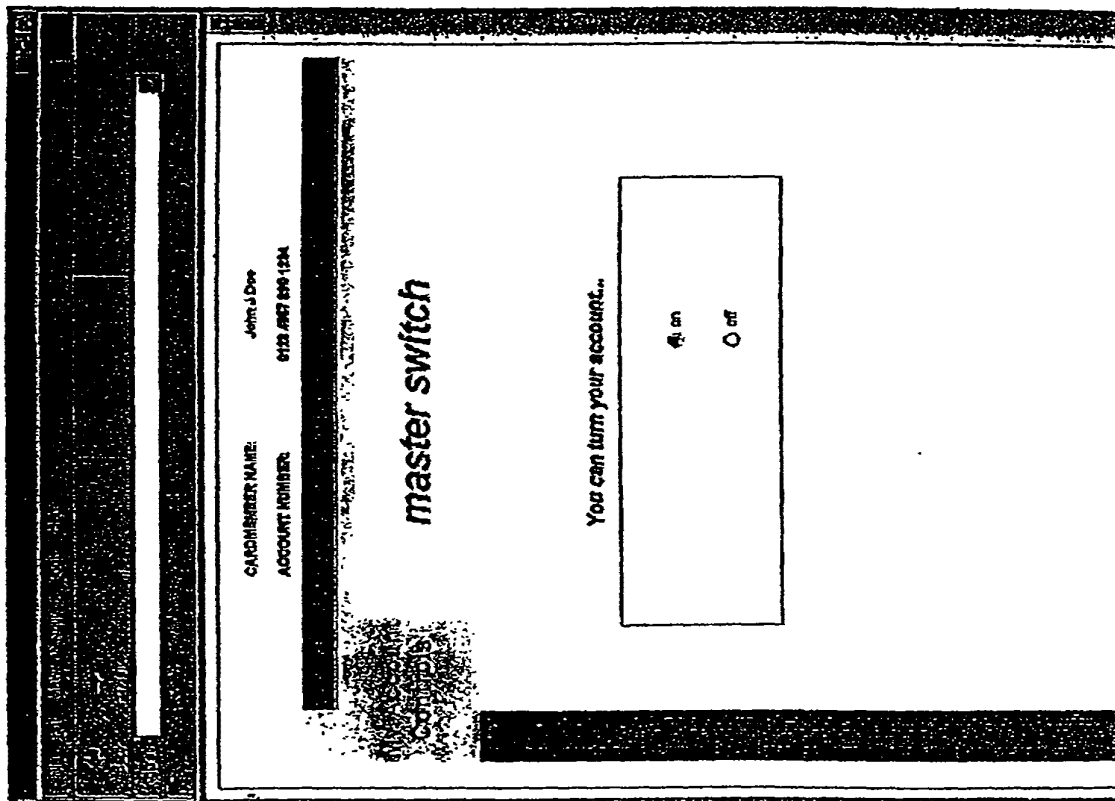
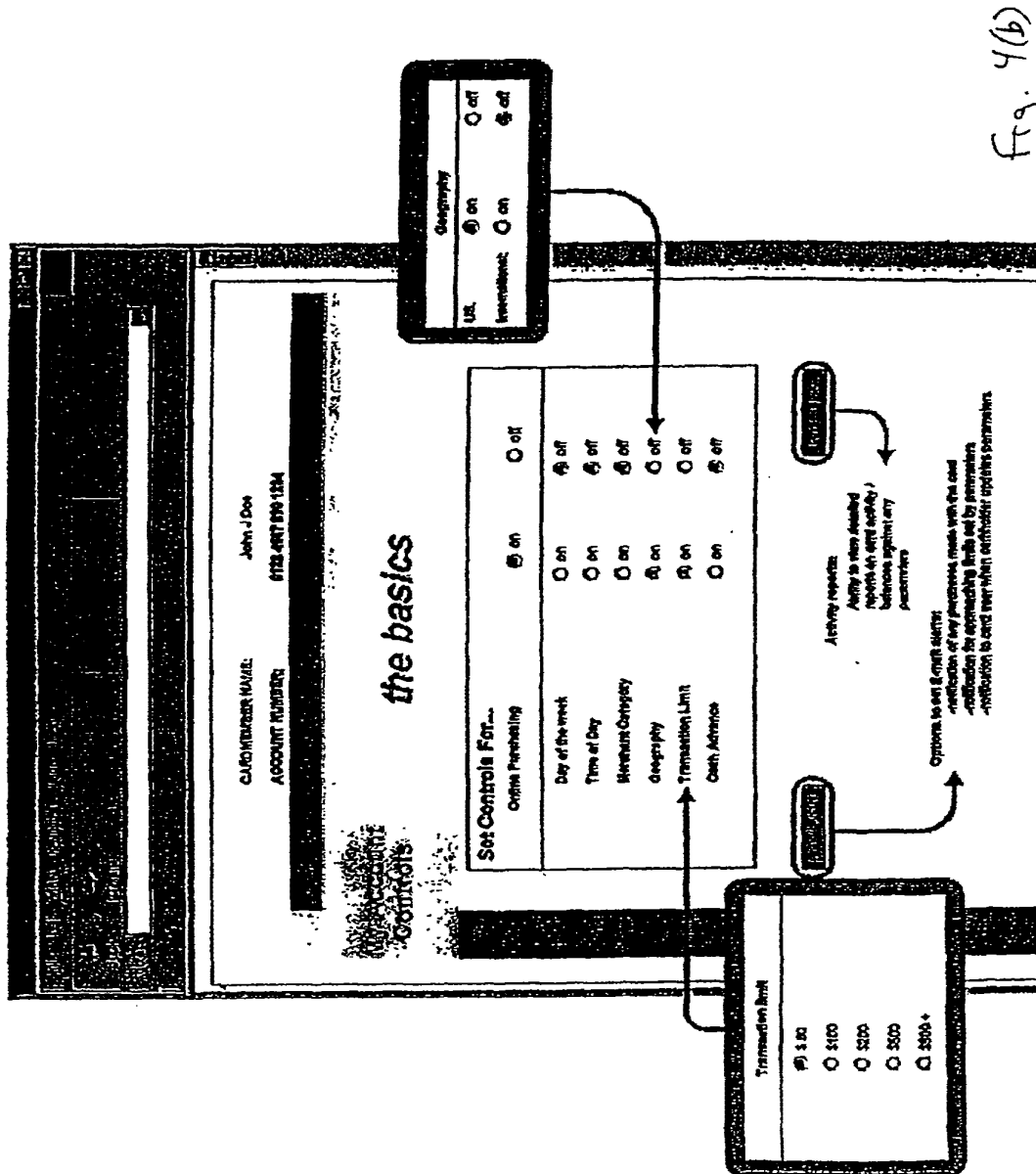


Fig. 3

Fig. 4(a)





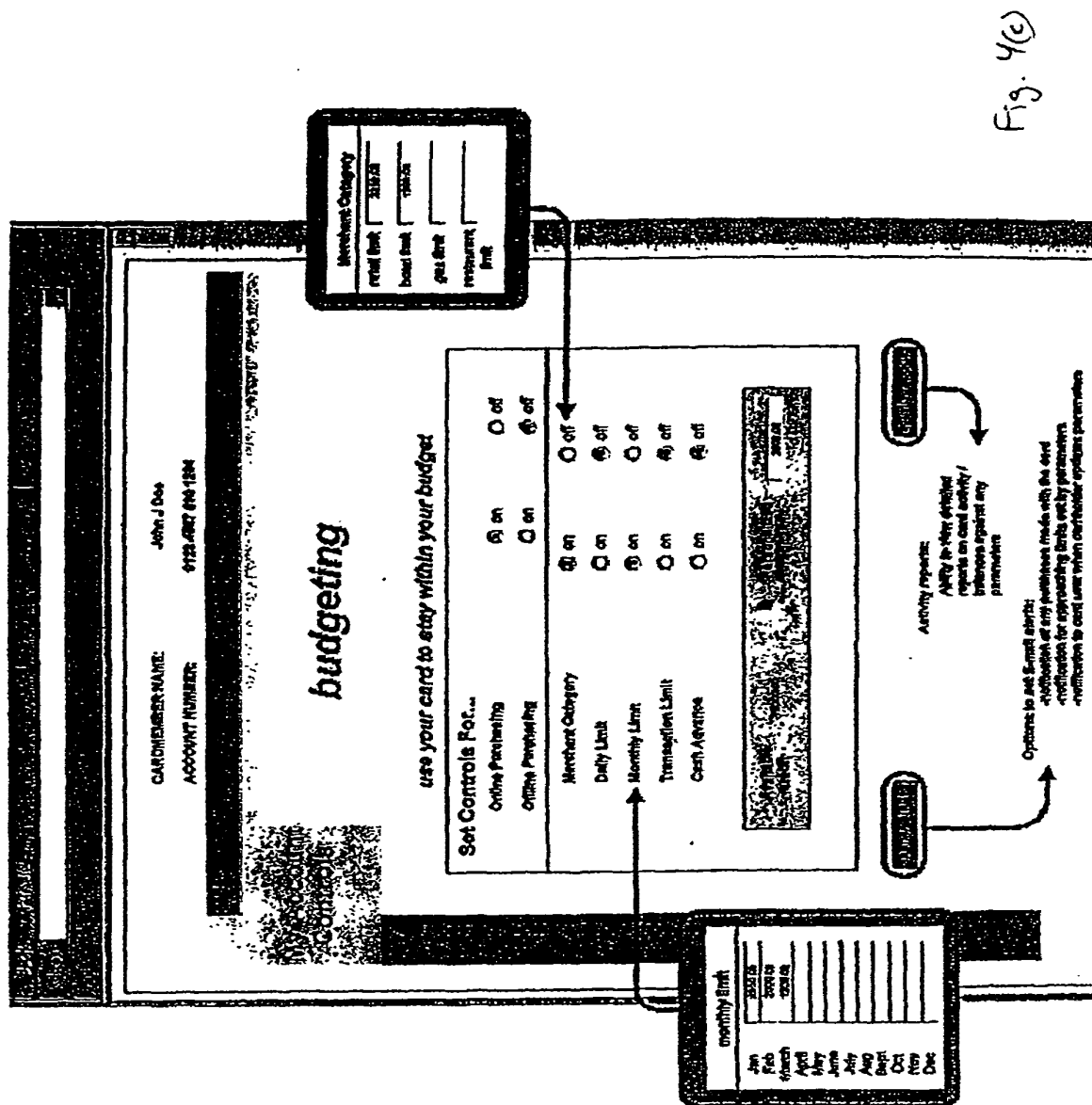


Fig. 4(d)

MEMBER NAME: Doe Inc.

