US 20060186195A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2006/0186195 A1

(43) Pub. Date: Aug. 24, 2006

Gray

(54) SYSTEM FOR INCREASING THE SECURITY OF CREDIT AND DEBIT CARDS TRANSACTIONS

(75) Inventor: R. O'Neal Gray, Dallas, TX (US)

Correspondence Address:
JONES, WALKER, WAECHTER, POITEVENT, CARRERE
& DENEGRE, L.L.P.
5TH FLOOR, FOUR UNITED PLAZA
8555 UNITED PLAZA BOULEVARD
BATON ROUGE, LA 70809 (US)

(73) Assignee: Quake!, LLC

(21) Appl. No.: 11/061,616

(22) Filed: Feb. 22, 2005

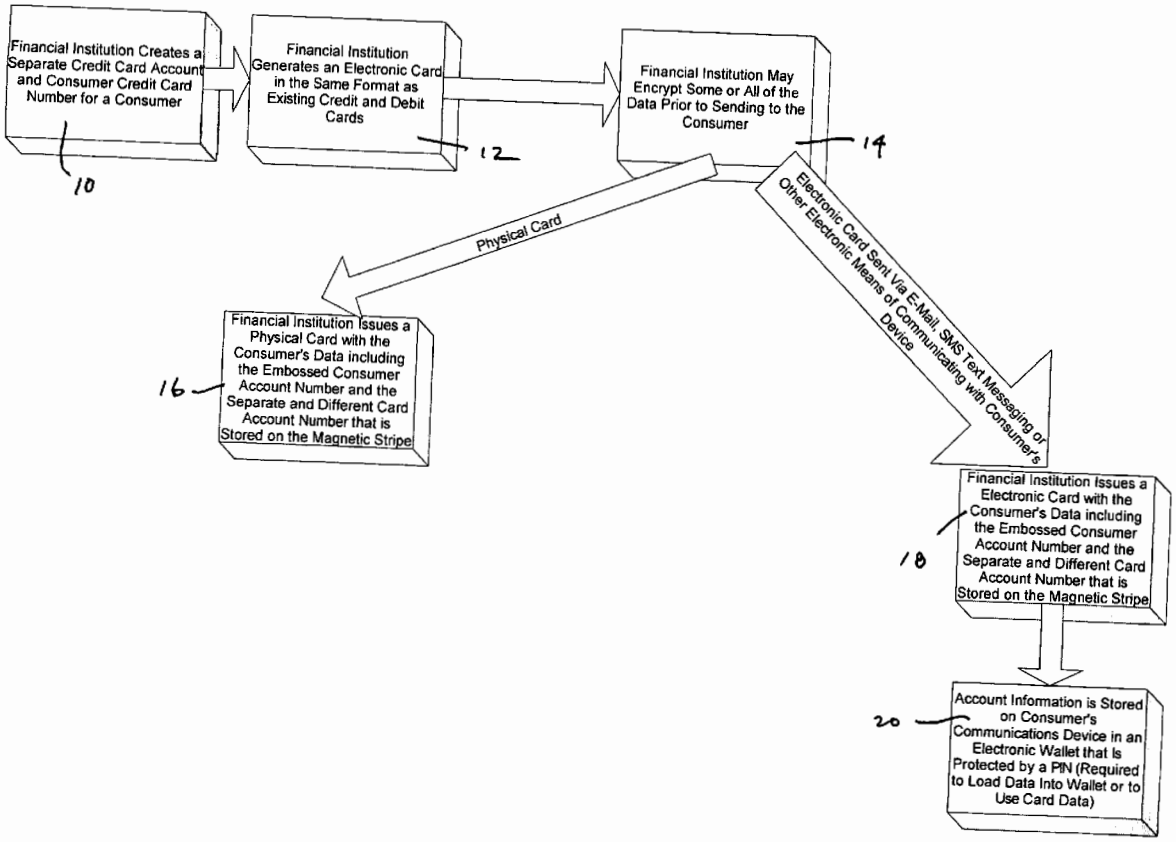
Publication Classification

(51) Int. Cl.
G06K 5/00 (2006.01)

(52) U.S. Cl. 235/380

(57) ABSTRACT

A system for facilitating a commercial transaction by a consumer includes a card or electronic storage device which includes a first number for identifying a financial account of the consumer and a second number, related to the first number, for use in authorizing a transaction involving the financial account of the consumer.



