SYSTEM AND METHOD FOR SECURE ELECTRONIC TRANSACTIONS

RELATED APPLICATIONS

This Application claims the priority of previously filed U.S. Provisional Patent Application No. 60/160,945 filed October 22, 1999, which is hereby incorporated by reference in its entirety; and U.S. Provisional Patent Application No. 60/204,439 filed May 15, 2000, also hereby incorporated by reference in its entirety

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a system and method which substitutes proxy transaction numbers for real credit card numbers and other financial account identifiers during electronic transactions. Further, by substituting proxy transaction numbers that can be used in an identical manner to conventional credit card numbers, a customer can conduct online transactions without ever exposing a genuine credit card number to misuse. As well, charges can be applied to financial accounts other than credit cards (i.e., debit cards and checking accounts), and transactions can be conducted via wireless devices.

2. Description of the Prior Art

Purchasing products from merchants who offer goods and services over the Internet is a rapidly expanding segment of the economy. Many consumers find it more convenient to browse the website of an online merchant and make product selections and purchases electronically than traveling to traditional retail establishments that often offer less attractive pricing and more limited product selection. Being quick to take advantage of this opportunity, many traditional brick and mortar retailers now operate online sites where a

full selection of products and services is offered to customers. Moreover, many retail establishments have been created exclusively for the purpose of selling products online.

Conventionally, to purchase a product from an online retailer, a customer points web browsing software to an address where a retailer's online "store" is located. The customer then browses the product selection displayed at the website and determines which products they wish to purchase. The retailers' website then presents the customer with an order form asking for the customer's name, address, payment information, etc. The customer fills out the order form, including their credit card number and submits the form to the retailer's website for processing. The retailer's website submits the credit card number offered by the client for authorization; and upon approval of the credit card ships the products or services offered to the customer at the address specified on the order form.

Many security risks arise as a result of the conventional method of making purchases over a public network such as the Internet. First, transmitting a credit card number over the internet makes it possible for anyone with access to the network to intercept, i.e., steal, the credit card number. Those who intercept the credit card numbers generally use them to make a series rapid, fraudulent charges against the credit card account. This results in a loss for the online merchant who pays a "loss fee" and an "administrative fee" for disputed purchases. Further, the consumers whose credit card information is stolen may have a liability (usually up to $50) for fraudulent charges applied to their account. The possibility of interception, therefore, causes many consumers to refrain making online transactions, to safeguard their credit card number. For this reason, online retailers lose potential customers.

Other consumers are concerned that even if their credit card number is not intercepted en route to an online merchant, the online merchant's website may be

susceptible to penetration by "hackers" who steal credit card data from a merchant's website and misuse it. A security breach of this nature can be devastating to an online retailer's reputation and can result in a dramatic decrease in the number of consumers who are willing to make purchases from that retailer's website.

Since many retailers require an authorized form of payment prior to shipping a product to a customer, those people who prefer to purchase using debit cards and checks are unable to make purchases from online retailers. The lack of online retailers who accept forms of payment other than credit and charge cards is problematic to potential purchasers in Europe and other areas of the world where purchases are usually made using debit cards, checks and cash, as opposed to the United States where most consumers rely on credit cards. Aside from the inconvenience this presents to potential customers, online merchants lose sales when they are unable to process transactions for otherwise able purchasers who do not possess a credit card.

In U.S. Patent No. 5,883,810 to Franklin et. al., a system and method is described which attempts to provide security for credit cards by substituting proxy transaction numbers for a customer's credit account number when making electronic transactions. The '810 patent first requires a customer to obtain a new credit card in the form of an electronic commerce card. The electronic commerce card exists only in a digital format and cannot be used in traditional brick and mortar retail establishments; as described, the customer never receives an actual credit card number. Once a consumer has applied for and been granted an electronic commerce card, purchases can be made from online retailers. The '810 patent discloses that to pay for goods and services using the electronic commerce card, the purchaser sends a request for a proxy number to a central server. The central server then generates the transaction number and associates it with the customer's real

credit card number. The proxy number is then sent to the customer who forwards it to the merchant. The merchant uses the proxy number to obtain a credit card authorization and to submit charges to the customer card's issuing bank as though the proxy number were a real credit card number.

While the '810 patent discloses a method of conducting online transactions which avoids sending a customer's actual credit card number over the internet, it does not provide an adequate solution to the problem associated with securing credit card numbers for those consumers who already possess credit cards they wish to use in online transactions. To many consumers, applying for and obtaining an additional credit card is undesirable. Moreover, obtaining a credit card that is useful for the limited exclusive purpose of conducting online transactions is particularly burdensome, due to the annual fees many credit card issuers charge to those people who primarily use their credit cards for day-to-day activities in conventional retail establishments and only purchase products from online retailers on an occasional basis.

The '810 patent only addresses the substitution of proxy transaction numbers for credit card account numbers that are in the conventional sixteen (16) digit format. Many debit cards have nineteen (19) digit account numbers and the number of digits in a checking account can vary based on the institution that created the account. The '810 patent, therefore, does not describe a system or method which can accommodate the needs of those persons which wish to make online purchases using debit or checking account numbers.

