System And Method For The Prevention Of Unauthorized Transactions Using Common Payment Instruments Over A Public Network

Field of the Invention

This invention relates generally to a system and method for facilitating electronic commerce over a public network (such as the Internet, a wireless telecommunication network or an Interactive TV/Cable Network) using common payment instruments such as credit cards and debit cards. More particularly, this invention relates to a system and method for the prevention of unauthorized transactions using such payment instruments over the public network, and to facilitating electronic commerce using such network.

Background of the Invention

Transactions online, or what is generally referred to as electronic or "e"-commerce, have increased in recent years. With the increase in consumer-oriented sites created by merchants on the World Wide Web (or simply "www"), consumers can access such sites and shop for goods and services by browsing catalogs, selecting a product, placing orders and making the necessary payment, all electronically over the Internet.

A common mode of payment for purchases is the use of credit cards. In an online transaction, the consumer is expected to enter into the order form personal data such as their name, address, telephone number, and credit card information, for example account number and expiry date.

This information is transmitted to the merchant over the Internet. The merchant then verifies whether the credit card number is valid and that the payment amount can be charged. The card verification is usually done with a well-established card network, such as the VisaNet™ network.

As the credit card information is transmitted via the Internet, there is concern over the lack of security in the online transaction. Such information can be intercepted

en route, copied into a database, and used for unauthorized transactions. There have been incidents of hackers breaking into a merchant's credit card information database. The credit card information may be passed on to any person who may use it to conduct online transactions long before the unauthorized use is discovered. The development of a secure online system of payment will reduce or eliminate the incidence of theft of credit card information for unauthorized use.

There are existing well-established systems that verify credit card purchases and settle accounts. These systems and associated protocols are entrenched in the merchant and banking communities and experience a high level of acceptance and trust. A new online payment model should integrate and compliment these systems.

US patent 5,883,810 to Franklin et al discloses a system to secure credit card information. Upon request from a buyer, the system issues a proxy number to the buyer for use in an online transaction. The buyer sends the proxy number to a merchant in place of the credit card number. The merchant processes the proxy number in the same manner as the credit card number and seeks authorization for the transaction. While authorizing the transaction, the system substitutes the real credit card number for the proxy number. An authorization message is then sent to the merchant using the proxy number. This system provides some security, in that it offers a facility for buyers to use proxy numbers and avoid providing their credit card information over the Internet. However, it does not address the unauthorized use of credit card information if the credit card information is obtained form other sources.

International patent specification WO 00/16219 discloses a method for the detection of fraudulent transactions. Authorized users of payment instruments and merchants register with an authorization agent. Registered merchants seek approval from the authorization agent as a part of the transaction process. The authorization agent notifies the authorized user of the payment instrument of all activity from registered merchants. The authorized user can then notify the authorization agent of any fraudulent activity, which is then reported to the merchant. One disadvantage of this system is that it requires that the merchant

be registered in order to be effective. Thus, fraudulent use of the payment instrument is still possible with merchants that are not registered.

The inventor has developed a secure payment system that improves security and integrates with existing verification and settlement systems including the existing credit card verification and settlement systems.

Summary of the Invention

In accordance with a first aspect of this invention, there is provided a method for preventing unauthorized transactions over a telecommunications network among a merchant, a buyer who will make a purchase from the merchant using a payment instrument, and an authorization agent that is at least partly responsible for providing authorizations regarding the payment instrument, comprising the steps of:

an authorised user of the payment instrument registering the payment instrument with a validation agent;

the authorization agent registering with the validation agent;

an authorised user of the payment instrument submitting a transaction window request to the validation agent concerning a proposed transaction using the payment instrument;

the buyer making a purchase from the merchant, including providing the merchant with payment instrument identification information during said purchase;

the authorization agent receiving a request that originated from the merchant to provide authorization that the payment instrument is able to honour the transaction to the merchant, and determining from said request whether the transaction was provided over the telecommunications network; and

if said authorization agent determines that said transaction was performed over said telecommunications network, said authorization agent then determines from

the validation agent whether said transaction satisfies the criteria of at least one transaction window for that payment instrument, and if all such criteria are not met for any of said transactions windows, rejecting the transaction.

Preferably, the step of registering the payment instrument with a validation agent comprises the validation agent receiving registration information regarding the payment instrument, said registration information including verification information regarding the authorized user of the payment instrument.