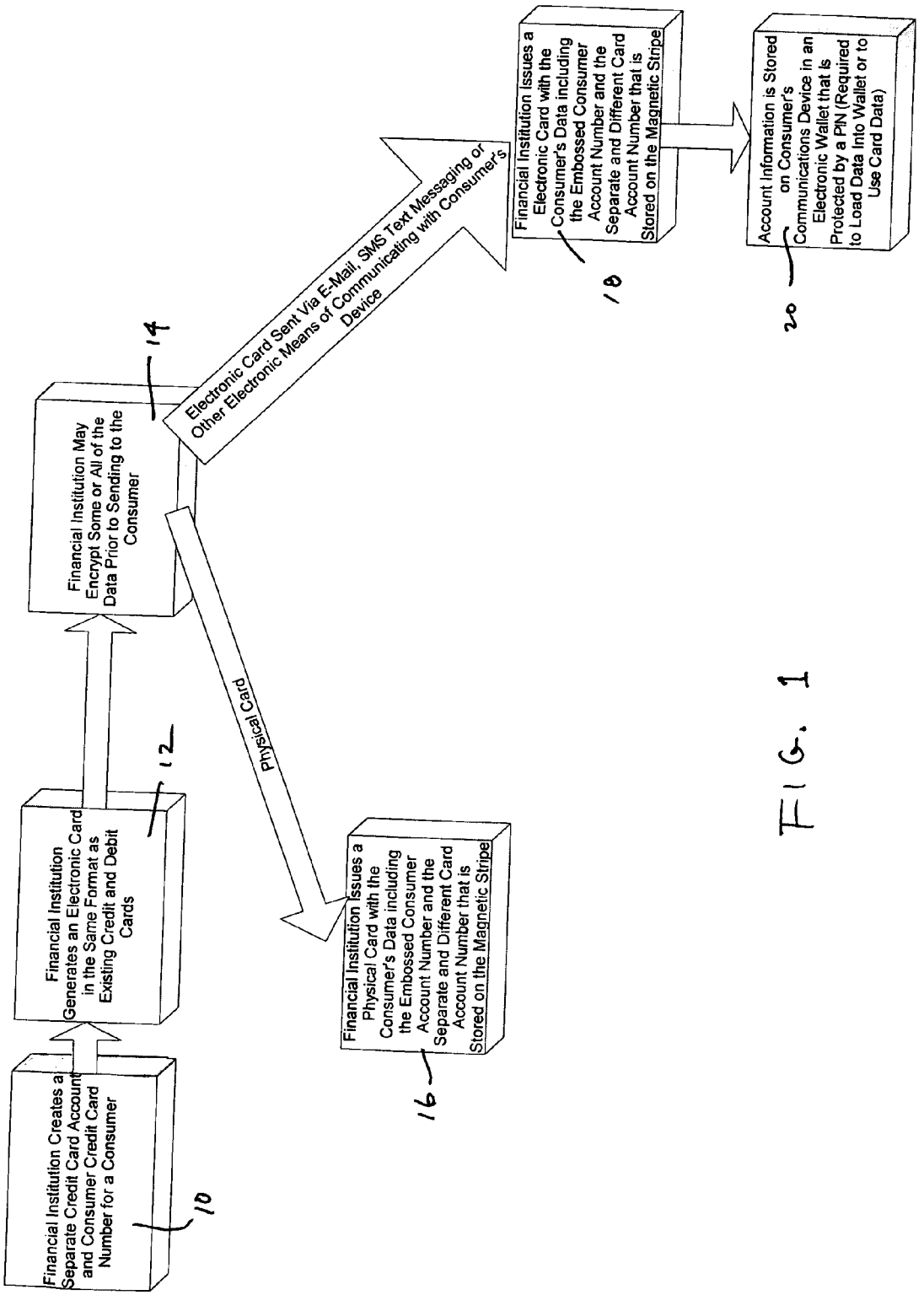

Financial Institution Creates a Separate Credit Card Account and Consumer Credit Card Number for a Consumer
10
Financial Institution Generates an Electronic Card in the Same Format as Existing Credit and Debit Cards
12
Financial Institution May Encrypt Some or All of the Data Prior to Sending to the Consumer
14
Electronic Card Sent Via E-Mail, SMS Text Messaging or Other Electronic Means of Communicating with Consumer's Device
Physical Card
Financial Institution Issues a Physical Card with the Consumer's Data including the Embossed Consumer Account Number and the Separate and Different Card Account Number that is Stored on the Magnetic Stripe
16
Financial Institution Issues a Electronic Card with the Consumer's Data including the Embossed Consumer Account Number and the Separate and Different Card Account Number that is Stored on the Magnetic Stripe
18
Account Information is Stored on Consumer's Communications Device in an Electronic Wallet that is Protected by a PIN (Required to Load Data Into Wallet or to Use Card Data)
20