International patent publication WO 99/49424 to Flitcroft et al., describes a credit card system which generates limited use credit card numbers to reduce the potential for the interception of credit card numbers and their misuse. The system and method describe

within WO 99/49424 includes a central server which generates the limited use transaction numbers and distributes them to customers to use in online transactions. It is also described how a person lacking a credit card can purchase limited use transaction numbers to use in online transactions or be invoiced for charges which are incurred using the limited use transaction numbers. In order to reduce central server processing requirements, WO 99/49424 discloses that it is preferable to generate the limited use numbers in large batches and forward them to customers for use at a later time.

Alternately, persons without credit cards could purchase disposable credit cards with a credit limit equal to the purchase amount of the disposable card. The disposable credit cards would offer security by having a credit limit equal to the purchase amount of the disposable card. This method, however, offers less security than a conventional credit card which typically limits the risks to the customer to the first $50 of fraudulent purchases. The purchaser of a disposable credit card would risk losing the entire unused balance on the disposable card if the credit card number was stolen and misused.

It is, therefore, desirable to have a system and method which can generate transaction numbers which can be used as proxies for actual credit card number, for customers wishing to make online transactions using their preexisting credit cards, debit cards, or other financial accounts. Such a system should be able to generate the proxy transaction numbers while placing a minimum load on the central server, avoid the transmission of the customer's actual credit card number, and be able to process authorization requests and settlements in a manner which is seamlessly integrated into the current credit card system infrastructure and avoiding any participation on the part of merchants.

SUMMARY OF THE INVENTION

The present invention is directed toward a system and method which generates and substitutes transaction numbers for actual customer account numbers. The proxy numbers are generated within a client user interface located on a customer's computer and sent to a central server for activation and cross-referencing with a customer's financial account. Upon activation and cross-referencing of the proxy number, notification is sent to the client user interface, by the central server, indicating that the proxy number is available and has been reserved for use the customer.

To create the transaction number that the customer eventually sends to the merchant, in place of an actual credit card number, the client user interface must create a number that is in a format which is identical to a genuine credit card. To do this, the client user interface must create a 16 digit number that contains a BIN, or bank identification number, and a checksum. The BIN is usually the first 2 to 7 digits of the credit card number. The checksum digit is always the final digit of the credit card number. Accordingly, the proxy number generated by the client user interface should be from about 5 to 12 digits, to leave space for the BIN and checksum if the final transaction number is to be recognized in place of a credit card number. The system can, of course, be used to prepare transaction numbers which can be used as proxies for numbers other than credit cards and can even be used to provide proxy data for personal information and non-numerical sequences. Those skilled in the art will readily recognize the programming changes necessitated by a desire to provide proxies for information and numbers other than credit card data. For purposes of describing the invention, however, the specification will describe the generation of transaction numbers to be used as proxies for conventional credit

card numbers over the internet as an ongoing example with a non-exclusive summary of other methods of use of the invention provided at the conclusion of the written description.

Once the transaction number has been generated by the client, it is forwarded to a merchant to complete an online purchase for goods and services. The merchant, unaware that the credit card number received is a proxy for an actual credit card number, will forward the transaction number through current credit card association network routing systems, such as those operated by VISA™ and Mastercard™.

The current credit card association network routing system receives authorization requests from merchants and evaluates the BIN (specifically, the card association network uses packet switched routing that is blind to individual credit card numbers, as a whole, and reads only the BIN portion of the entire card number.). Based on the BIN, the credit card association network routers forward the authorization request to the card issuer corresponding the BIN (each issuer has at least one, and usually many more, unique BIN numbers associated with it.) The present invention contemplates the use of central servers having their own unique BINs, so that the credit card association network routers forward only proxy transaction numbers to the central servers. Non-proxy transaction numbers, i.e., real credit card numbers, are forwarded directly to the issuing bank or institution.

When the central server of the present invention receives a transaction number it determines the real customer account from a cross-reference database and forwards the real account number along with the transaction routing number (also synonymously referred to as the network identification number, retrieval reference number and transaction-ID) to the issuing bank's authorization server. The issuing bank's authorization server generates an authorization response based on the customer's real credit card number and forwards the response back to the central server. The central server then substitutes the transaction

number for the real credit card account number and transmits the authorization response back to the network address specified by the credit card association network router. By cross-referencing the transaction number received for authorization with the transaction-ID number, the central server ensures that the correct proxy transaction number is returned to a merchant who requests an authorization, in instances where the customer has multiple transaction numbers active.

After an online purchase has been completed, a merchant forwards the transaction number for settlement. During the settlement phase, charges applied to transaction numbers are cross-referenced with real customer account numbers and substituted therefor so that the issuing bank can properly generate statements to send to cardholders.

Since the central server places no restrictions on the format for actual credit card or financial account numbers, it is possible for customers to use debit card accounts (which typically includes nineteen (19) digits) or checking accounts to make purchases from online merchants that only accept credit card as a valid form of payment. Further, customers using wireless devices such as PDAs and cellular phones can purchase products from online retailers by having a proxy number generated which will associate the charges incurred thereon to their cellular or PDA online account.