Preferably, said step of submitting a transaction window request to the validation agent includes the step of the validation agent validating the transaction window request using the verification information, whereby said transaction window request is disregarded if said validation is not correct.

Preferably, said criteria includes a transaction window duration, after which the transaction window expires.

Preferably, said criteria include the identity of the merchant.

Preferably, said criteria include a transaction value.

Preferably, said criteria include a transaction value range.

Preferably, said criteria includes repeat transaction period data, specifying a period after which the transaction window again becomes valid.

Preferably, said validation agent provides the authorization agent with access to validated transaction windows from authorized users of payment instruments relating to that authorization agent, and said step of the authorization agent determining from the validation agent whether said transaction satisfies the criteria of at least one transaction window comprises the authorization agent performing said determination by directly accessing the transaction windows.

Preferably, said authorization agent comprises the issuing institution of the payment instrument.

Preferably, said authorization agent comprises a credit card association responsible for the payment instrument.

In accordance with a second aspect of this invention, there is provided computer software, embodied on a computer-readable medium that, when executed on an authorization agent's computer and a validation agent's computer executes method steps for preventing unauthorized transactions over a telecommunications network among a merchant, a buyer who will make a purchase from the merchant using a payment instrument, and an authorization agent that is at least partly responsible for providing authorizations regarding the payment instrument, the method steps comprising:

registering an authorised user of the payment instrument with the validation agent;

registering the authorization agent with the validation agent;

the validation agent receiving a transaction window request from the authorised user of the payment instrument concerning a proposed transaction using the payment instrument;

the buyer making a purchase from the merchant, including providing the merchant with payment instrument identification information during said purchase;

the authorization agent receiving a request that originated from the merchant to provide authorization that the payment instrument is able to honour the transaction to the merchant, and determining from said request whether the transaction was provided over the telecommunications network; and

if said authorization agent determines that said transaction was performed over said telecommunications network, said authorization agent then determines from the validation agent whether said transaction satisfies the criteria of at least one transaction window for that payment instrument, and if all such criteria are not met for any of said transactions windows, rejecting the transaction.

Preferably, the step of registering the payment instrument with a validation agent comprises the validation agent receiving registration information regarding the payment instrument, said registration information including verification information regarding the authorized user of the payment instrument.

Preferably, said step of submitting a transaction window request to the validation agent includes the step of the validation agent validating the transaction window request using the verification information, whereby said transaction window request is disregarded if said validation is not correct.

Preferably, said criteria includes a transaction window duration, after which the transaction window expires.

Preferably, said criteria include the identity of the merchant.

Preferably, said criteria include a transaction value.

Preferably, said criteria include a transaction value range.

Preferably, said criteria includes repeat transaction period data, specifying a period after which the transaction window again becomes valid.

Preferably, said validation agent provides the authorization agent with access to validated transaction windows from authorized users of payment instruments relating to that authorization agent, and said step of the authorization agent determining from the validation agent whether said transaction satisfies the criteria of at least one transaction window comprises the authorization agent performing said determination by directly accessing the transaction windows.

Preferably, said authorization agent comprises the issuing institution of the payment instrument.

Preferably, said authorization agent comprises a credit card association responsible for the payment instrument.

In accordance with a second aspect of this invention, there is provided a system for preventing unauthorized transactions over a telecommunications network among a merchant, a buyer who will make a purchase from the merchant using a payment instrument, and an authorization agent that is at least partly responsible for providing authorizations regarding the payment instrument, the buyer making a purchase from the merchant including providing the merchant with payment instrument identification information during said purchase, the system comprising:

a validation agent computer system configured to register an authorised user of the payment instrument;

the validation agent computer system further configured to register the authorization agent;

the validation agent computer system further configured to receive a transaction window request from an authorised user of the payment instrument concerning a proposed transaction using the payment instrument;

an authorization agent computer system configured to receive a request that originated from the merchant to provide authorization that the payment instrument is able to honour the transaction to the merchant, and determining from said request whether the transaction was provided over the telecommunications network; and

if said authorization agent computer system determines that said transaction was performed over said telecommunications network, said authorization agent computer system then determines from the validation agent computer system whether said transaction satisfies the criteria of at least one transaction window for that payment instrument, and if all such criteria are not met for any of said transactions windows, rejecting the transaction.

Preferably, the validation agent computer system receives registration information regarding the payment instrument during registration of the authorized user, said

registration information including verification information regarding the authorized user of the payment instrument.