FIG. 1

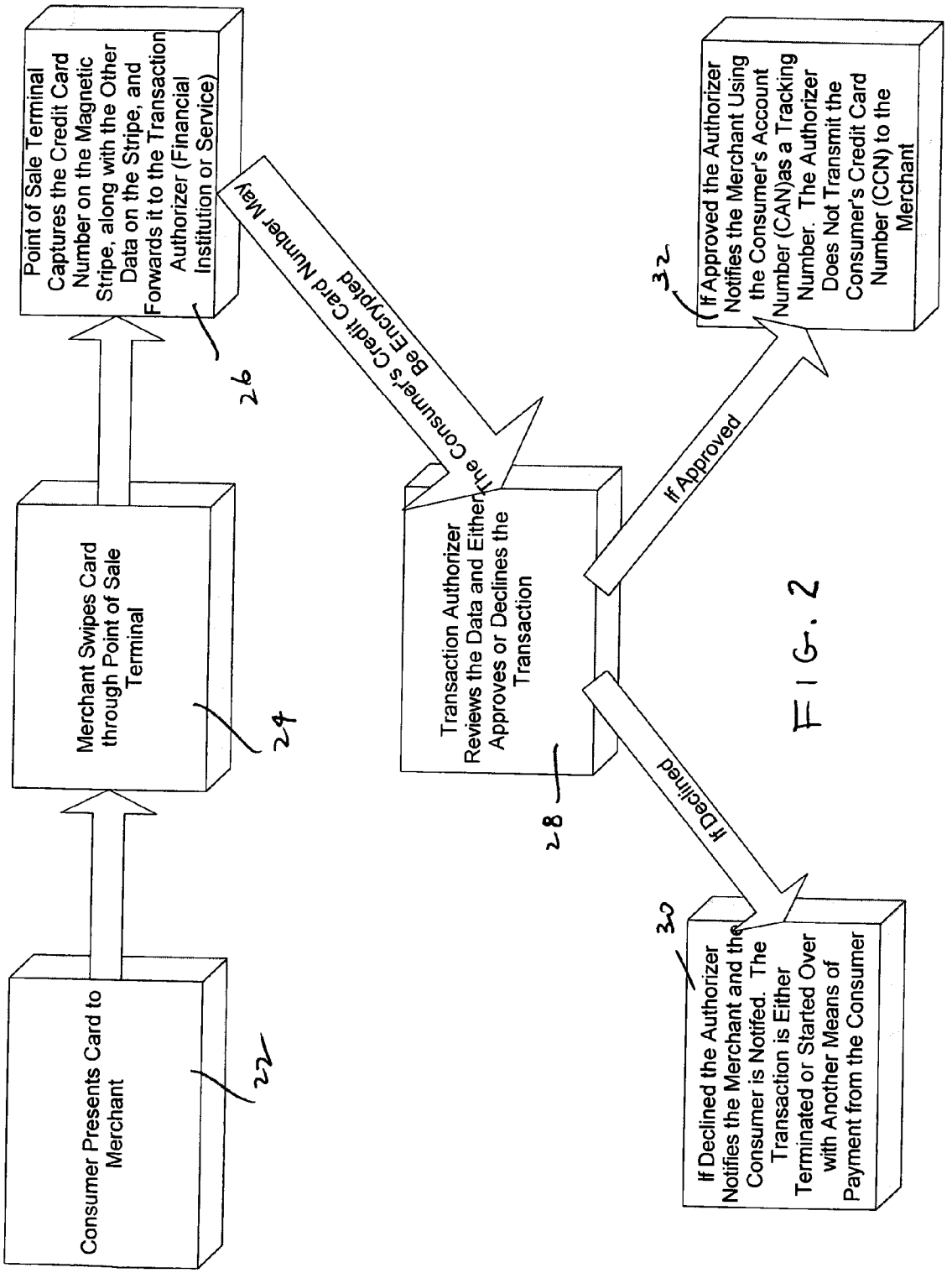

Consumer Presents Card to Merchant
22
Merchant Swipes Card through Point of Sale Terminal
24
Point of Sale Terminal Captures the Credit Card Number on the Magnetic Stripe, along with the Other Data on the Stripe, and Forwards it to the Transaction Authorizer (Financial Institution or Service)
26
The Consumer's Credit Card Number May Be Encrypted
Transaction Authorizer Reviews the Data and Either Approves or Declines the Transaction
28
If Approved
If Approved the Authorizer Notifies the Merchant Using the Consumer's Account Number (CAN)as a Tracking Number. The Authorizer Does Not Transmit the Consumer's Credit Card Number (CCN) to the Merchant
32
If Declined
If Declined the Authorizer Notifies the Merchant and the Consumer is Notified. The Transaction is Either Terminated or Started Over with Another Means of Payment from the Consumer
30