Unlike prior art methods, the present system is not limited to the single use transaction numbers as taught by Franklin et al. in U.S. 5,883,810, or the limited use numbers taught in WO/9949424. The present system allows for the generation of transaction numbers which must be used in accordance with rules applied by the central server and the customer. This allows a customer to obtain, for example, a proxy transaction number to be used for a long-term subscription. The advantage to the customer is that they do not need to forward their actual credit card number to the subscription service and the

customer can place a limit on the number of billing cycles during which charges can be applied. Moreover, if the subscription, or other on-line service used by the purchaser, is penetrated by "hackers" and the credit card numbers stored on the system are stolen, the proxy transaction number could not be misused so as to incur liability to the issuer or the customer since most, if not all, transaction numbers will be limited to use by a single vendor, for specific amounts, or for any other criteria contemplated by the customer or the system administrator. An attempt to use a transaction number which does not fall within the criteria specified at the time of transaction number generation will not be authorized by the central server.

In another embodiment of the invention, transaction numbers are generated for use by customers who do not possess any credit card accounts. These customers have debit card accounts that require the use of a pin number to authorization purchases. Many merchants, especially those who operate online, are not equipped to handle transactions involving debit cards.

In order to provide a transaction number in place of a debit card account number the central server must associate the transaction number with a debit card account number and a debit card account pin number. When a merchant sends a request to authorization a purchase based on a transaction number that is a proxy for a debit card account, the central server cross-references the proxy number (which was used to generated the transaction number within the client user interface and cross referenced to the actual financial account by the central server at the time the proxy number was validated and reserved for use) to the debit card account number and pin number and forwards the actual customer data to the issuers authorization system. Provides that the customer has sufficient funds available to cover the amount of the purchase, the bank authorization server sends a positive reply to

the central server of the present invention. The central server then forwards the reply to the network address from which the authorization request was received.

Since online merchants who are not equipped to process debit card transactions do not have debit card financial accounts to which money can be immediately transferred from customers accounts, issuers who provided proxy transaction numbers for debit card account numbers create a transitory debit account into which fund are placed at the time an electronic transaction occurs using a transactions number. When a clearance file is received by the issuing bank or institution during what is called "settlement" the funds are transferred from the transitory debit account to the credit account of the merchant.

In another embodiment of the invention, transactions numbers are generated to allow wireless device users to purchase goods and services from online merchants. For this type of transaction, the central server uses a single master credit account number to associated with all transaction numbers generated. In addition, the central server also cross-references the transaction number with the wireless account number of the customer who purchased goods or services using a transaction numbers.

By associating the transaction number with the customer's wireless account number, the wireless service provider can provide a detailed statement of charges to each individual customer.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a diagram illustrating an electronic transaction system.

Figure 2 is a diagram illustrating a central server, a client computer, and an issuer computer and their relation to a credit card association network and merchant computer in an electronic transaction system.

Figure 3 depicts an electronic transaction system for a wireless device.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is directed toward an electronic transaction system in which proxy numbers are generated, formatted as transaction numbers and sent to merchants and processed as credit card numbers during electronic transactions. By only supplying a transaction number to a merchant over public network, such as the internet, a customer's actual credit card account, or other financial account number, is never exposed to interception which can lead to misuse and unauthorized charges being placed on the customer's account. To maximize the efficiency and overall acceptance of the disclosed electronic transaction system, it is preferable that in all instances the merchant is unaware that it is processing a transaction number and not a genuine credit card number. In this manner, no participation on the part of the merchant, i.e., such as installing specialized software or hardware, is necessary; and, therefore, the only requirement for successfully conducting electronic transactions using transaction numbers according to the present invention is for the customer to have the desire to shield a credit card from the exposure of using that card in online transactions.

In order for a customer to use the electronic transaction system of the present invention, a user account must first be established on a central server. With reference to Figure 1, a customer uses the client computer **20** to connect to the internet **10**. Using a web

browser installed on the client computer **20**, the customer contacts a website operated in conjunction with central server **50** via the internet or other public network **10**. To verify that the customer using the client computer **20** currently has an established financial account with the issuing bank or institution associated with the central server **50**, the website operating in connection the central server **50** will require a registration code be input by the customer operating the client computer **20**. The registration code can be sent from the issuing bank or institution to the customer in many ways: the registration code could be included in a monthly statement, sent by mail, or provided in any other manner that essentially ensures that the customer will receive the registration code. Within the customer database **54**, as shown in Figure 2, the registration code has previously been crossed referenced to the customer's actual financial account established with the issuing bank or institution.

For security reasons, the issuing bank or institution may deactivate registration numbers after a short period of time so that unauthorized persons do not use the registration codes to establish electronic transactions system accounts on the central server. Further, the website operating in connection with the central server **50** may also require the customer operating the client computer **20** to enter personal information submitted to the issuing bank or institution at the time the financial account was created. Such information could include mother's maiden name, date of birth, social security number, or other information normally collected by financial institutions to verify the identify of a customer.

Once the website operating in connection with the central server **50** has verified that the customer operating the client computer **20** has correctly entered a valid registration code and answered any questions that verify the identity of the customer, software modules are then downloaded from the central server **50** to the client computer **20** via the internet.

The software modules include a proxy number generator **28** and a client user interface **26**, as shown in Figure 2. A data file, not shown, which includes authorization and verification information and may also be encrypted can be sent to the client computer **20**. Alternately, the transaction number generator **28** and the client user interface **26** can be combined into a single software download and even operate as a single software program on the client computer **20**. To simplify the customer's experience when using the client computer **20**, the client user interface **26** and proxy number generator **28** can be seamlessly integrated as an applet, i.e., a computer program running within another program, operating within the web browser **24**.