ACCOUNT NUMBER: 9123 4567 890 1234

business budgeting

Card User: John William (Admin) - Card OK

set limits on your employees' spending

Set Controls For...

Online Purchasing ☒ on ☐ off

Offline Purchasing ☐ on ☒ off

Merchant Category ☐ on ☒ off

Day of the Week ☐ on ☒ off

Time of Day ☒ on ☐ off

Pin/Limit ☐ on ☒ off

Monthly Limit ☐ on ☒ off

Limit purchases to IP address ☐ on ☒ off

Pre-authorized payments ☐ on ☒ off

Transaction Limit ☐ on ☒ off

Number of purchases ☐ on ☒ off

Cash advance ☐ on ☒ off

Time of Day

8 am - 12 pm	☐ on	☒ off
12 pm - 6 pm	☐ on	☒ off
6 pm - 12 am	☐ on	☒ off
12 am - 8 am	☐ on	☒ off

Activity Report:

Activity is view enabled
reports on card activity /
business spend / any
permissions

Options to set Email Alerts:

- notification of any purchases made with the card
- notification for upcoming limits set by purchasing
- notification to card user when cardholder updates permissions

Number of purchases

per day	per week	per month	per year
1	1	1	1

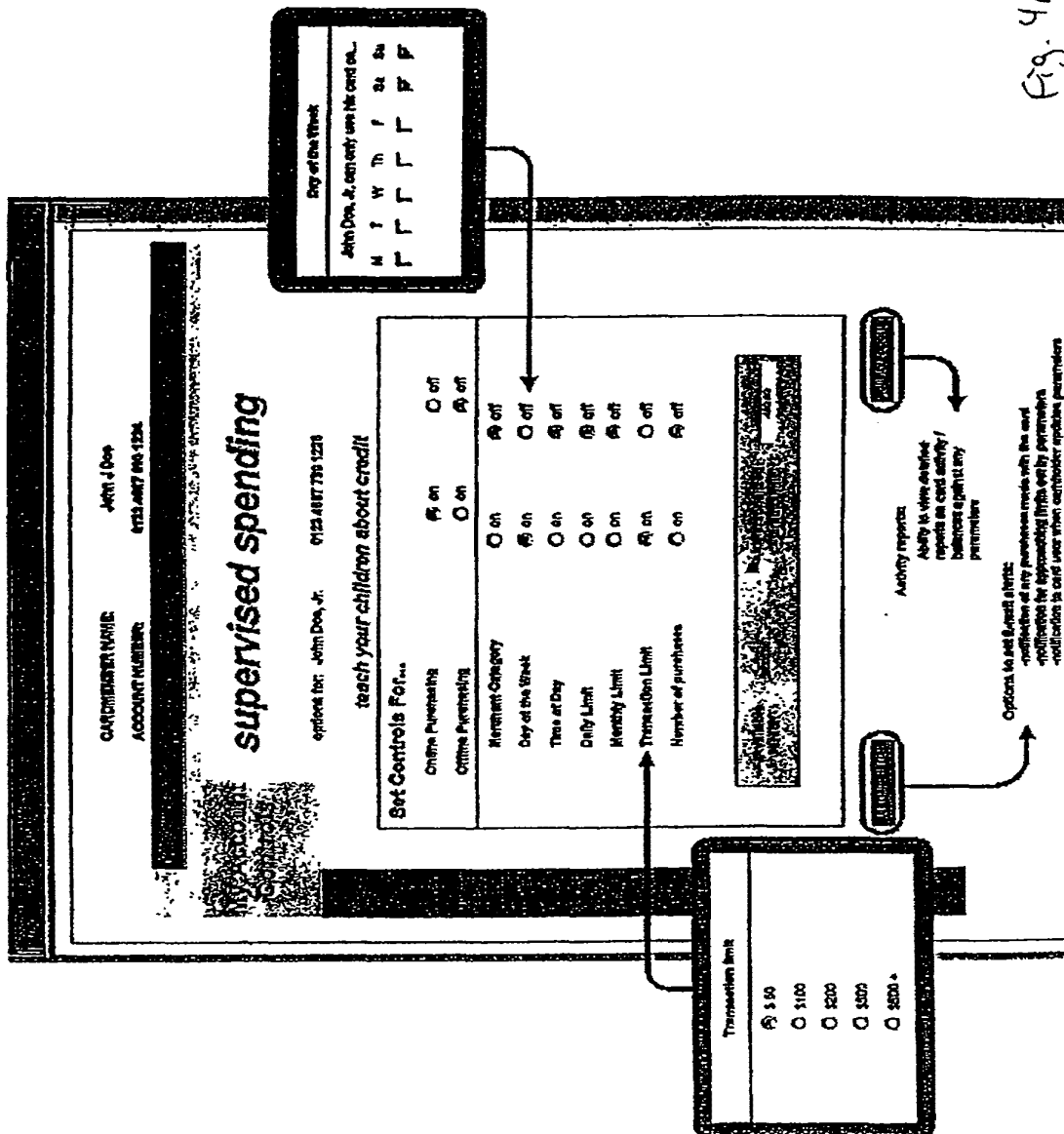


Fig. 4(e)

SYSTEM FOR PERSONAL AUTHORIZATION CONTROL FOR CARD TRANSACTIONS

FIELD OF THE INVENTION

[0001] The present invention relates to financial transaction processing systems in general and more specifically to financial transaction processing systems that relate a transaction to a cardholder and include authorization systems that authorize or deny credits or debits related to transactions.

BACKGROUND OF THE INVENTION

[0002] Credit card transactions are a common method of effecting payment in connection with a transaction. In a typical transaction, a cardholder selects merchandise or services and presents a card, such as a VISA credit card, check card or debit card, to a merchant. Before the merchant releases the merchandise or performs the service, the merchant will typically get authorization for a charge in the amount agreed on for the merchandise or service, at the point-of-sale.

[0003] Today, most authorizations are electronic, where the merchant obtains the cardholder name, account number and possibly other information. The merchant transmits that information, along with transaction-specific information, possibly including a merchant identifier, a transaction amount and a transaction description. The merchant transmits the information as part of an authorization message directed through an authorization network to a card issuer. When a card issuer approves a transaction, the merchant is given certain assurances that the merchant's bank account will be credited with the amount of the transaction and accordingly is willing to release the goods or services to the purchaser.

[0004] The cardholder generally agrees to pay for any transactions applied to the cardholder's account. In some cases, however, the cardholder's issuer financial institution (FI) or the network operator will be liable to the merchant instead of the cardholder, as in the case of a stolen card being used after the cardholder notified the issuer FI. Naturally, the issuer FI and network operator have a large incentive to limit the number of transactions for which they are liable. As a result, the typical merchant agreement requires that the merchant perform an authorization before the risk of non-payment passes from the merchant to the issuer FI or the network operator and the issuer FI and network operator place constraints on authorizations.

[0005] For example, where a card is typically used for small transactions relating to groceries and gasoline, frequent transactions relating to expensive jewelry might prompt the authorization system to deny the transaction as a suspect activity even if ultimately the cardholder is legitimately purchasing jewelry. The denial serves to protect the issuer FI and limit the liability of the issuer FI for transactions that the cardholder might later indicate as being fraudulent. The authorization system would not necessarily deny transactions that were not intended by the cardholder, and is generally limited to denying transactions under conditions that the issuer FI or the network operator might deem indicative of fraud. The issuer FI might also deny authorization where the transaction amount would cause the cardholder's credit limit to be exceeded.

[0006] In many cases, the openness and independence of the card network makes it more difficult to control the uses of the cards, but that becomes even more important where the cards used in the card network are so widely accepted and pervasive.

BRIEF SUMMARY OF THE INVENTION

[0007] In one embodiment of an authorization system according to the present invention, a cardholder provides parameters to a personal authorization subsystem. The parameters can be selected by the cardholder to limit the authorizations that would otherwise be granted on the card. The parameters can indicate limits by frequency, dollar amount, merchant, merchant type, credit limits, geographic location, time of day, combinations thereof, or the like. In a preferred embodiment, the cardholder provides the parameters to the cardholder's issuer financial institution, which integrates the cardholder authorizations with the issuer financial institution authorization process. The issuer financial institution is independent of the merchants accepting the card and the card network operator operates an open, independent network for accepting the cards of many issuer financial institutions usable with many independent merchants.

[0008] For a further understanding of the nature and advantages of the invention, reference should be made to the ensuing description in conjunction with the accompanying drawings

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. 1 is a block diagram of a transaction system wherein the present invention might be used.

[0010] FIG. 2 is a more detailed block diagram illustrating aspects of an authorization subprocessor and a cardholder's interaction with the subprocessor.

[0011] FIG. 3 is a flowchart illustrating a process of authorization control.

[0012] 4(a)-(e) illustrate aspects of a user interface usable to set cardholder authorization parameters.

DETAILED DESCRIPTION OF THE INVENTION

[0013] FIG. 1 is a block diagram of a transaction system 10. As shown there, transaction system 10 includes a merchant processing networks 12, an automated teller machine (ATM) interchange 14 coupled to a transaction network 16, such as the VISA[®] network, which is in turn coupled to an issuer bank network 18. As shown, a plurality of point of sale (POS) terminals 20 are coupled to merchant processing network 12 and a plurality of ATM's 22 are coupled to ATM interchange 14. It should be understood that the typical transaction system couples many merchant networks, ATM interchanges and issuer bank networks, in addition to merchant bank networks.