FIG. 2

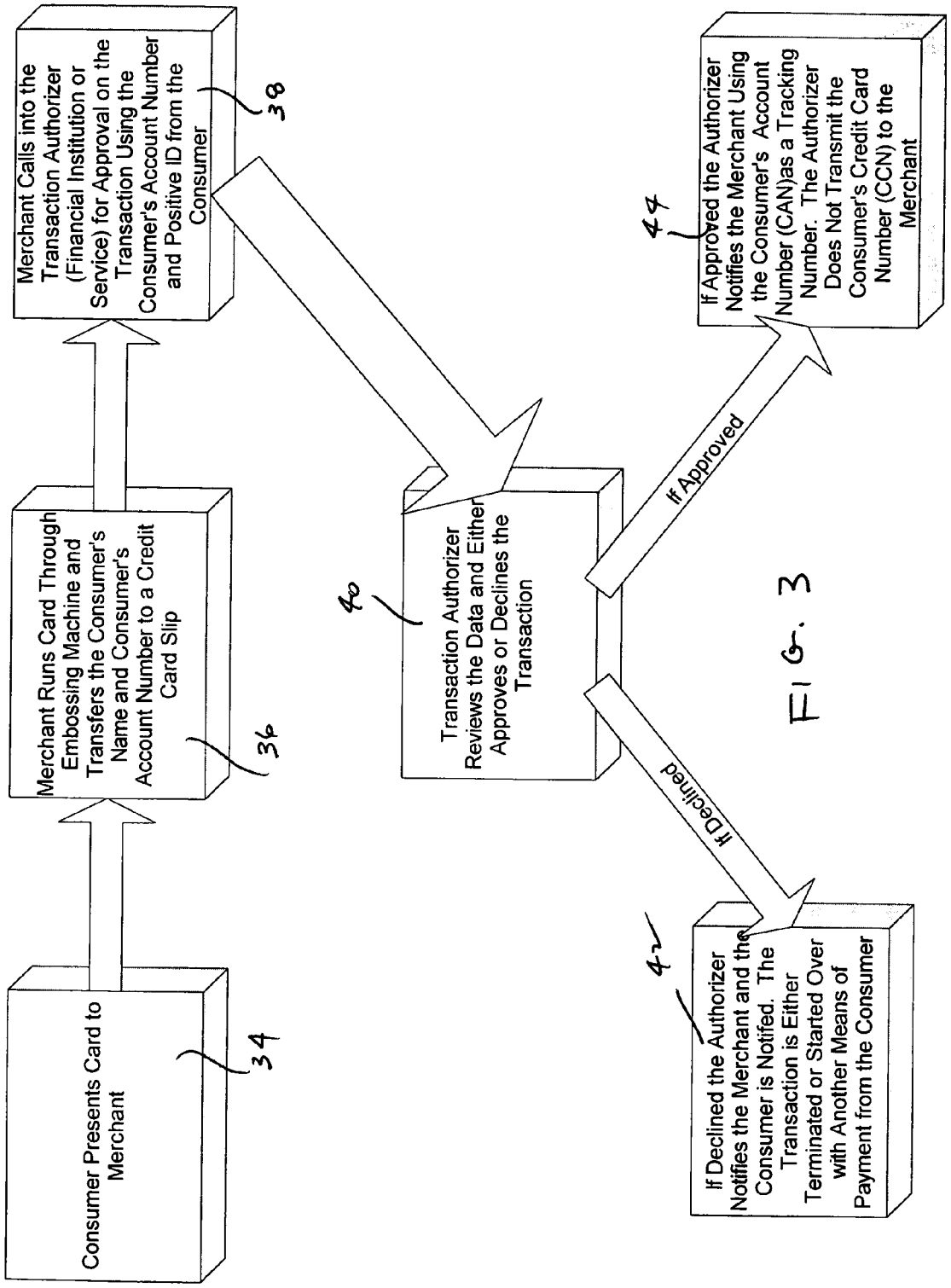

Consumer Presents Card to Merchant
34
Merchant Runs Card Through Embossing Machine and Transfers the Consumer's Name and Consumer's Account Number to a Credit Card Slip
36
Merchant Calls into the Transaction Authorizer (Financial Institution or Service) for Approval on the Transaction Using the Consumer's Account Number and Positive ID from the Consumer
38
Transaction Authorizer Reviews the Data and Either Approves or Declines the Transaction
40
If Declined
If Approved
If Declined the Authorizer Notifies the Merchant and the Consumer is Notified. The Transaction is Either Terminated or Started Over with Another Means of Payment from the Consumer
42
If Approved the Authorizer Notifies the Merchant Using the Consumer's Account Number (CAN)as a Tracking Number. The Authorizer Does Not Transmit the Consumer's Credit Card Number (CCN) to the Merchant
44

FIG. 3

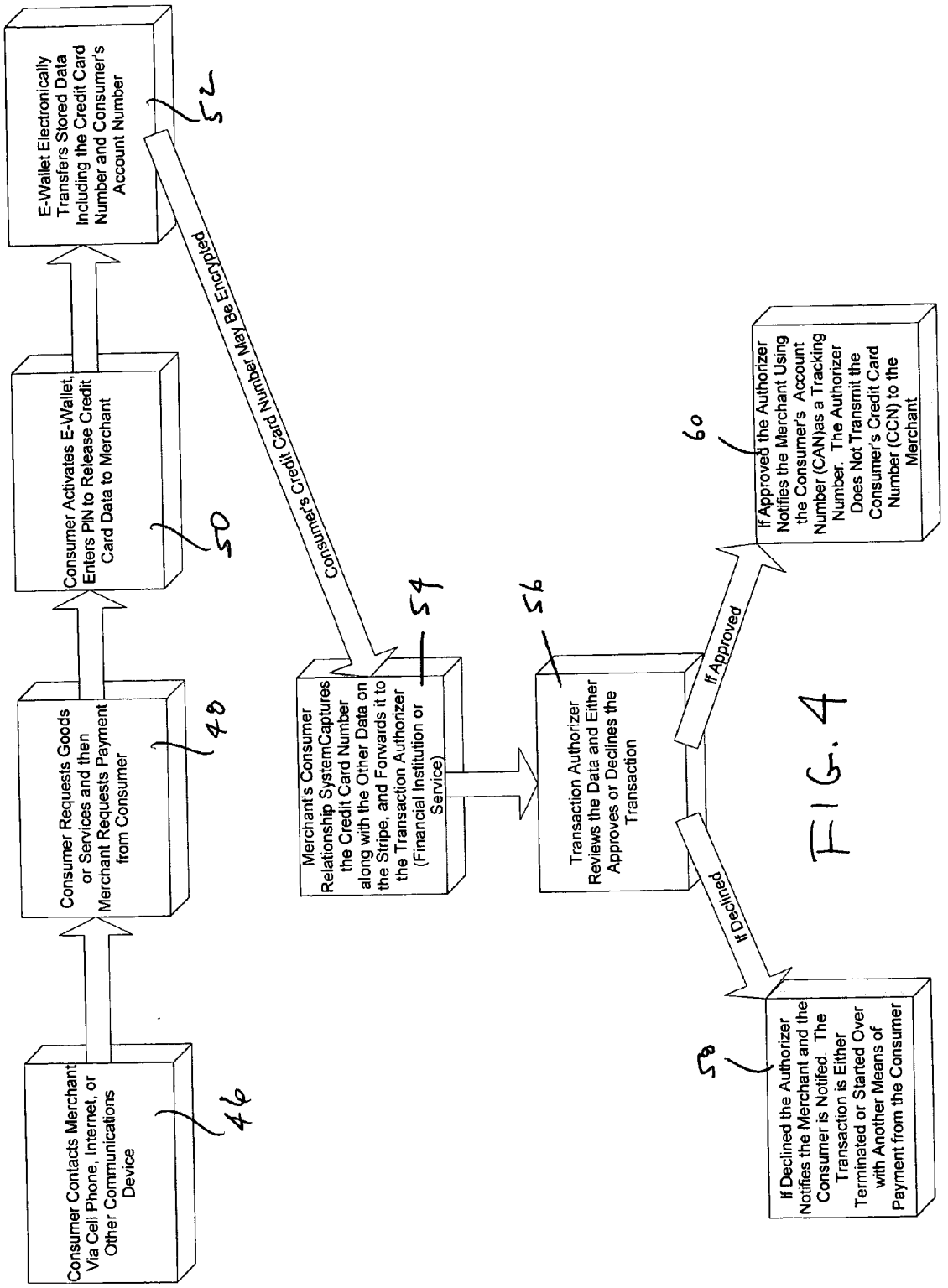

Consumer Contacts Merchant Via Cell Phone, Internet, or Other Communications Device
46
Consumer Requests Goods or Services and then Merchant Requests Payment from Consumer
48
Consumer Activates E-Wallet, Enters PIN to Release Credit Card Data to Merchant
50
E-Wallet Electronically Transfers Stored Data Including the Credit Card Number and Consumer's Account Number
52
Consumer's Credit Card Number May Be Encrypted
Merchant's Consumer Relationship SystemCaptures the Credit Card Number along with the Other Data on the Stripe, and Forwards it to the Transaction Authorizer (Financial Institution or Service)
54
Transaction Authorizer Reviews the Data and Either Approves or Declines the Transaction
56
If Approved
If Approved the Authorizer Notifies the Merchant Using the Consumer's Account Number (CAN)as a Tracking Number. The Authorizer Does Not Transmit the Consumer's Credit Card Number (CCN) to the Merchant
60
If Declined
If Declined the Authorizer Notifies the Merchant and the Consumer is Notifed. The Transaction is Either Terminated or Started Over with Another Means of Payment from the Consumer
58