Once the client user interface **26** and proxy number generator **28** are installed on the client computer **22**, the customer then uses a web browser **24** to reach a merchant's computer **32** via the internet. Referring back to Figure 1, the customer operating the client computer **20** is now able to use the electronic transaction system **100** to purchase goods and services from a merchant's website operated at the merchant computer **30** over the internet **10** without having exposed a genuine credit card account number, or other financial account number, to interception by unscrupulous persons who "eavesdrop" on communications between merchants and customers on the internet to intercept credit card account information and make unauthorized purchases.

Referring to Figure 2, a customer points the web browser **24** on the client computer **22** to a website operated on a merchant computer **32** which displays goods or services that the customer wishes to purchase. To complete the transaction between the customer and the merchant, the website operated at the merchant's computer **32** submits a purchase and order form to the customer via the web browser **24** on the client computer **22**. In the purchase and order form, personal information about the customer is requested such as a

name, shipping address, telephone number and payment information. In a preferred embodiment, the client user interface **26** will automatically recognize the order form submitted to the customer from the merchant computer **32** and will activate the proxy number generator **28** to initiate the generation of a proxy number. Alternately, if the client user interface **26** does not recognize the order form submitted from the merchant computer **32,** the customer can manually activate the client user interface **26** to begin the process of generating a proxy number. In either instance, once the client user interface **26** is active the customer will be prompted to enter authentication data such as a user identification number and password to verify that the customer operating the client computer **22** is authorized to conduct electronic transactions using the customer's credit card account or other financial account associated with the user account stored in the customer database **54** on the central server **52**.

Assuming the client user interface **26** has received proper authorization from the customer using the client computer **22**, the customer will then be asked to enter details regarding the nature of the transaction they wish to make. Such details may include the amount of the purchase, the identity of the merchant from which the purchase is to be made, whether the purchase is to be recurring in nature (such as a magazine subscription), etc. In one embodiment of the invention, this data is stored in the cache memory **25** of the client computer **22** and forms a set of transaction number usage limitations. The client user interface **26** then activates the proxy number generator **28** which generates a proxy number for the electronic transaction.

The client user interface **26** forwards the transaction number usage limitations and proxy number to the central server **52**. The central server **52** forwards the proxy number to the proxy number verifier and activator **57** to insure that the proposed proxy number is not

already in use. Provided that the proxy number is not already in use, the proxy number verifier and activator **57** sends a response to the client user interface **26** indicating that the proxy number has been verified and activated and can be used in an electronic transaction. The proxy number verifier and activator **57** records the proxy number in the proxy number database **58** as a proxy number transaction cross-reference. The proxy number transaction cross reference record includes the proxy number and the actual customer financial account number. Further, the transaction number usage limitations sent from the client user interface **26** to the central server **52** are stored in the transaction number usage limitations database **53** with a cross-reference record to the proxy number to which they correspond.

Having received confirmation that the proxy number generated by the proxy number generator **28** is available for use by the customer in an electronic transaction, the client user interface **26** appends to the beginning of the proxy number a bank identification number ("BIN") and completes the generation of the transaction number by generating a "checksum" and appending that to the end of the proxy number. Those skilled in the art will appreciate that the generation and use of checksum digits in credit card numbers is well known.

At this point, the transaction number has been created. Transaction numbers differ from the proxy number by the inclusion of the BIN and checksum and generally contains 16 digits (when they are to be used as proxies for credit cards) and are in a format which is indistinguishable, to a merchant, from a conventional credit card number.

Those skilled in the art will readily recognize that only minor programming changes are necessary to generate transaction numbers to simulate the numerical format of other types of numbers, such as social security numbers, telephone numbers, etc. As well, text strings can be simulated in the same manner as credit cards numbers, so that anonymous

data can be entered for people who wish to retain their privacy in electronic communications, while retaining the ability to allow authorized persons and entities to obtain a cross-referenced record containing the person's genuine data.

Depending on whether the purchase and order form submitted from the merchant computer **32** to the web browser **24** was recognized by the client user interface **26**, the transaction number will either be automatically inserted into the purchase and order form by the client user interface **26**, or is manually transferred into the appropriate field on the order form by the customer. The customer then submits the form to the merchant computer **32** for further processing.

In another embodiment of the invention, a server-based wallet can be used to fill in the purchase and order form for the user when asked by the merchant. As previously mentioned, certain websites are recognized by the client user interface **26** and some information is automatically entered when these websites are used by the customer to make purchases. To further enhance the user's experience, the server may also recognize the website where the customer wishes to make a purchase and intercept the purchase and order form before it reaches the user's web browser **24**. The server-based wallet of the present invention completes the purchase and order form for the user and returns it directly to the merchant with a transaction number.