[0014] In a typical operation of transaction system 10, a card is presented to a POS terminal 20 and a transaction is generated between a cardholder and a merchant that 1) debits a cardholder's account at the cardholder's issuer bank, 2) credits a merchant's account at the merchant acquirer bank and generates the necessary electronic messages for

settlement among the banks and other transaction processing. As part of the transaction, an authorization will be performed, wherein the merchant gathers up the transaction information and sends an authorization request message to the network and receives back an authorization result, such as "approved" "denied" "ask for ID" etc.

[0015] FIG. 2 is a more detailed block diagram illustrating aspects of authorization. In one such process, a card is presented to POS terminal 20 which includes means for reading card contents, such as a magnetic card reader or a smartcard reader. POS terminal 20 is coupled to merchant network 12 and transaction network 16, which performs authorizations to protect the issuer FI or the network operator.

[0016] Transaction network 16 is also coupled to an authorization subprocessor 30, which can cause an otherwise allowable transaction to be denied, based on cardholder-provided authorization parameters available in an authorization parameter table (APT) of a plurality of authorization parameter tables 32. A cardholder's APT can be populated and updated or modified by a web server database interface 34 under the direction of a web browser 36 operated by the cardholder. As used herein, the cardholder refers to the person or persons that that issuer FI holds responsible for payment. A legitimate card presenter, i.e., the person presenting the card in a transaction, might be the cardholder, but could also be other authorized agents, such as a person to whom an additional card was issued. While this description describes a Web client-server based interface, it should be understood that other interfaces, such as direct connections, local network connections, kiosks, telephone interfaces or the like would be used instead to allow a cardholder to modify the APT associated with that cardholder's account.

[0017] In a typical operation, illustrated in FIG. 3, the cardholder (i.e., one of those ultimately responsible for nonfraudulent transactions on the card) will create, modify or update the corresponding APT to set self constraints using a browser and the linked-to web server interface stores such self constraints in the corresponding APT. Once the APT contains the cardholder supplied self constraint parameters, if a card is presented at a POS terminal, a normal authorization process occurs, wherein the issuer FI or network owner criteria for allowing the transaction are tested. If the issuer FI and network owner would deny the transaction, no further processing is needed and a denial message can be sent to the POS terminal. However, if the issuer FI and network owner would approve the transaction, the transaction details are then presented to the authorization subprocessor. The authorization subprocessor approves or denies the transaction based on the cardholder's APT, which contains constraints set by the cardholder.

[0018] While the self constraints are set by the cardholder and therefore could easily be overridden by the cardholder himself or herself, they nonetheless constrain the cardholder's account, at least by denying transactions where the cardholder unintentionally exceeds constraints, another card carrier exceeds the constraints and also constrain fraudulent use of the card that is only detectable in advanced based on constraints set by the cardholder.

[0019] The authorization subprocessor is described above as acting to approve or deny a transaction. In some embodiments, the authorization subprocessor might, in addition to

or in lieu of approval/denial, perform cardholder notifications. A cardholder notification is a message to the cardholder, or to a system designated by the cardholder, that a transaction occurred and fell within cardholder-set parameters. In some cases, the transaction is also denied, but typically the transaction is allowed, with notification. Such details can be specified by the cardholder in the parameters. The notification messages can be by mail, by telephone, by pager, by e-mail, by instant message, or by other messaging methods currently known or otherwise.

Examples of Constraints

[0020] Detailed examples of some of the possible constraints will now be described. Such constraints are specified in the APT. For ease of management, the constraints might be grouped for the cardholder into a few categories of constraints, as follows:

[0021] Transaction Type

[0022] Deny cash advances, but allow purchases.

[0023] Transaction Amount

[0024] Allow a transaction below a set limit

[0025] Allow transaction if total transactions would remain below a limit (personalized credit limit)

[0026] Allow transaction if total transactions in a set time period are below a limit

[0027] Daily Limits

[0028] Limit on number of transactions

[0029] Transaction Details

[0030] Allow transaction only during set times of the day (this allows the cardholder to in effect, indicate that any transaction made between midnight and 5 AM is a priori a fraudulent transaction)

[0031] Allow transaction only during set times of the week (e.g., movie purchases not allowed during the week)

[0032] Allow offline transactions, but not online (telephone, Internet, etc.) transactions

[0033] Allow online transactions, but only from pre-specified IP addresses

[0034] Allow transactions based on geographic location (e.g., block purchases outside U.S.)

[0035] Allow transactions based on the merchant category type (e.g., restaurants and hotels but not retail stores)

[0036] Other Limits

[0037] Preauthorization for one-time transactions

[0038] Recurring Payment Authorization

[0039] Varying controls from card carrier to card carrier

[0040] Instant Cut-off (useful when the cardholder is aware of the theft but the issuer FI has not yet detected it or is still processing the cardholder's request for closing their account.)

[0041] Arbitrary combinations of these constraints might also be possible, such as a cardholder specifying that cash advances are allowed within the U.S., but not outside the U.S. and outside the U.S. transactions are allowed, but only for merchants in the food, medical, travel and lodging categories during a prespecified date range. As another example, a parent cardholder might get an e-mail whenever a child card carrier effects an online purchase.

[0042] In addition to constraints, the APT might also contain data that directs other actions unrelated to authorization. One such action is ancillary messaging, wherein under cardholder selected conditions, a message (such as a pager message, e-mail message or instant message) is sent to a prespecified address if the conditions are met. Such conditions include card carriers that are minors effecting a transaction with an inappropriate merchant. In some cases, the cardholder might set the condition such that an e-mail is generated with every transaction, thus allowing for the electronic collection of receipts. The messages might be selective, such that only approvals result in messages or only denials result in messages (and might include the reason for the denial).

[0043] User Interfaces

[0044] Examples of the user interfaces that might be presented to a cardholder via a cardholder browser are shown in FIGS. 4(a)-(e). Other user interfaces might also be used, such as a calendar view where the cardholder could click on calendar days to allow or deny transactions for those dates. Another user interface might provide a listing of various merchant types to allow that cardholder to set predetermined ranges for each of a plurality of merchant types.

[0045] Variations

[0046] In the above, described system, the cardholder creates, modifies or updates the cardholder's APT via a Web interface. In another variation, the cardholder can interact with a telephone voice response unit (VRU) or automatic response unit (ARU) using the telephone keypad, to interact with a server that performs the requested actions on the APT. In a useful combination, the Web interface is accessible from a Web page maintained by the issuer FI for card customers. Such a Web interface might be provided to show transaction details and other account information. In some embodiments, the e-mail messages sent to the cardholder could include a hypertext link to a page showing details of the transaction so the cardholder can jump directly to a detail page from an e-mail.

[0047] Where multiple card carriers (i.e., persons with cards to present for purchases who are not necessarily the cardholder responsible for the account) are present, the user interface might allow for any variations of constraints to be selected and be different for different card carriers.

[0048] In a permissive variation, the authorization subprocessor never denies an authorization that would have otherwise been granted by the issuer FI or network operator, but just sends a message to the prespecified location when the transaction hits certain constraints. This might be useful where a cardholder needs or wants to observe transactions as they happen, to allow for early intervention. This might be

useful for businesses where the card carriers are employees empowered to make purchases for the business.

[0049] Cardholder specified constraints, implemented in an authorization system has now been described. As explained, the cardholder can apply constraints to the use of a card, typically to constrain the purchases of other authorized card carriers and of unauthorized users operating with transaction patterns not likely to be used by the cardholder and thus not constraining on the cardholder (e.g., limited to selected countries, times of day, size of transactions that the cardholder would not participate in), but could also be used by the cardholder to constrain the cardholder himself or herself for particular transactions. The latter might be useful for budget controls or controls on inadvertent spending.

[0050] As will be understood by those familiar with the art, the present invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. For example, the authorization subprocessor can be integrated in with the authorization processor that applies the issuer FI or network operator criteria to the transaction. As another example, while the present invention is described primarily with reference to credit cards, it is also usable for debit card transactions. As yet another example, while the present invention is described primarily with to merchant POS terminals, it should be understood that other systems for initiating purchase transactions might be used instead, without departing from the scope of the invention, such as the use of a merchant payment server, a PC-based cardholder terminal, a telephone, etc. or other location or system a cardholder might interface to in making a purchase, possibly even including systems where the cardholder does not interface to a system at all.

[0051] Accordingly, the disclosure of the preferred embodiments of the invention is intended to be illustrative, but not limiting, of the scope of the invention which is set forth in the following claims.

What is claimed is:

1. A credit card transaction system, wherein a cardholder or their agent is authorized to effect transactions in the credit card transaction system and bind the cardholder, the system comprising:

a transaction network coupled to merchant terminals for receiving requests for authorization from merchants who are independent of an operator of the transaction network;

an authorization server for processing the requests for authorization according to criteria set by at least one of an issuer financial institution that issued a card to the cardholder and is independent from the network operator; and

an authorization subprocessor configured to override an authorization of the authorization server based on contents of a parameter table associated with the cardholder, wherein the parameters used to override authorizations are provided by the cardholder.

2. The credit card transaction system of claim 1, wherein the parameters used to override authorizations are provided by the cardholder to the issuer financial institution.