FIG. 4

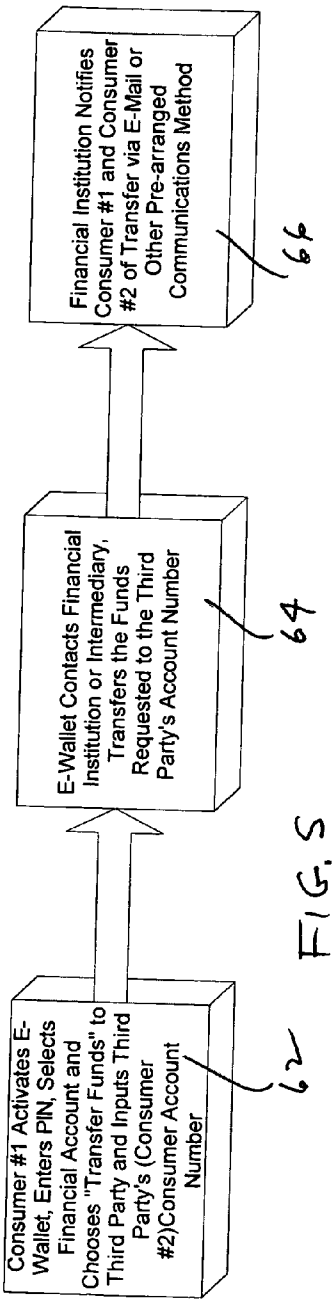

Consumer #1 Activates E-Wallet, Enters PIN, Selects Financial Account and Chooses "Transfer Funds" to Third Party and Inputs Third Party's (Consumer #2)Consumer Account Number
62
E-Wallet Contacts Financial Institution or Intermediary, Transfers the Funds Requested to the Third Party's Account Number
64
Financial Institution Notifies Consumer #1 and Consumer #2 of Transfer via E-Mail or Other Pre-arranged Communications Method
66

FIG. 5

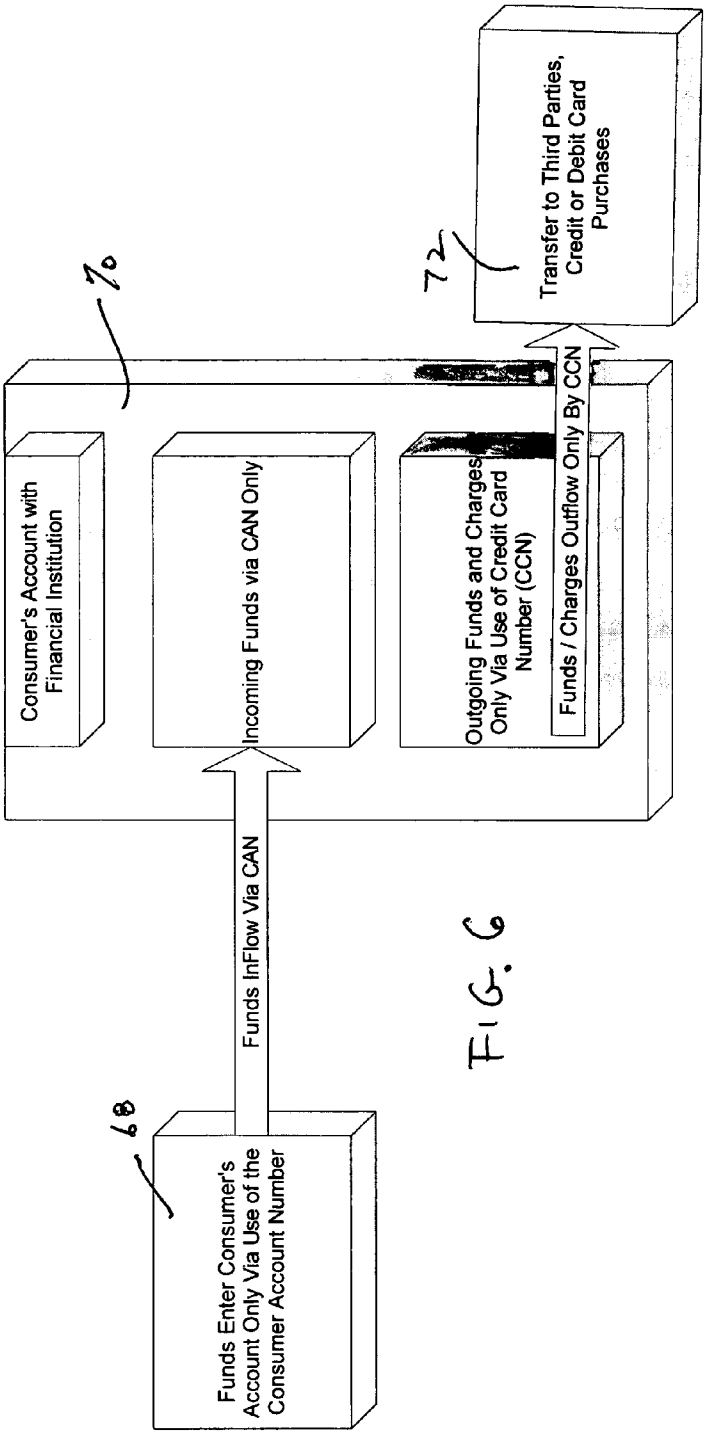

Funds Enter Consumer's Account Only Via Use of the Consumer Account Number
68
Funds InFlow Via CAN
Consumer's Account with Financial Institution
Incoming Funds via CAN Only
Outgoing Funds and Charges Only Via Use of Credit Card Number (CCN)
Funds / Charges Outflow Only By CCN
70
Transfer to Third Parties, Credit or Debit Card Purchases
72

FIG. 6

SYSTEM FOR INCREASING THE SECURITY OF CREDIT AND DEBIT CARDS TRANSACTIONS

TECHNICAL FIELD OF THE INVENTION

[0001] The present invention relates to a commercial transaction system, and more particularly to a system for allowing the use of credit or debit accounts while increasing the security of the transaction.