The Authorization Process

Having received a transaction number, the merchant computer **32** will attempt to process the transaction number in the same manner it would process any conventional credit card number. The merchant computer **32** forwards the transaction number to the credit card association network (usually through an "acquirer" which is the bank or institution used by the merchant to process credit card transactions). The credit card

association network, i.e., the routing system for credit card transactions operated by major credit card companies such as MasterCard and Visa, then evaluates the BIN number which was appended to the proxy number by the client user interface **26**. Based on the BIN number, the credit card association forwards the authorization request to the appropriate server. In the preferred embodiment of the present invention, transaction numbers include a BIN number so that at no point in the process is it necessary to distinguish transaction numbers which are proxies for actual credit card numbers from genuine credit card account numbers. Based on the BIN number of the credit card included in the authorization request by the merchant computer **32**, the credit card association network **42** will forward any transaction numbers received to the central server **52** for authorization processing. Further, with each authorization request forwarded from the credit card association network **42** to the central server **52** a retrieval reference number, i.e., transaction-ID or network identification number, is included to identify the originator of the authorization request. In the ongoing example discussed herein, the retrieval reference number will correspond to the merchant computer **32**.

Having received an authorization request, the central server **52** will remove the BIN number and checksum from the transaction number received in the authorization request, reducing the transaction number to the original proxy number. The central server will then compare the proxy number to cross-referenced records stored in the proxy number database **58** to determine the actual financial account number for the customer using the transaction number. Further, the central server **52** will compare the proxy number with the records stored in the transaction number usage limitation database **53** to determine what transaction number usage limitations were specified in the transaction number request originated by the customer. If any data received by the central server **52** as part of the authorization request

from the merchant computer **32**, does not meet the limitations stored in the transaction number usage limitations database **53** for the transaction number that is the subject of the authorization request, the central server will generate a rejection response and forward it to the merchant computer **32**. This indicates to the merchant that the issuing bank or institution will not honor the charges for the requested credit transaction. In most circumstances, the merchant will refuse to deliver goods or services to the customer when the credit card transaction has been denied, or rejected, by the issuing bank or institution.

Some issuing banks or institutions may, in an alternate embodiment, nevertheless require transmitting the authorization request to their conventional authorization process, even in instances where the central server has determined that the transaction number submitted for authorization has not been used within the guidelines specified by the transaction number usage limitations. This is done prior to the central server **52** sending an authorization reply to the merchant computer **32** and may be done for accounting purposes or other reasons which the issuer decides are necessary to provide service to their customers or in instances where the issuer determines that they must issue the authorization rejections from their conventional authorization system.

The reasons why the central server **52** may send a rejection response to the merchant computer **32** can include factors such as where the merchant computer that requests the authorization response is not the merchant specified by the customer when the transaction number request was generated. Also, the purchase amount specified in the authorization request may exceed that which was specified by the customer at the time the transaction number request was made. If, for example, the proxy transaction number was intercepted by someone, other than the customer, who attempted to use it to purchase goods and services from a merchant other than that specified by the customer, the attempt would

be foiled by the safeguard imposed by the transaction number usage limitations of the present invention.

When the data received in the authorization request from the merchant computer **32** meets the requirements imposed by the transaction number usage limitations, the central server **52** substitutes the actual financial account information for the customer for the transaction number and forwards the authorization request to the issuing bank or institution's computer **62** where it is handled by the authorization processor **65**. Further, in conjunction with sending the authorization request to the issuer computer **62**, the central server **52** stores within its cache memory **55** a temporary cross-reference record relating the retrieval reference number of the authorization request and the transaction number.

When the authorization processor **65** in the issuer's computer **62** has generated an authorization response, the authorization response is sent to the central computer **52** where the retrieval reference number is again cross-referenced with the correct transaction number and is substituted for the actual customer financial account number in the authorization response. The central server **52** then forwards the authorization response to the network address specified within the retrieval reference number, i.e., the electronic address, specified in the authorization request, so that it is received by the merchant computer **32**. By cross referencing the proxy transaction number in an authorization request with the retrieval reference number of the merchant computer which generates the authorization request, the central server **52** insures that the correct transaction number is associated with the correct authorization response in instances where the customer has multiple transaction numbers active at a given time.

In the situation where the actual financial account information stored in the financial account database **59** relates to a debit card or other financial account the customer

holds with the issuing bank or institution other than an actual credit card, it is necessary to transfer the funds out of the customer's financial account immediately upon completing the transaction. In this embodiment of the invention, the electronic transaction system allows customers with debit cards or checking accounts to conduct transactions with online merchants who otherwise only accept credit cards as an acceptable form of payment. Such online merchants generally do not have debit accounts where they can immediately receive funds transferred from a customer's checking or debit card account. To overcome this problem, the present invention contemplates the use of a transitory debit account to which the funds from the customer's checking or debit account are transferred immediately upon completion of the electronic transaction. The function of the transitory debit account is simply to store funds until the merchant's acquiring bank or institution requests that the funds be transferred during the settlement, or clearance, process.

At the end of each business day, in one embodiment of the invention, the funds are transferred to a transitory credit account and, therefrom, disbursed to merchants during the settlement process. The function of the transitory credit account is to act as an intermediary account between the transitory debit account and a merchant's actual credit account, since it is not possible to transfer funds directly between a debit account and a credit account.

Provided that the merchant computer **32** receives a positive authorization response, i.e., or an approval, from the central server **52**, the merchant computer **32** releases the goods or services for shipment to the customer.