* * * * *

Authentication Strategy: Acquirers

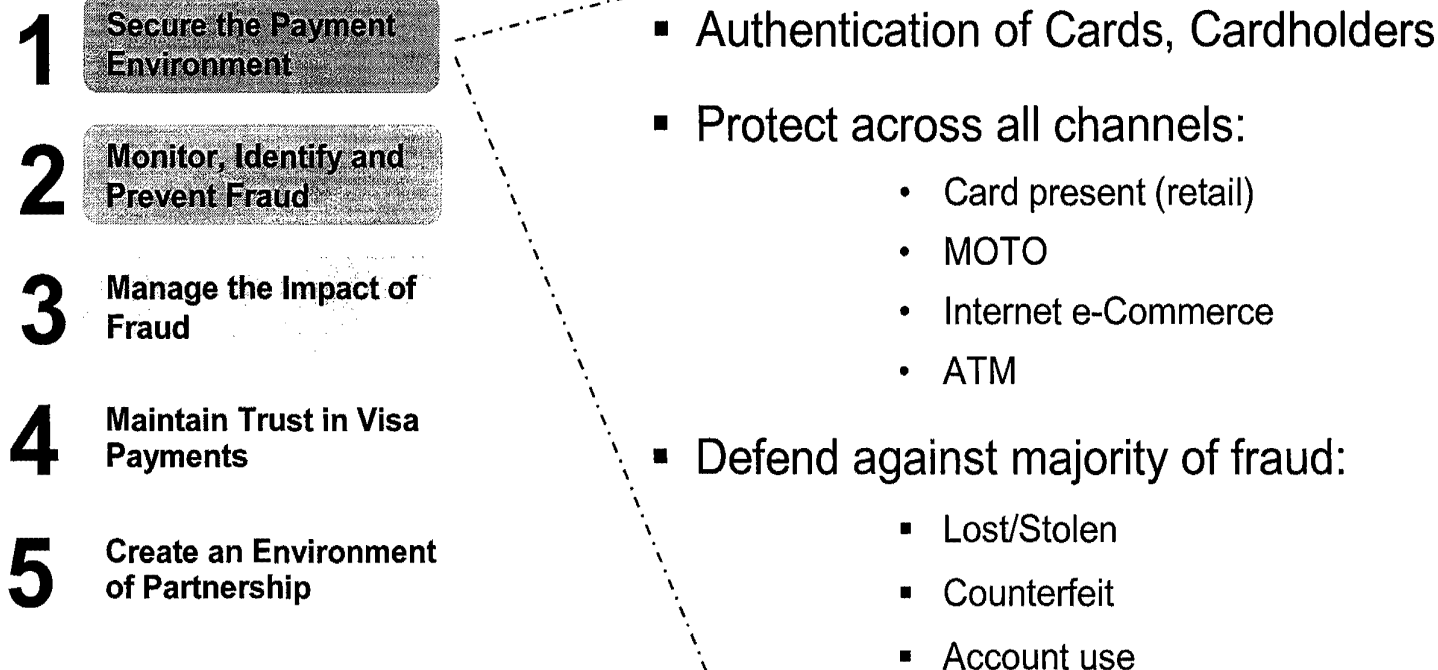
Agenda

- Visa's Authentication Strategy
- Review of Fraud Landscape
- Authentication Objectives
- Authentication Approaches & Benefits

Authentication Security Strategy

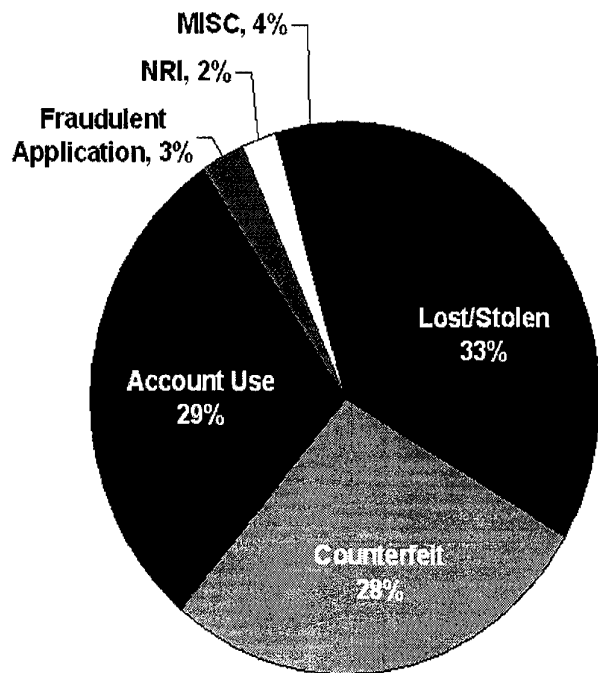
Securing the Environment is a pillar of the Security Strategy

Authentication of cards and cardholders can protect account data and render the data useless across channels and fraud types

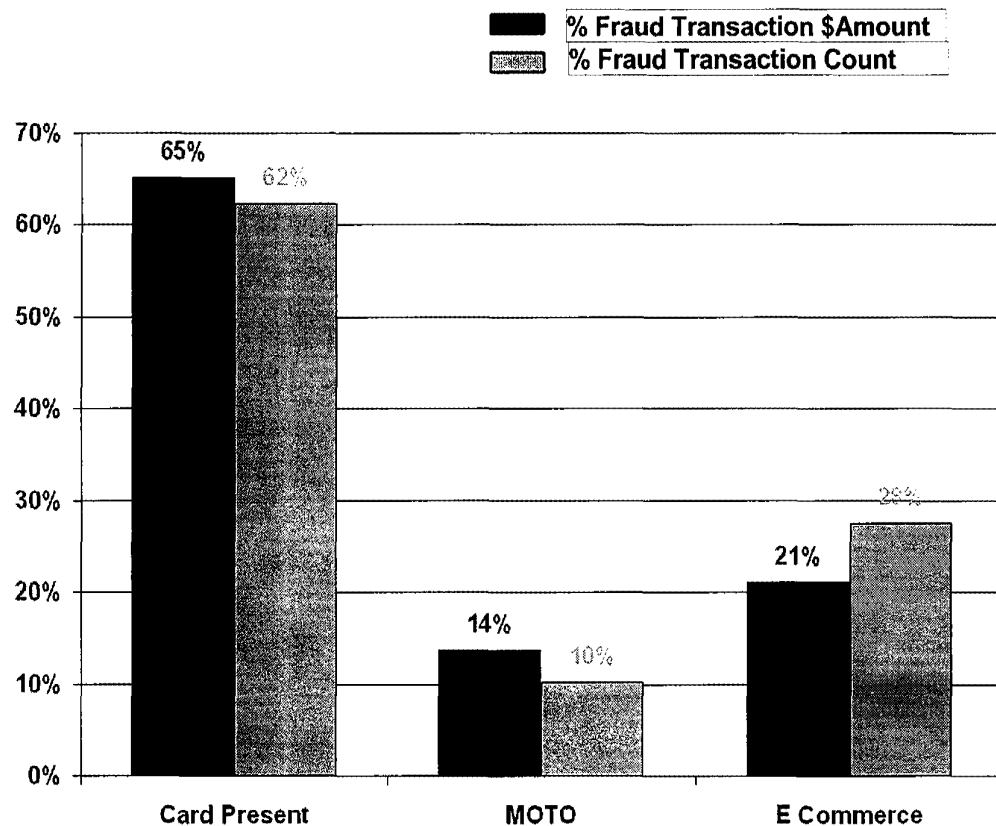


Authentication Fraud Landscape

Visa's Authentication Strategy addresses different fraud types and payment channels of the payment process



Types of Fraud by \$Amount



Fraud Distribution by
Payment Channel

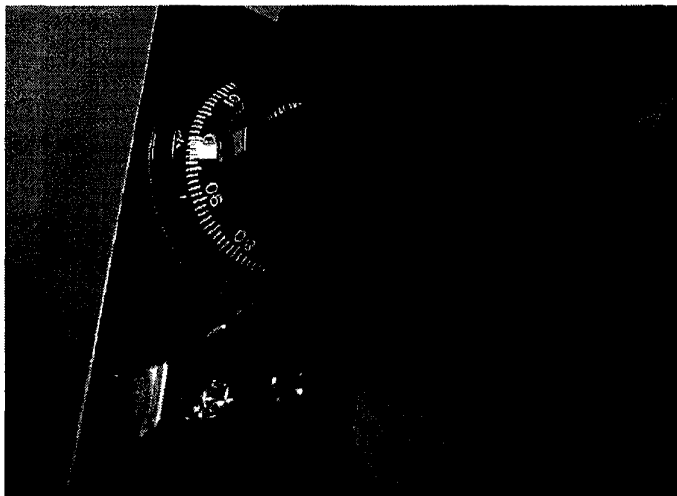
Source: 2005 Settlement Fraud , GFRS

Authentication Strategy - Acquirers

Visa Confidential

4

Authentication Fraud Landscape Statistics



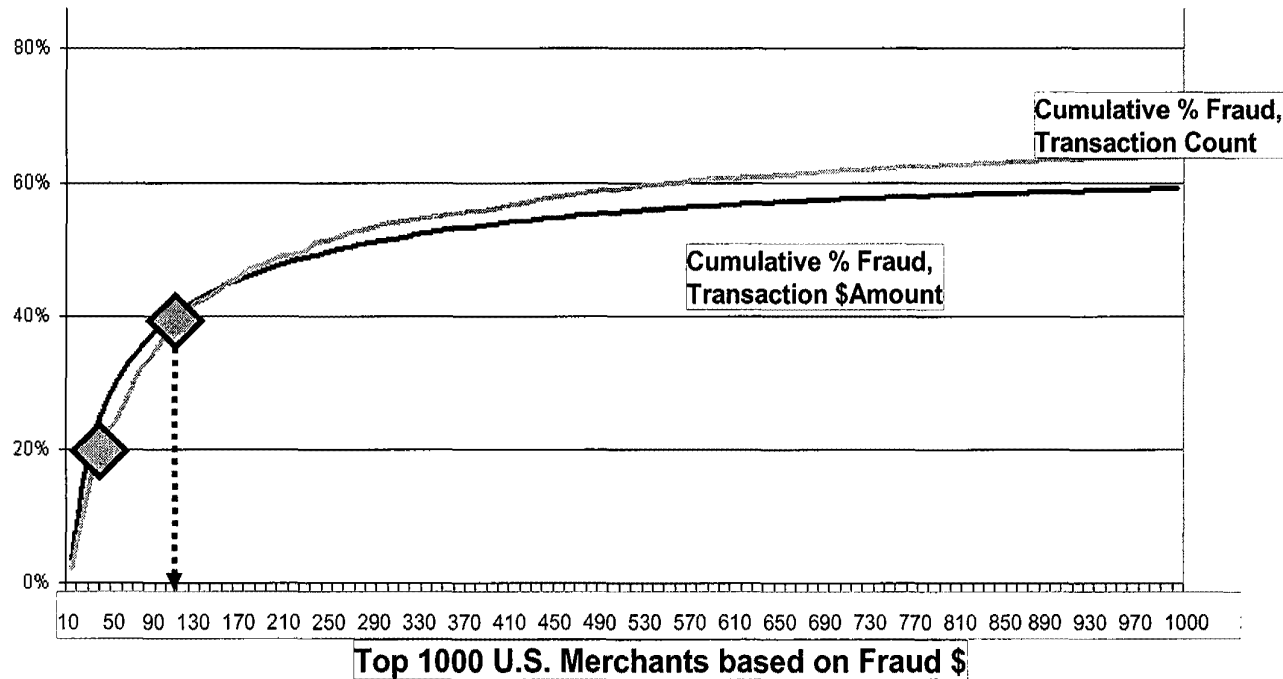
- 20% of fraudulent transactions are over \$150 but represent 80% of the total fraud amount
- Top 100 merchants in fraud represents 40% of the total fraud