BACKGROUND OF THE INVENTION

[0002] Currently consumers who wish to use their credit or debit accounts must use a physical credit card or debit card and/or provide sensitive financial and personal data to a third party to initiate and complete the transaction. The consumer's account number and consumer credit card number are identical and are visible for theft by third parties or employees of third party merchants or financial institutions. As used herein, the term "card" will include both credit cards and debit cards.

[0003] Presently cards are constructed from plastic or polyvinyl chloride and contain a magnetic stripe on the back of the card. The cardholder's name is embossed on the front of the card along with the card's expiration date and the actual credit card number. The back of the card contains the magnetic stripe, a signature line, information on how to contact the card issuer and, possibly, the card number printed along with a three or four digit card verification number. The magnetic stripe may store up to three tracks of information, tracks one and two are typically read-only magnetic tracks, and track three is a read/write magnetic stripe. Tracks one and two have standard formatting as specified in the standard ISO/IEC 7813. Track three is formatted according to the standard ISO/IEC 4909.

[0004] Track one includes the information that is embossed on the front of the card, the account number, the cardholder's name and the expiration date of the card along with additional information such as the three digit service code (the first digit specifies the type of exchange permitted, the second digit specifies the authorization process required, and the third digit indicates the type of services available to the card), the country code possibly depending on the card number, and discretionary data. A check digit is included at the end of the first track as a verification of the data on track one.

[0005] Track two includes the same information as track one, excluding the cardholder's name and the discretionary data that is proprietary to the card issuer.

[0006] Track three includes the account number, sometimes the country code, and the card expiration date. Additionally track three may include up to two additional, subsidiary account numbers that may provide fallback authorization in case authorization is refused with the primary account. Track three has fields that may be updated, or written to by certain types of point of sale terminals. Track three thus offers the possibility of storing and updating financial parameters that control the cardholder's spending, or for control uses by the issuer.

[0007] Using the existing card methodology of having the same number for both the consumer account number and the consumer credit card number means that, in order to track a sales transaction, the merchant must store the consumer's credit card number. Recently there have been numerous publicized occurrences of merchants' consumer relationship management systems having been hacked by cyber thieves who have stolen consumer's credit card data. This potential for theft from the merchant increases the security risk, and liability, to both the consumer cardholder and the merchant.

[0008] In the case of a purchase that is completed verbally over a cell phone, fixed based telephone, IP phone or other means of verbal communication the consumer must orally relay his or her personal information in order to complete the purchase transaction. Transactions conducted over the Internet require the consumer to input the same information as required for a verbal order, which exposes the consumer to the possibility of the theft of the consumer's credit or debit card information and the consumer's personal data. Transactions where the card holder is not physically present are known as "card not present" or mail order/telephone order transactions. These types of transactions also include transactions that are conducted over the Internet.

[0009] Card Verification Value which is also known as CVC2 or Card Identification Number (CID) has been in use for over ten years. The system is basically a 3 digit or 4 digit number printed on the credit card separate from the actual credit card number and is not on the magnetic stripe. The merchant, whether via the Internet or telephone, asks for the number at the same time the card number is provided to the merchant. This number is then passed along to the verifying institution, which confirms that the card is in the presence of the cardholder. This method is subject to fraud, such as in the case of a criminal obtaining the credit card number may just as easily copy the verification number. When cards are swiped and thus stolen electronically then the verification number is copied at the time of the swiping and provided to whomever the card number is sold.

[0010] MasterCard's recent security enhancement, in response to consumer demand for greater security and privacy in card not present transactions, implemented a system MasterCard named "MasterCard SecureCode". This system requires that the consumer, in an Internet transaction, input a private code (that has been given to the consumer by the bank that issued the card) into a "pop-up" screen that appears on the merchant's web page when the consumer has notified the web page that the consumer has completed the order. The consumer then inputs his/her private code and the authentication value is then passed along to the issuing bank in the merchant's normal authorization process. Using the MasterCard SecureCode system thus eliminates the possibility of "one click" purchasing, requires that the merchant install a SecureCode compliant "plug-in" application on the merchant's web site, and still provides the merchant with the consumer's credit card and other personal data. This method, while improving security over the previously existing system, is cumbersome and does not accomplish the objective of keeping the consumer's card number and personal information hidden from the merchant and improve ease of use by the cardholder. This method does not allow for notification to the consumer of the purchase, nor does it add security or ease of use to transactions conducted verbally using a cell phone or land based telephone.

[0011] Visa's recent security solution is called "Verified by Visa" and using Three Domain security (3D or 3D-Secure), which operates by the cardholder inputting a personal iden-

tification number (PIN) into the merchant's web site when requested. This solution does not work on telephone sales (as the PIN would have to be verbally given to the merchant's call center employee) and is cumbersome to operate on the Internet.

[0012] The Verified by Visa process works in the following steps in an Internet transaction:

[0013] 1. The cardholder enters payment details using the merchant's web page.

[0014] 2. The cardholder is automatically directed to the card issuer's server, who generates a pop-up screen on the consumer's computer.

[0015] 3. The issuer authenticates the cardholder via the cardholder inputting his/her PIN number of password.

[0016] 4. The issuer then transmits to the cardholder a digitally signed approval, which is then retransmitted to the merchant's server to begin the normal credit approval process.