The Settlement Process

The settlement process is the phase of the electronic transaction system wherein funds are dispersed by the issuing bank or institution to a merchant via the merchant's acquirer, i.e., the bank or institution which handles the credit card transactions processed by

the merchant. In the continuing example, the acquiring bank associated with the merchant computer **32** prepares a "clearance file" containing an entry for each credit card transaction processed by the merchant computer for each issuing bank or institution. Since each transaction number used in accordance with the present invention contains a BIN number unique to the central server that verifies and activates it, an individual clearance file can be generated which details only the transactions conducted using transaction numbers. The acquiring bank associated with the merchant computer **32** forwards the clearance file to the central server **52** through the card association network as a result of the central server **52** being identified by the card association network by its unique BIN, i.e., for all practical purposes the central server is viewed by the card association network as an independent issuer.

The central server **52** passes the clearance file and removes from each transaction number the BIN and checksum digits. The remaining portion of the transaction number, i.e., the proxy number, is cross referenced against the record stored in the proxy number database **58** and financial account database **59**. A new clearance file is created in which the customer's financial account number is substituted for the proxy number and includes the rest of the transaction information from the clearance file. In a preferred embodiment of the invention, a flag, or identifier, is placed in each record in the clearance file to identify to the issuing computer that each of the listed transactions was conducted using a transaction number. This can assist the issuing bank or institution's customer service department to quickly identify those situations in which an inquiry is received that is identified by a transaction number. The clearance file is then forwarded to the issuer's payment processor **63** and processed according to the issuing bank or institution's conventional practices. To further aid the customer service system, the clearance file may, as the flag, include the

retrieval reference number associated with the transaction as a cross-reference identifier. Since the retrieval reference number will be unique to each credit card transaction processed by online merchants, this method of cross referencing avoids any ambiguity which could arise when transaction numbers are cross-referenced against customer's actual financial account numbers in instances where a customer has multiple transaction numbers active at a given time.

This ambiguity would primarily arise when the cross reference attempts to determine a transaction number from a customer's actual financial account number when multiple transaction numbers exist and have been related to a single financial account number. U.S. Patent No. 5,883,810, discloses the cross-referencing of transaction numbers directly to actual financial account numbers without resolving how a transaction number could be determined from a financial account number when multiple transaction numbers are active.

The Adjustments Phase

After a transaction has been completed between a customer and an online merchant, it is possible that either one of the parties involved may dispute or disagree with some aspect of the transaction. In the case of a merchant who attempts to partially or fully cancel a transaction, i.e., for example where the goods or services are unavailable for shipment and money must be refunded to the customer, it is called a reversal. Under the present invention, if a merchant attempts to fully or partially cancel a transaction they are likely to send the retrieval reference number included in the original authorization request with the transaction number via the card association network to the central server **52**. If a significant period of time has passed, the central server may have deactivated or reissued the transaction number for reuse. In the preferred embodiment of the invention, however,

the transaction number is not issued for reuse for a period of at least six months from its original deactivation (deactivation occurs after the first authorization of a transaction number unless the transaction number usage limitations specified by the customer at the time the transaction number is requested specify that the transaction number is to be used more than once, as is the case in a recurring magazine subscription.)

To insure that customers always receive refunds offered by merchants, the preferred embodiment of the present invention allows for the authorization of reversals in all instances. Further, if the transaction number included in the reversal request had previously been deactivated, it may be reactivated to allow for an additional transaction to occur using that transaction number. For example, in the situation where a customer orders particular goods or services from a merchant and that merchant obtains an authorization for a single use limited transaction number, the transaction number will be deactivated and can not be authorized if another authorization request is received using that transaction number. If the goods or services which the customer requested are unavailable, however, many times the merchant will cancel the original order and attempt to authorize a second transaction using the original transaction number (for substitute goods selected by the customer.) Under the present system and method, if the merchant cancels the original transaction, the original transaction number will be reactivated and authorized for one more transaction. This feature of the present invention helps make the system and method taught herein much more transparent to online merchants than prior art methods such as that taught in U.S. Patent No. 5,883,810, to Franklin, et al. which does not contemplate or disclose any method for handling charge back or reversal situations.

Another situation which may arise, the chargeback, is where the card holder has disputed charges relating to a particular transaction number. This can arise where the

customer has received defective goods, didn't get the product they requested, or finds unauthorized charges have been applied to their account. Using the original retrieval reference number received with the authorization request from the online merchant, the present system permits using the original clearance file to locate the proxy number used in the disputed transaction. The transaction number is regenerated by appending thereto the BIN of the central server **52** prior to the first digit of the proxy number and the checksum after the last digit of the proxy number to recreate the 16 digit transaction number used by the merchant. The remainder of the chargeback process is handled according to each issuing bank or institution's existing procedures.

Wireless Transactions

Figure 3 depicts a wireless device **70** connected to a wireless service provider **80**. The wireless service provider **80** allows the user of the wireless device **70** to connect to the internet or other public network **12** and to browse the product selection of online merchants through a server which may be operated by the merchant's computer **34**. Should the user of the wireless device **70** decide to purchase a product offered at the merchant's website on the merchant computer **34** the electronic transaction system of the present invention can be used with only slight modifications to the embodiment contemplated for use in conventional credit card transaction.