Source: 2005 Settlement Fraud , GFRS; 2005 U.S. Acquired Settlement Fraud , MARS

Authentication Fraud Landscape

Cumulative Fraud Losses for top 1000 U.S. Merchants

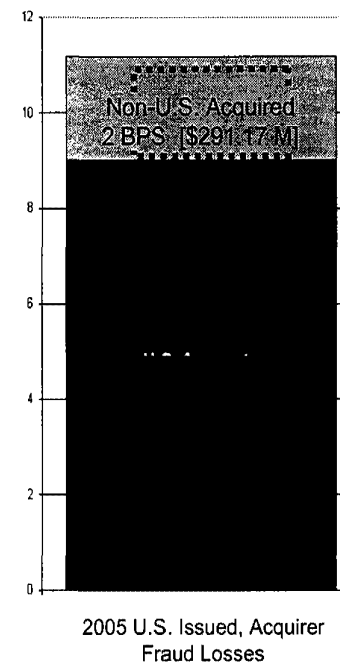
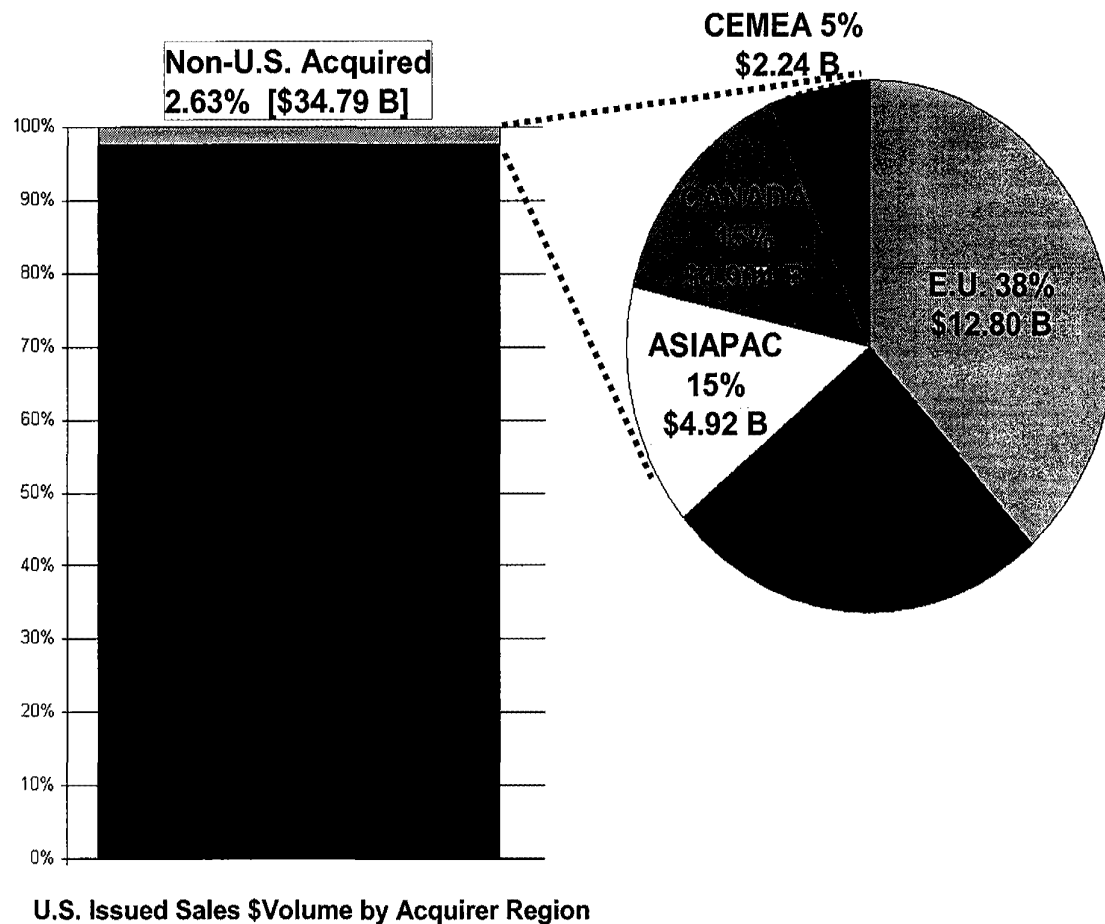
- 40% of fraud could be impacted by focusing on top 100+ merchants (by fraud \$ volume)



Source: 2005 U.S. Acquired Settlement Fraud , MARS

Authentication Sales and Fraud Landscape

U.S. Issued Activity, Acquired Worldwide



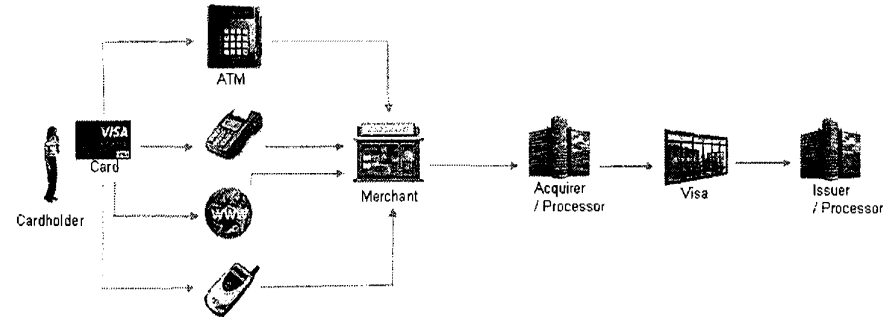
Source: 2005 Acquirer Settlement Fraud, GFRS

- 34
- This authentication strategy provides:
 - Means to be proactive towards security
 - Relatively immediate impact to fraud
 - Lower cost of entry
 - Positions acquirers to address future data needs
 - Maximize fraud mitigation efforts and help drive operational costs for fraud monitoring downward
 - Participate in authentication activities in conjunction with the issuing side of the Bank

Authentication Objectives

1. Render data useless

- Address all payment channels
- Allow for flexibility and evolution over time
- No single point of failure



2. Minimize the impact to the payment system

- Target high risk transactions without additional time or complexity
- Add functionality to the backend taking advantage of the existing Infrastructure

3. Maintain positive consumer experience

- Maintain speed and convenience value proposition
- Minimize complexity and impacts on cardholders

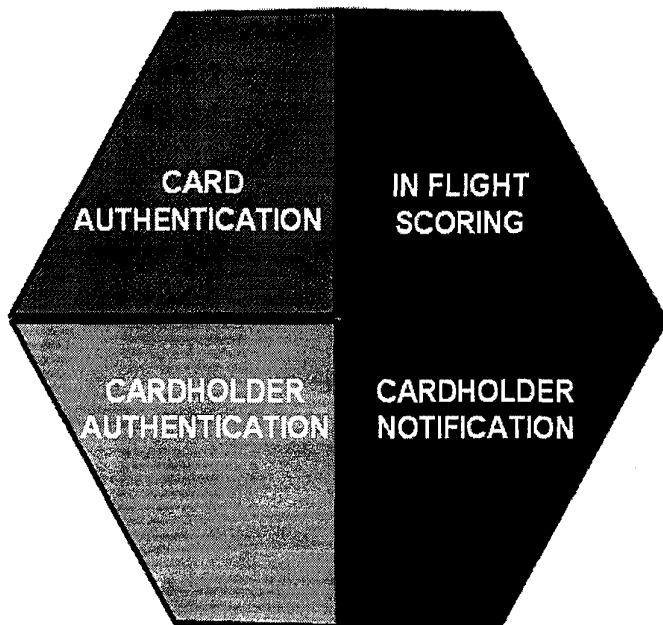
4. Support business drivers

- Be deployable in a reasonable time frame with mid/long term dividends
- Authentication method should not drive the transaction type
- Align with other processing and product strategies

5. Be aligned across the industry and globally interoperable

Authentication Multiple Layers

Visa's Authentication Strategy is a multi-layered, risk-based approach



Current Authentication Layers

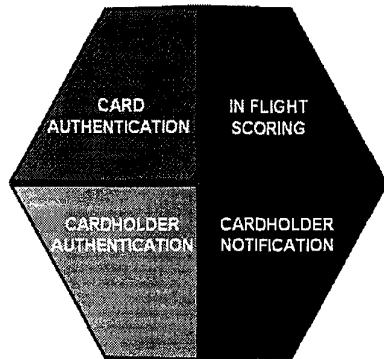
Dove Hologram
CVV - Track
CVV2 - On Card
dCVV - Contactless
Advanced Authorization
Signature
Address Verification Service AVS
VbV Password
Debit PIN

Proposed Additional Authentication Layers

Electron Magnetic Signature	✓
Dynamic Magnetic Signature	
Contactless 2.1	✓
Challenge Response	✓
Field Protection	

Effort required for Acquirer

Authentication Layers (cont'd)



ElectroMagnetic Signature (EM)

- The magnetic signature of the magstripe is captured at first transaction or at card personalization
- Digital signature of the magstripe is compared to the stored host based signature for MATCH or NO MATCH during transaction authorization

Dynamic Magstripe (DM)