[0017] The normal credit approval process begins after the authentication process in order for the digital authorization from Visa to be included with the authorization request from the Merchant to Visa or, more likely, the authorization service for the card issuer.

[0018] Verified by Visa requires that the cardholder send the purchase authorization request from the consumer's computer to the merchant, who then sends the request to Visa's server, who then sends the request to the issuer's server. The issuer's server prompts for the password from the consumer, who then inputs the password or PIN, sends it to the issuer's server who then sends it to their (the issuer's) authentication server. The issuer's server then sends the approval to the consumer's computer who then passes the approval to the merchant's server. Then the merchant processes the payment for approval in the normal approval process and includes the authentication data along with the approval request to the card issuer for credit approval. Verified by Visa is cumbersome and will not work on telephone orders, and offers little compensation to consumers while taking more time to complete the transaction. Verified by Visa does not add the functionality of auto-filling forms on the Internet Merchant (or other merchants') customer relationship management systems, allow "one-click purchasing", ties up Visa, the merchant and the authorization entity's servers, increases communications between all of these servers, thus increasing the possibility of a communications error or drop, and still exposes the cardholder's data to theft.

[0019] Surrogate Card Numbers have been tried by American Express (Private Payments) and by MBNA (ShopSafe). The surrogate card number is basically a system where the consumer uses a software application to generate a one-time use credit card number that has a short validity period (normally two months or less) and a fixed charge value. The surrogate card number is tied to the consumer's "real" card number. This method is cumbersome (the consumer has to obtain the surrogate number and then keep track of it) and prevents the use of one click purchasing. Besides these issues, if surrogate numbers become widespread then, based on the current length of a credit card number (16 digits normally) there would soon be a shortage of numbers available. Of the 16 digits only 10 are available for actual account numbers as the other numbers designate the type of card, etc.

[0020] None of the above existing methods provide a solution that incorporates additional layers of security for both verbal and Internet transactions. Nor do any of the existing methods solve the combined problems of security, ease of use, and allow for one-click" purchasing. Nor do any of the existing methods improve the accuracy and speed of the remote sales type, mail order/telephone order, transaction. Several of the above methods require additional hardware to implement and many increase the volume of communications (and thus the possibility for information theft and communications break down).

[0021] Other proposed solutions require additional equipment, require that the transaction data be handled differently by either the consumer, the merchant or the financial institution and do not provide the increased security or speed of the sales transaction required by consumers.

[0022] Thus there exists a need for either a physical or virtual method of securing and enhancing credit and debit transactions, whether the transaction is conducted in person, on the Internet, over the telephone or via other communications methods available to the consumer.

SUMMARY OF THE INVENTION

[0023] In accordance with the present invention, a system for providing a secure method for storing and transmitting data required for a transaction between a consumer and merchant is made possible by the providing the consumer with both a consumer number, personal data and a credit or debit account number which may be encrypted. This information may be provided physically via a credit card type device, smart card type device and or virtually via the Internet, SMS text messaging, or other means of communicating with a consumer and his/her communications device. The present invention requires the issuance by the financial institution of two numbers, a credit card number and a related consumer account number.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] For a more complete understanding of the present invention and for further advantages thereof, reference is now made to the following Description of the Preferred Embodiments taken in conjunction with the accompanying Drawing in which:

[0025] **FIG. 1** is a block diagram of the present system;

[0026] **FIG. 2** is a block diagram illustrating a transaction process utilizing the present card at a point of sale terminal;

[0027] **FIG. 3** is a block diagram illustrating a transaction process utilizing the present card for use with a credit card slip;

[0028] **FIG. 4** is a block diagram illustrating a transaction process utilizing the present card in an electronic format;

[0029] **FIG. 5** is a block diagram illustrating the transfer of funds utilizing the present card in an electronic format; and

[0030] **FIG. 6** is a block diagram illustrating the transfer of funds utilizing the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0031] The present invention provides a substantial additional layer of security to remote sales type transactions and card present transactions while allowing the use of the current credit, debit and other financial instrument approval process. The present invention provides the consumer with, in the case of a physical credit or debit card, a card identical in size and shape to the current card, with the addition of an additional credit account number to the card's magnetic stripe. The present invention also provides for the existence of an electronic card wherein there may not be a physical card. In the case of a wholly electronic "card" the same information that is provided on a physical credit or debit card is sent via the Internet, SMS text messaging or other method of communication to the consumer's cell phone, desktop computer, PDA, or other communications device for secure storage in a resident electronic wallet.

[0032] The additional number in accordance with the present invention replaces the credit card number that is currently assigned to the consumer. The existing credit card number (or a new number, if so determined by the issuer or consumer) becomes the consumer's account number and will be visible on the surface of the card. This consumer account number will be used by the consumer when inquiring about his/her bill, making card payments, making application for credit, and other times when necessary to provide evidence of the account. The merchant will use the consumer account number to track the transaction and activity with the cardholder for product returns, warranty work and other normal consumer and merchant issues.

[0033] The additional credit card number, which may be encrypted, is stored on the back of the credit card in the magnetic stripe and is not disclosed to the consumer and is not visible on the surface of the card. In the example of the virtual card, the encrypted credit card number (CCN) is pushed to the consumer's communications device (computer, PDA, cell phone, etc.) and is stored for use. The stored data, which may include all of the data currently stored on today's credit card, is used for online and other types of transactions.

[0034] An additional benefit of having two separate but related numbers is that the consumer account number may be used as a reference by the consumer when paying the bill, inquiring about a particular transaction or when following up with the merchant. The merchant is able to use the consumer account number to track the transaction and the consumer without having to have access to the actual credit card number.