To accommodate wireless communications, the wireless service provider **80** establishes a user account on the central server **90** with a master credit account. All charges applied to transaction numbers used for transaction conducted via wireless device are applied to the credit account of the wireless service provider **80**. In this example of the present system and method, once the user of the wireless device **70** has chosen goods or services to purchase via the website operating on the merchant computer **34**, the user of the

wireless device **70** indicates through electronic means that they wish to purchase a particular product. When the website operating on the merchant computer **34** forwards the purchase and order form to the user of the wireless device **70** via the wireless service provider **80** the form is intercepted by the wireless service provider and, in one embodiment of the invention, the relevant information for the customer is provided by the wireless service provider; and, in another embodiment, the form is forwarded to the central server **90** to be completed. For each wireless transaction initiated by the customer using the wireless device **70**, the wireless service provider requests a transaction number be generated by the central server **90** and associated with the wireless account number, e.g., customer's telephone number or other identifier, and used to cross-reference the transaction number generated by the central server and the customer ordering the goods or services. In an alternate embodiment of the invention, a proxy number is generated by the wireless service provider and sent to the central server **90** to be cross referenced against the account number of the user of the wireless device **70**. In this embodiment the central server verifies and activates the proxy number in the same manner as discussed in relation to conventional credit card transactions. Once verified and activated, the central server **90** will cross reference the proxy number to the account number of the user of the wireless device **70** and respond to the wireless service provider **80** to indicate that the proposed proxy number has been activated for use. The wireless service provider **80** will then generate a transaction number by appending to the proxy number a BIN, prior to the first digits of the proxy number, and by appending a checksum digit after the last digit of the proxy number. The wireless service provider **80** then forwards the transaction number via the internet **12**, or other public network, to the merchant computer **34** for further processing.

To authorize the transaction using the transaction number submitted by the wireless service provider **80**, the merchant computer **34** prepares an authorization request and forwards it to the card association network **44** which then routes the request to the central server **90** based on the BIN included in the transaction number. In the case of wireless device transactions, a unique BIN may be used for each wireless service provider to avoid the necessity of cross referencing between the transaction number and the actual customer account number during the authorization process. Accordingly, each time the central server **90** receives an authorization request from the credit card association network **44**, the account number of the wireless service provider **80** is substituted for the transaction number in the authorization request, and the authorization request is forwarded to the issuing bank or institution's computer to be handled by their conventional authorization process. Further, the central server **90** will cross-reference the transaction number received in the authorization request with the retrieval reference number contained in the authorization request, so that the central server **90** can properly route the authorization reply when it is received from the issuer computer **62**.

When the central server **90** receives the authorization reply from the issuer computer **62**, the account number of the wireless service provider **80** is substituted for with the transaction number included with the authorization request. To obtain the original transaction number, the central server cross references the retrieval reference number included in the authorization response from the issuer computer **62** to obtain the correct transaction number. The authorization response is then forwarded by the central server via the card association network **44** to the merchant's computer **34** containing the correct transaction number.

The remainder of the wireless method functions in substantially the same manner as that previously described. However, an additional step in the settlement process is necessary in order to allow the wireless service provider **80** to properly reflect charges incurred by the user of the wireless device **70** and apply the charges to the monthly statement sent from the wireless service provider **80** to the user of the wireless device **70**.

The additional step is to create a unique clearance file specific for the wireless service provider **80** by the central computer **90**. When the central server **90** receives the clearance file for the BIN associated with the central server **90** from the credit card association network **44**, the unique clearance file is generated by cross referencing each transaction number in the clearance file received from the card association network and substituting therefore the account number of the user of the wireless device **70** from which the request for each transaction number was initiated. The unique clearance file is then forwarded to the wireless service provider **80** and the information stored therein is used to apply charges to the account of the user of the wireless device **70**.

Person to Person Transactions

In many instances, people are conducting credit card transactions among individuals in day-to-day commerce. In another embodiment of the present invention, a person to person server is established that allows individuals to use transaction numbers to send money to one another for such things as purchases made in online auctions.

When a person wishes to send money directly to another person, one way of transferring funds between them can occur if the first person requests a transaction number with a usage limitation specifying the amount of money they want to give to the second person. By way of example, we assume that amount if $1000. The first person establishes a transaction number usage limitation of $1000 for the transaction number they request.

The person to person server then generates a transaction number (or alternately a proxy number is generated by the customer's client user interface and forwarded to the server for validation, activation, and cross-referencing with the customer's credit or financial account number and the transaction number is generated within the customer's client user interface software.)

The first person then forwards the transaction number to the second person as either payment for goods or services or, merely, as a gift. The second person can use the transaction number as a prepaid credit card until the credit limit is met, at which time the transaction number will no longer be authorized by the person to person server. Unlike a conventional payment process or gift certificate, however, the present invention contemplates that the first person's credit card is not charged for the amount of money sent to the second person until the second person actually uses the transaction number to obtain goods or services. A benefit of the present invention is, also, that since the second person receives an transaction number in the form which is indistinguishable from a conventional credit card number, the transaction number can be used for any type of transaction where the physical, plastic credit card is not required (such as for telephone orders, etc.)

In another embodiment of the invention, which also includes the first person having a merchant's credit account, allows the first person to send money to a second person by issuing a reversal to the second person's credit card. This is done by the second person requesting the generation of a transaction number by the disclosed means and sending it to the first person. The first person issues a reversal, as previously described. As a result of the reversal, the second person's credit card receives funds from the first person which can be spent, used to satisfy the credit account's current balance, or used to obtain cash.