- Provides dynamic CVV functionality to the magstripe

Contactless 2.0

- Expands Contactless security features globally using a cryptogram

First Transaction

- Evaluates transaction risk at first usage

Challenge Response

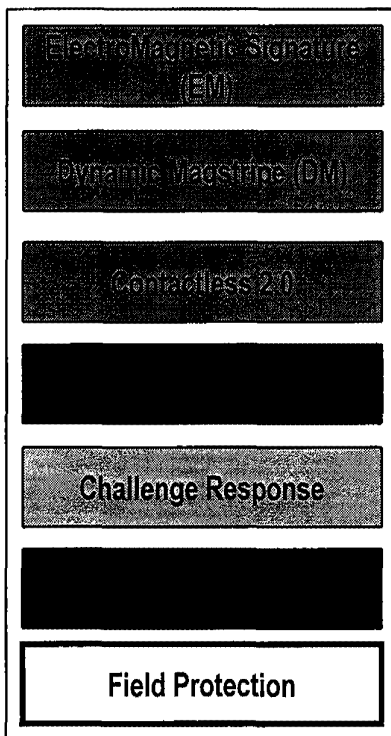
- Empowers the cardholder to further authenticate their purchase by answering a question at the POS

Notification

- Alerts the cardholder of transactions that have heightened risk

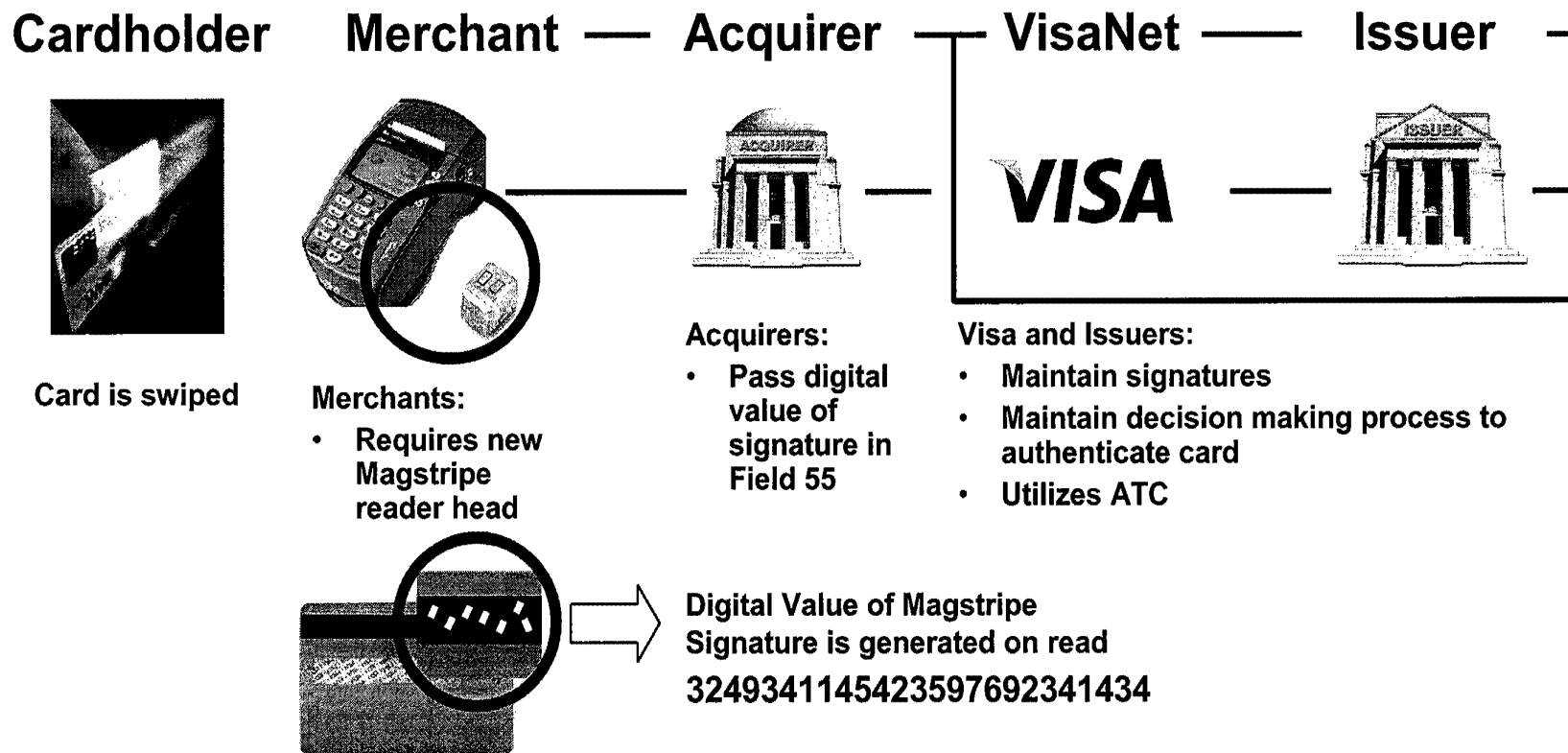
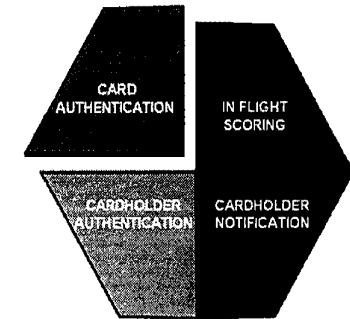
Field Protection

- Renders key data items useless outside of the Visa network



Card Authentication ElectroMagnetic Signature (EM)

EM layer requires acquirer to implement new magstripe reader; send additional data fields



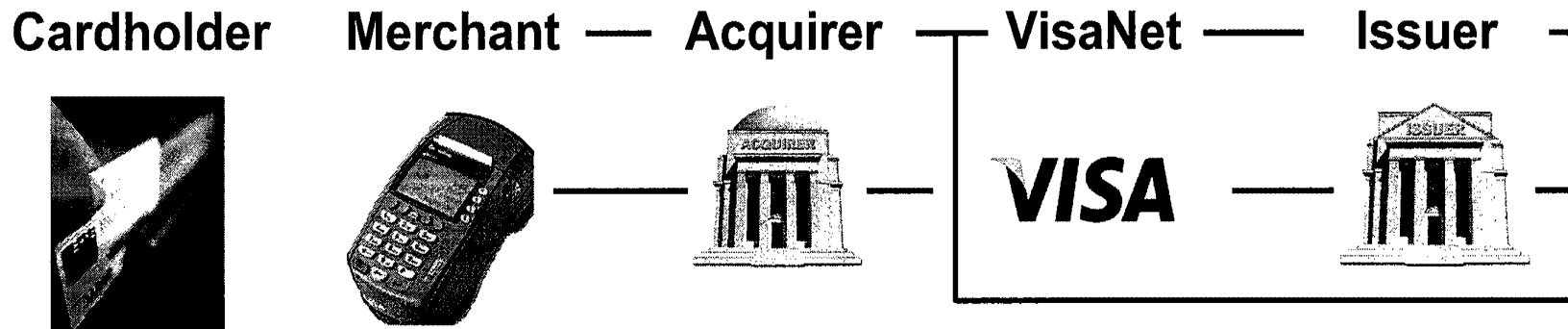
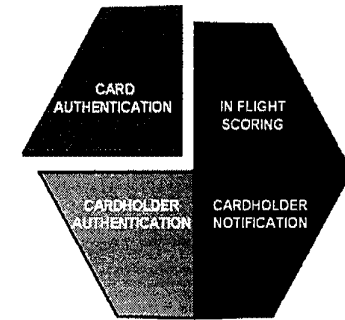
Acquirer Benefits From ElectroMagnetic Signature (EM)

- Offers an additional card authentication tool for acquirers and merchants that can potentially lower fraud, chargebacks, and declines
- Provides opportunity for targeted approach since acquirers can implement as a fraud reduction tool at specific merchants/locations, i.e. merchants with a high average ticket amount or with a high incidence of card fraud
- May provide acquirer opportunities to enhance merchant retention through this value added tool
- Can be deployed fairly quickly without need to migrate to more complex POS acceptance options
- This Authentication layer applies to Card Present (POS/ATM) environments

Note: EM requires support for processing Field 55 in the Transaction Processing Record

Card Authentication Dynamic Magstripe (DM)

DM layer has no impact to the acquirer or merchant



Card is swiped

Merchants:

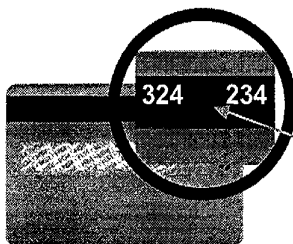
- No impact; standard terminal used for read

Acquirers:

- No impact

Visa:

- Implements new algorithm, keys, and dynamic data



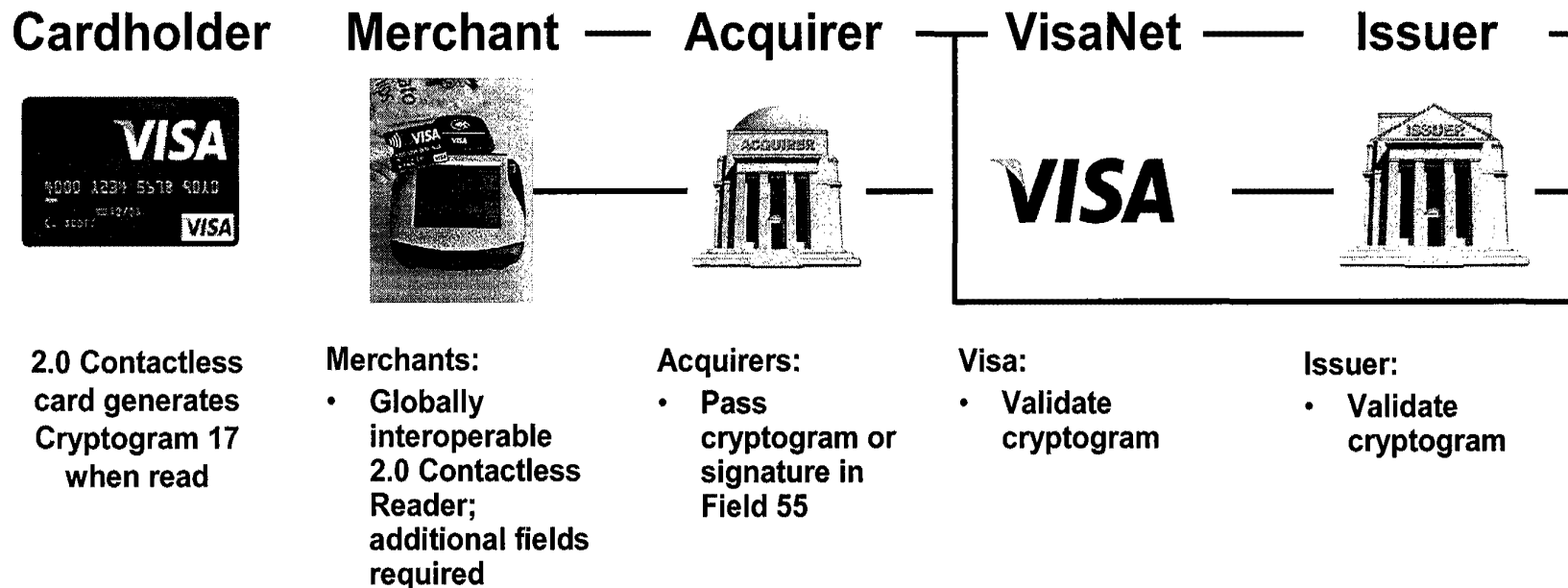
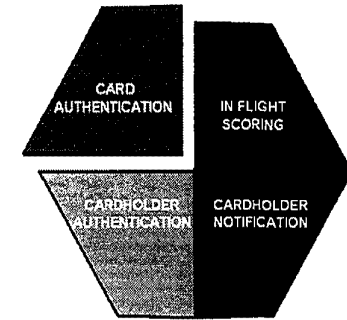
Chip in the magstripe does the work; Dynamic Magstripe Card Verification Value (dmCVV) changes with each card read

Acquirer Benefits From Dynamic Magnetic Stripe (DM)

- Used to provide stronger card authentication
- No investment required by acquirer or merchant as issuers implement this authentication layer
- May help to prevent purchases using a fraudulent card
- May lead to a reduction in potential losses by merchants
- Acquirers may lower operational costs supporting fraud related transactions
- This Authentication layer applies to Card Present (POS/ATM) environments

Card Authentication Contactless 2.0

Contactless 2.0 requires acquirers to send additional data fields; 2.0 reader at merchant



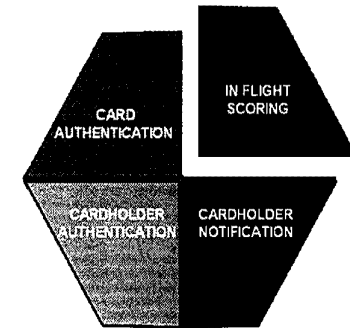
Acquirer Benefits From Contactless 2.0

- Support Version 2.0 of Contactless Payment Specification at Merchant POS
 - Provides global interoperability
 - Potential to use field for additional merchant-specific purposes
- This Authentication layer applies to Card Present (POS/ATM) environments

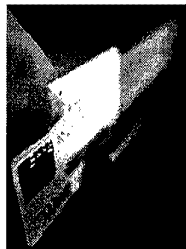
Note: Contactless 2.0 requires support for processing Field 55 in the Transaction Processing Record

In Flight Scoring Advanced Auth Features

Implementing the new Advanced Authentication features have no impact to the acquirer or merchant



Cardholder



Card is read

Merchant



Merchants:
• No impact

Acquirer



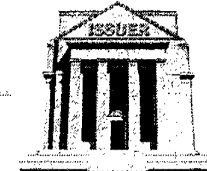
Acquirers:
• No impact

VisaNet

VISA

Visa:
• Advanced Authorization (AA) Risk Score & Risk Condition Code; incorporating Real-time decisioning, CAMS Compromised Accounts, and First Transaction

Issuer



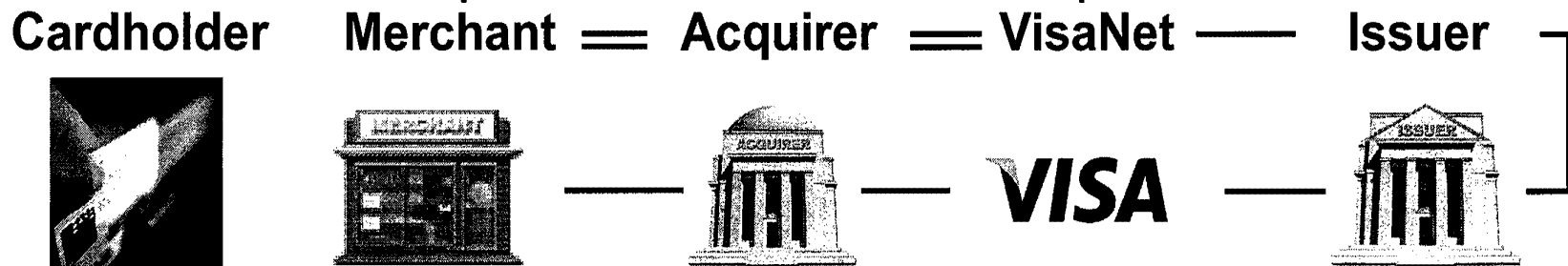
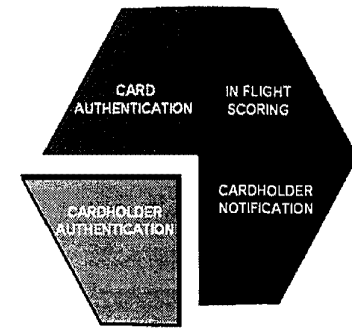
Issuer:
• No impact

Acquirer Benefits From Advanced Authentication

- Provides Advanced Authentication (AA) Risk Score & Risk Condition Code to help reduce fraudulent transactions
- Evaluates transactions from Card Present environments, ATMs, Mail Order / Telephone Order (MOTO), and Internet / E- Commerce

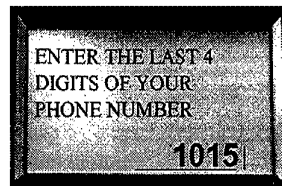
Cardholder Authentication Challenge Response

Challenge response requires additional data fields for both acquirer and merchant; terminal software update



Card is swiped

Terminal software update (also Internet / MOTO); additional fields req'd



Cardholder enters Response to Challenge question

Acquirers:

- Field changes, sequential change, Field 55

Visa:

- Presents Challenge back to merchant, e.g., Enter the last 4 digits of your phone number
- Once Response is received, VisaNet validates and sends to Issuer to authorize

Issuer:

- No impact

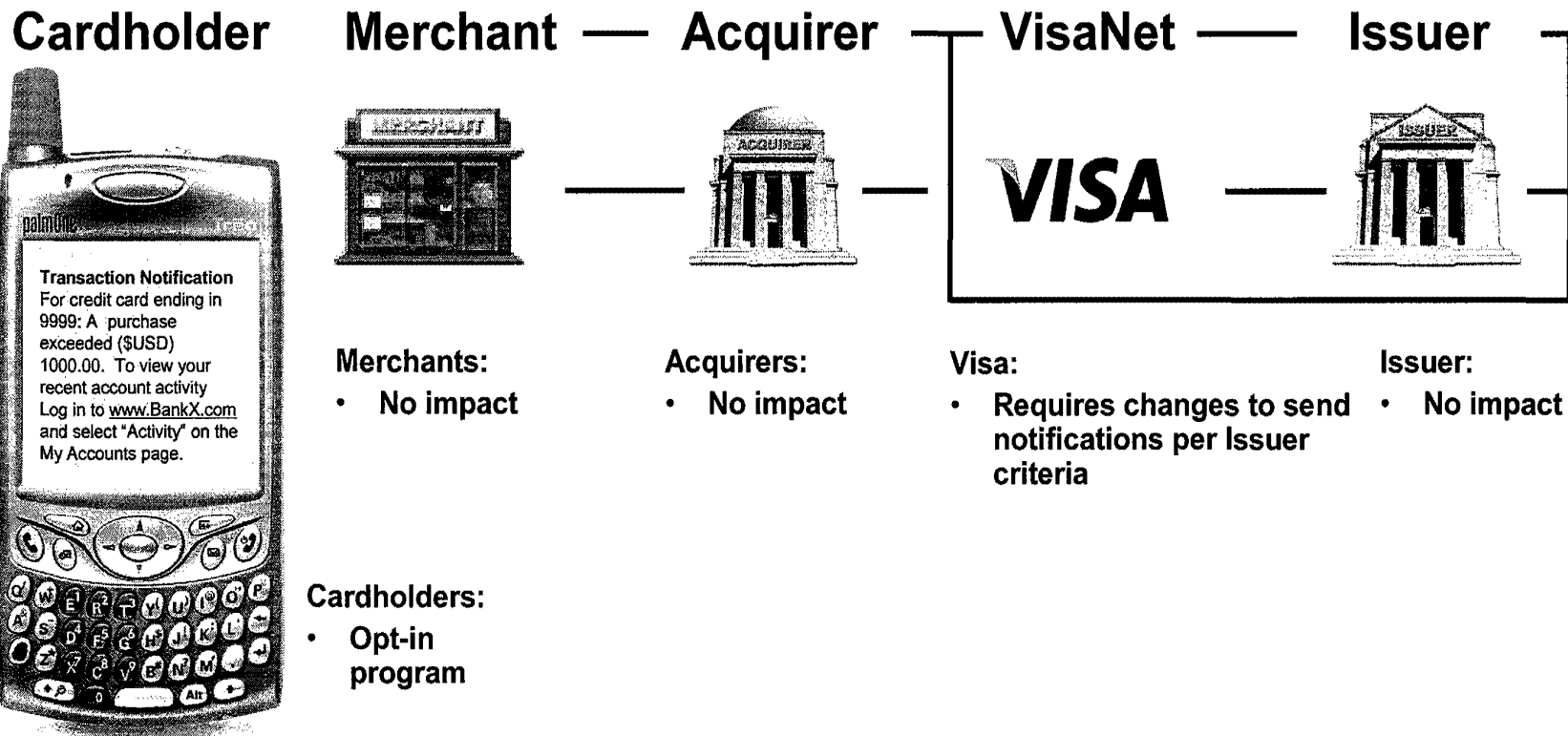
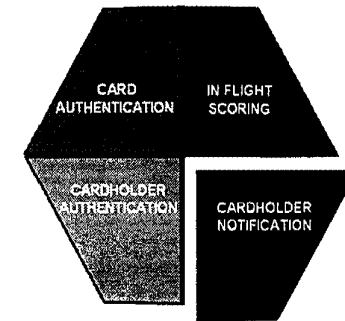
Acquirer Benefits From Challenge-Response