[0035] An additional benefit of having two separate but related numbers is that the consumer/cardholder may use the consumer account number to provide a third party the information to send the cardholder funds. Disclosing the consumer account number does not open the door to a thief to transfer funds out of the cardholder's account, as the only way to charge or debit the cardholder's account is by using the credit card number, which is unavailable to the third party. The inflow of funds, using the consumer account number is similar to a one-way trap door. Funds are allowed in via the consumer account number but are not allowed out by use of the consumer account number. The only way charges may be made or funds transferred out are by use of the credit card number. Thus the present invention meets the demand of cardholders to safely and securely transfer funds to or from third parties over the Internet. The only requirement is for both the sender and receiver to have a dual account number activated account and to provide the sender with the consumer account number.

[0036] The dual account number information is sent to the cardholder via the Internet, SMS text messaging, Wi-fi, Bluetooth, and other methods of communications available to the specific device the cardholder wishes to store the dual account number information on. Thus the cardholder may have his or her dual account number account information stored on the cardholder's cell phone, notebook computer, desktop computer, PDA, and any other device that is equipped to store this data. The cardholder may wish to have a physical card issued to him/her, but the physical card would not be necessary.

[0037] When the financial institution that issues the dual account numbers sends the information to the cardholder's device the financial institution may also send the cardholder's name, mailing address, telephone number, fax number, email and other contact information that the cardholder's electronic wallet will store along with the account information. This additional information may be released upon approval by the cardholder to a merchant in an online, telephone, or other type of transaction to facilitate the transaction and eliminate the need for the cardholder to either have to verbally provide the information, in the instance of a telephone sale, or to have to input the data in the example of an Internet sale.

[0038] Referring to **FIG. 1**, the present system is illustrated in which a card is issued by a financial institution. The financial institution creates a consumer account number and a related consumer credit card number for a consumer at block **10**. An electronic card is generated at block **12** including a separate consumer account number and a related consumer credit card number for the consumer. At block **14**, the financial institution may encrypt some or all of the data prior to sending the physical card or electronic card to the consumer. At block **16**, the physical card is issued and includes an embossed consumer account number and the second number, related to the embossed consumer account number, in the form of a number encoded on a magnetic stripe on the card. In the electronic card format, at block **18**, the financial institution issues the electronic card. At block **20**, the account information is stored on the consumer's communications device.

[0039] **FIG. 2** illustrates a transaction process utilizing the present card at a point of sale terminal. At block **22**, the consumer presents a card to a merchant. At block **24**, the merchant swipes the card through a point of sale terminal. At block **26**, the point of sale terminal captures the credit card number on the magnetic stripe and forwards this information to a transaction authorizer such as a financial institution or credit card service. At block **28**, the transaction authorizer reviews the data and either declines the transaction at block **30** or approves the transaction at block **32**. If approved, the authorizer notifies the merchant utilizing the consumer's account number as a tracking number, but does not transmit the consumer's credit card number, the second number, to the merchant.

[0040] Referring to **FIG. 3**, a transaction process utilizing a credit card slip is illustrated. At block **34**, the consumer

presents a card to the merchant. At block **36**, the merchant passes the card through an embossing machine and transfers the consumer's name and consumer's account number to a proper credit card slip. At block **38**, the merchant calls the transaction authorizer for approval of the transaction using the customer's account number and positive identification from the consumer. At block **40**, the transaction authorizer either declines or approves the transaction. The transaction is declined at block **42**. If the transaction is approved, at block **44**, the authorizer notifies the merchant using the consumer's account number as a tracking number. Again, the second number or consumer's credit card number is not passed on to the merchant.

[**0041**] Referring to **FIG. 4**, a process utilizing the present invention in the form of an electronic card is illustrated. At block **46**, the consumer contacts a merchant via an electronic communications device. At block **48**, the consumer requests goods or services from the merchant, and the merchant requests a form of payment. At block **50**, the consumer activates the electronic communications device such as, for example, an E-wallet and enters a personal identification number to release credit card data to the merchant. At block **52**, the electronically stored data including the credit card number and consumer's account number are transmitted to the merchant's consumer relationship system which captures the credit card number and consumer's account number. This information is forwarded to the transaction authorizer at block **56** which either declines at block **58** or approves at block **60** the transaction.

[**0042**] **FIG. 5** illustrates the steps in making a funds transfer utilizing the present invention. At block **62**, a consumer activates an E-wallet and chooses to transfer funds to a third party by entering the third party's consumer account number. The E-wallet contacts the financial institution and requests that funds be transferred to the third party's account number. The financial institution notifies at block **66** consumer number **1** and consumer number **2** of the transfer. In accordance with the present invention, neither consumer number **1**'s nor consumer number **2**'s credit card number is visible to either party.

[**0043**] **FIG. 6** illustrates the flow of funds during a transfer process utilizing the present card. At block **68**, funds enter a consumer's account using only the consumer account number. Funds flow into the financial institution at block **70** utilizing the consumer account number. Funds flow out of the financial institution at block **70** to be transferred to a third party at block **72** utilizing the consumer credit card number.

[**0044**] Other alteration and modification of the invention will likewise become apparent to those of ordinary skill in the art upon reading the present disclosure, and it is intended that the scope of the invention disclosed herein be limited only by the broadest interpretation of the appended claims to which the inventor is legally entitled.

1. A system for facilitating a commercial transaction by a consumer including:

a card, said card including a first number for identifying a financial account of the consumer; and

said card including a second number, related to said first number, for use in authorizing a transaction involving the financial account of the consumer.

2. The system of claim 1 wherein the first number is visible on said card and said second number is not visible.

3. The system of claim 1 wherein said card includes a magnetic storage media and said second number is stored on said magnetic storage media.

4. The system of claim 3 wherein said second number is encrypted.

5. A system for facilitating a commercial transaction by a consumer including:

an electronic storage device for use in the transaction, said storage device including a stored first number for identifying a financial account of the consumer; and

said storage device including a stored second number, related to said first number, for use in authorizing a transaction involving the financial account of the consumer.

6. The system of claim 5 wherein said second number is stored in an encrypted format.

* * * * *