Finally, the present system and method provides the ability for parents, or other primary credit account holders to provide their children or corporations to provide their employees with credit card accounts that are proxies for a single, master account. In this embodiment, multiple user ID's and passwords are provided to a user to allow that user to generate transaction number requests relating to the same credit account which are each linked to a separate user account. Each user can have transaction number usage limitations automatically applied to each of their transaction number requests which were specified by the master account holder at the time the individual user account was created. In this manner, a parent could specify the maximum total expenditures a child could make or an employer could give a credit card to an employee that can only be used for purchases from specified merchants. Such a system is far superior to current methods where an employer may grant actual credit cards to their employees and have to face situations where employees use them irresponsibly or for personal use.

Although online electronic transactions have been described throughout the examples and description of the invention. Those skilled in the art will readily recognize the similarity between online transactions and any other credit card based transaction that occurs without the need for a physical credit card to be present, e.g., over the telephone. The present system can be applied to such situations and only requires the customer to use their personal computer to obtain the transactions number. In the event that the person wishes to use the transaction number offline, they simply supply the offline merchant with the transaction number. The remainder of the credit card processing system functions as previously described.

Although the invention has been described with respect to specific features, structure, and process elements, it is to be understood that the appended claims defined the disclosed invention without limitation to the specific features, steps, or structure described.

CLAIMS

We Claim:

1. A method for conducting credit card transactions comprising:

generating a proxy number in a client user interface software to be used in place of a credit card number in a transaction;

associating said proxy number with a financial account number;

generating a transaction number which comprises a BIN, a proxy number and a checksum digit; and

transmitting said transaction number to a merchant in place of an actual credit card number.

2. The method of Claim 1 wherein said transaction number is in an identical format to a conventional credit card number.

3. The method of Claim 1 wherein said transaction number has sixteen digits.

4. The method of Claim 1 wherein said customer financial account is a credit card.

5. The method of Claim 1 wherein said customer financial account is a debit card.

6. The method of Claim 5 wherein said debit card has greater than sixteen digits.

7. The method of Claim 1 wherein said financial account is a master credit card account.

8. The method of Claim 7 further comprising the step of associating said master financial account with an individual customer account.

9. The method of Claim 8 wherein said individual customer account is a wireless account number.

10. A method for authorizing a proxy transaction number used in an electronic transaction comprising:

receiving at a central server an authorization request for a transaction number from a card association network, wherein said authorization request includes a retrieval reference number;

associating said transaction number with said retrieval reference number;

generating an authorization reply in response to said authorization request;

transmitting said authorization reply to an address identified by said retrieval reference number.

11. A method of conducting an electronic transaction from a wireless device comprising:

generating a proxy number;

generating a transaction number comprising said proxy number, wherein said transaction number has 16 digits

associating said transaction number with the customer account number of said wireless device; and

transmitting said transaction number to a merchant in place of a credit card number.

12. A method of generating a proxy transaction number comprising:

generating a proxy transaction number having from five to ten digits;

appending to said proxy number, prior to the first digit in said proxy number, a bank identification number having from four to ten digits; and

appending after the last digit of said proxy transaction number a checksum digit.

13. A method of cross referencing a proxy transaction number to a customer financial account comprising:

generating a proxy number having from five to ten digits;

creating a record in a cross reference database having first and second data fields;

inserting into said first data field said proxy transaction number; and

inserting into said second data field a customer's actual financial account number,

wherein said first data field and said second data field have an unequal number of digits and are related for cross referencing.

14. A method for controlling the usage of a proxy transaction number comprising:

generating a transaction number;

creating a record in a transaction number usage limitations database having at least one field for storing said proxy transaction numbers and having at least one date field for storing a transaction number usage limitation.

15. The method according to Claim 14 wherein said transaction number usage limitation is a single use.

16. The method of claim 14 wherein said transaction number usage limitation is a specific merchant identifier.

17. The method of Claim 14 wherein said transaction number usage limitation is a maximum purchase amount.

18. A method of authorizing a proxy transaction number comprising:

receiving at a central server a request to authorize a transaction number;

retrieving from a transaction number usage limitation database a record containing at least one transaction number usage limitation which refers to said transaction number;

comparing said transaction number usage limitation to said authorization request; and

determining whether said authorization request falls within the limitations contained in the transaction number usage limitation.

19. The method according to Claim 18 further comprising sending a negative authorization response to a merchant if said authorization request does not meet said transaction number usage limitation.

20. The method according to Claim 19 further comprising forwarding said authorization requests to an issuer's authorization system when the authorization request meets said transaction number usage limitation.

21. A method of substituting a transaction number to be used in place of a debit card number comprising:

generating a transaction number having a format identical to a conventional credit card number;

associating said transaction number with a customer debit account number and debit account PIN number;

submitting said transaction number to a merchant in connection with the purchase of goods and services;

receiving from said merchant an authorization request for said proxy transaction number;

determining whether the amount of funds available in said customer debit card account exceed the purchase amount specified in said authorization request;

in the event where the funds available in said customer debit card account exceed said purchase amount specified in said authorization request, performing the following:

transferring from said customer debit card account to a transitory debit account an amount of money equal to said purchase amount specified in said authorization request.