- Used as a tool for merchants to authenticate the cardholder
- Can be used by merchant when a “Referral” Response is received on a purchase authorization request
- The on-line challenge response will replace need for merchant to perform the call referral process (3-10 minutes)
 - Shorter time to process referral purchase
 - Less impact to merchant and cardholder
- Used in Card Present environments when high value purchases are being made as well as high risk Internet purchases
- All payment channels supported: Card Present, ATM, MOTO, Internet / E-Commerce

Note: Challenge Response requires support for processing Field 55 in the Transaction Processing Record

Cardholder Notification

Cardholder notification has no impact to the acquirer or merchant



Acquirer Benefits From Cardholder Notification

- Used as a tool to notify the cardholder of activity
- All payment channels supported: Card Present, ATM, MOTO, Internet / E-Commerce

All Stakeholders Benefit from Efforts

The single investment for acquirers/merchants addresses 3 layers, but acquirers/merchants may also benefit from the other layers implemented by issuers

Authentication Layer	Issuer	Acquirer	Payment Channels
ElectroMagnetic Signature (EM)		✓	POS/ATM
Dynamic Magstripe (DM)	✓		POS/ATM
Contactless 2.0	✓	✓	POS/ATM
Advanced Authorization	✓		All
Challenge Response	✓	✓	All
Cardholder Notification	✓		All

Payment Channels: POS/ATM = Point Of Sale, ATM; All = POS/ATM, MOTO, Internet / E-Commerce

Authentication Strategy

Pilot Execution and Results

- Minimize impact to consumer and merchant
- Conducting offline evaluation; existing fraud mitigation processes will remain in place
- Protecting pilot and production data through Visa's existing intensive security policy
- Generating performance metrics to evaluate technology

Authentication Strategy

Acquirer Next Steps

- Acquirer to work with Visa to identify ElectroMagnetic (EM) Signature merchant candidates and locations
- Pilot merchants sign participation agreement
- Discussion for Field 55 support and subsequent sizing/timing

Additional authentication embodiments

1. Card Verification

Currently, thieves can "skim" a card, by copying the data on the magnetic stripe of the card. A payment processing organization can support different technologies that stop this. Two magnetic stripes on two cards can have identical information, but they would be different in certain physical aspects, which might be called a fingerprint or DNA of the magnetic structure. A copied or skimmed card would have a different fingerprint. Thus, when cards are initially made, the fingerprint of the magnetic stripe will be determined, and stored in a database along with the account number, for later verification.

There are currently two products supporting this magnetic stripe fingerprint with two different algorithms. The reading of the fingerprint of a card according to such an algorithm is done by the POS card reader. Two companies that are making these are Magtek and Semtek.

An embodiment of the invention is to make both of these systems practical, by supporting both. A different ID is assigned to the two types of algorithms, so that when a card is read and the information is sent to VisaNet, the back-end processor will be able to see which algorithm was used from the ID, or if no algorithm was used.

Another card verification technology comes from QSecure. It has a dynamic CVV number on the card, by putting a chip under the card stripe which can change the number. In addition, the entire number is not sent, but information from which the full number can be determined. For example, 106 might be represented by 6. A payment processing organization can also support this, using an ID from the card (not the reader) to identify that this system is used.

In this example, the system would accept information from either the Magtek or Semtek card readers, or the QSecure cards, with each assigned an ID to tell them apart. Thus, for example, a payment processing organization might use IDs like these:

01 - Magtek

02 - Semtek

03 - QSecure

2. Backend confidence assessment. The backend processor will determine whether a card transaction meets a desired confidence threshold of likely validity. For example, if one of the 3 card verifications above is present, and there has not been any recent suspicious transactions with the card, it will be considered valid. If an old (legacy) card and reader is used, with none of the 3 card protections described above, and there has

been recent suspicious activity, (1) a dynamic challenge (query) can be done of the user before approval, and/or (2) the cardholder can be notified.

Also, in the above example, one algorithm could be more reliable than the other. On the back end, algorithms can be evaluated. For example, one algorithm may have 90% reliability and another algorithm may have 70% reliability. There are a number of reasons why different algorithms may have different levels of reliability. For example, depending on the sensitivity of the terminal, depending on the way that the card is swiped, and depending on the aging of the card, some algorithms may be able to handle data more precisely.

Illustratively, McDonalds may have a relationship with Veriphone-Magtek and Taco Bell may have a relationship with Igenico-Semtek. They have different algorithms. Each one delivers two sets of data using two different algorithms. When they come back to a payment processing organization such as Visa, it may identify data as originating from a Semtek algorithm, and/or from Magtek algorithm. Weight can be put on the algorithms so that a confidence level can be determined.

Dynamic Magstripe Card Verification Value Algorithm

In some embodiments, an algorithm can vary on the card and an algorithm can vary on the terminal. There may be one technology on the card and another technology on the terminal. To conduct fraudulent activity, one must figure out the technology of the card and the technology of the terminal. Here is an example:

Terminal 1

Card 1 - magstripe characteristic 1
Algorithm 1 - DNA algorithm 1
Account number

Terminal 2

Card 2 - magstripe characteristic 2
Algorithm 2 - DNA algorithm 2
Account number

A back end server may determine that it is received various algorithms. Conflict resolution can take place to determine which algorithm is more reliable.

One may also verify the cardholder using embodiments of the invention. One could ask the cardholder for his PIN. However, someone can see the cardholder entering the PIN and can get the PIN. The problem with this is that PIN data are static. The data that are used in embodiments of the invention are preferably dynamic. A challenge response, as described above is a way that the question can be dynamic. For example, if one is using a gas pump, the issuer or payment processing organization may ask the cardholder for his

zip code. Different questions may be asked and the answers to the questions may be dynamic (e.g., a different answer to the same question such as "Where are you now?").

If one uses a card that does not have any of the above noted features (high tech algorithms), then a first line of defense would be to ask the cardholder for his four digit PIN. If the payment processing organization or issuer sees that the cardholder is using a card that is very well proven and that he is buying at a merchant that he normally buys at, and he is using a high tech terminal, then challenge questions may not be necessary.

One may come up with a probability. If the threshold is met, one does not need a challenge response. A challenge response may be appropriate if he does not meet the threshold.

In embodiments of the invention, the issuer or payment processing organization can indicate that a transaction is accepted, or denied, or that it needs more information to make a decision. For example, a customer may be a B of A customer who is in New York. The payment processing organization knows he is in New York, since the organization has seen the bills. The organization can ask about the hotel that the customer is staying at. The cardholder is most likely going to remember his hotel. This source of data is continuous and free for the processing organization. Note that the question "What hotel are you staying at?" is dynamic and has a different answer each time.

There may also be first transaction scoring. A first amount of data can be collected which will illustrate buying behavior. If this is the holder's first card, and he lives in San Francisco, and the first transaction is a jewelry purchase, then the holder is flagged in terms of his buying pattern. It does not mean that the transaction is rejected. The system knows the holder's history, and there are different categories of questions depending on the history. For example, questions may vary depending on how long he has been a cardholder. At the beginning of the relationship, the questions to the holder may be different than 4 months into the relationship between the cardholder and the issuer. The longer that the holder is in the relationship, the more the issuer and payment processing organization know about the holder's behavior. Challenges may also be location based if a GPS, merchant identifier, or some other location system is used.

Another component may include notification. The idea is to deliver a message back to the cardholder, based on a specific profile of the transaction. By using the notification channel, the issuer or processing organization can provide the holder with a challenge question.

One could use a "brute force" technique, by asking questions all of the time. However, this involves more time, cost, and inconvenience. By using embodiments of the invention, questions can be asked to holders to minimize this to 0.1% of transactions.

Cardholders could provide their own questions to the issuer or payment processing organization, or merchants may set their own challenge questions. For example, each

time a plasma TV is purchased, the merchant may request that additional authentication questions be asked to the consumer.

Electronic Patent Application Fee Transmittal

Application Number:

Filing Date:

Title of Invention:

AUTHENTICATION USING MULTIPLE COMPONENTS

First Named Inventor/Applicant Name:

Ayman Hammad

Filer:

Patrick Raymond Jewik/Andrea Beck

Attorney Docket Number:

16222U-024411US

Filed as Large Entity

Provisional Filing Fees

Description

Fee Code

Quantity

Amount

**Sub-Total in
USD(\$)**

Basic Filing:

Provisional application filing

1005

1

200

200

Pages:

Claims:

Miscellaneous-Filing:

Petition:

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

IPR2025-01149

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				200

Electronic Acknowledgement Receipt

EFS ID:	1426567
Application Number:	60884089
International Application Number:	
Confirmation Number:	1975
Title of Invention:	AUTHENTICATION USING MULTIPLE COMPONENTS
First Named Inventor/Applicant Name:	Ayman Hammad
Customer Number:	66945
Filer:	Patrick Raymond Jewik/Andrea Beck
Filer Authorized By:	Patrick Raymond Jewik
Attorney Docket Number:	16222U-024411US
Receipt Date:	09-JAN-2007
Filing Date:	
Time Stamp:	16:02:41
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$200
RAM confirmation Number	214
Deposit Account	201430
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)				
1		app.pdf	3837239	yes	89				
	Multipart Description/PDF files in .zip description								
	Document Description		Start	End					
	Application Data Sheet		1	3					
	Specification		4	21					
	Claims		22	26					
	Abstract		27	27					
	Drawings		28	32					
	Appendix to the Specification		33	89					
Warnings:									
Information:									
2	Fee Worksheet (PTO-06)	fee-info.pdf	8125	no	2				
Warnings:									
Information:									
Total Files Size (in bytes):			3845364						
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.									