Preferably, upon receipt of a transaction window request the validation agent computer system is configured to validate the transaction window request using the verification information, whereby said transaction window request is disregarded if said validation is not correct.

Preferably, said criteria includes a transaction window duration, after which the transaction window expires.

Preferably, said criteria include the identity of the merchant.

Preferably, said criteria include a transaction value.

Preferably, said criteria include a transaction value range.

Preferably, said criteria includes repeat transaction period data, specifying a period after which the transaction window again becomes valid.

Preferably, said validation agent computer system provides the authorization agent computer system with access to validated transaction windows from authorized users of payment instruments relating to that authorization agent, whereby said authorization agent computer system is configured to determine from the validation agent computer system whether said transaction satisfies the criteria of at least one transaction window by directly accessing the transaction windows.

Preferably, said authorization agent comprises the issuing institution of the payment instrument.

Preferably, said authorization agent comprises a credit card association responsible for the payment instrument.

The invention can be utilised by a validation agent in the conventional authorization process. Authorized users of a payment instrument register their instrument, e.g. a credit card, with the validation agent. The validation agent may be an existing validation agent, or it may be an additional validation agent in the authorization process. Upon approval of the registration of the payment instrument, the validation agent invalidates the payment instrument for all online transactions, which include genuine and fraudulent transactions.

When the registered payment instrument is used for an online transaction, the merchant will seek authorisation from a conventional authorization agent (e.g. the issuing institution of the payment instrument) in the usual manner. The conventional authorization agent, as a part of its authorization process, then requests the validation agent to issue an authorization for the transaction. The validation agent will reject the transaction by default, and accordingly the conventional authorization agent will reject the transaction and notify the merchant.

The authorized user of a payment instrument can choose to be notified of any and all activity on the payment instrument. The notification speed and means can be selected by the authorized user, and can include pager service, telephone, facsimile, e-mail, and other notification methods. The validation agent can notify the authorized user of the payment instrument of attempts to obtain authorization for transactions using the payment instrument.

When the authorized user desires to conduct an online transaction, the authorized user sends a request to the validation agent to issue a transaction window for a single or recurring transaction using the registered payment instrument. This request is performed over a public network, which includes the Internet or the telecommunications network. The validation agent stores the transaction window as a record in a data store. The authorized user receives confirmation of the request and continues with the purchasing process as determined by the merchant. This could include filling and returning the completed order form containing the payment instrument information (e.g. credit card number and expiry date) to the merchant over the Internet. The merchant handles the transaction

according to traditional protocols, including seeking authorization from the conventional authorization agent to honor the payment instrument.

During the authorization phase, the authorization agent recognizes the authorization request as a result of an online transaction. This may be achieved in any convenient manner, such as by reference to codes present in the authorization request. One such suitable code is "CARD NOT PRESENT".

The authorization agent will seek extra validation from the validation agent by forwarding the full or partial authorization request to the validation agent. The validation agent then references the transaction window records associated with the payment instrument, using the payment instrument number as a full or partial index to the appropriate data record. The validation agent validates the authorization request against the transaction window, and once validated, sends the authorization reply to the requesting authorization agent. Depending on the result of the validation agent's authorization, the authorization agent can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the authorization agent sends an authorization reply back to the merchant.

Advantageously, the merchant does not need to implement any new devices, software, or protocols to participate in the new secure payment system.

For added security, the transaction window can additionally be linked to extra transaction information to ensure that the transaction window is only used for one specific transaction. For instance, the validation agent might tie the transaction window to a specific purchase merchant ID and a particular amount. The validation agent might further impose a short expiration term on the transaction window so that the payment instrument associated with the transaction window again becomes invalid after the expiration term lapses. Alternatively, the authorized user of the payment instrument may be provided with the option to provide the extra transaction information when submitting the request for a transaction window.

The secure payment system substantially reduces the value of stolen credit card information since a valid transaction window must be present to complete the online transaction. In addition, the system seamlessly integrates with existing verification and settlement protocols. Software modules are implemented at the authorisation agent, but no additional components are implemented at the customer, merchant, settlement participants, or any other member in the online commerce transaction.

Brief Description of the Drawings

The invention will now be described, by way of example, with reference to one embodiment thereof and the accompanying drawings, in which:

Figure 1 shows communication paths between a customer's computer 25, a merchant's computer 26, an authorization agent's computer 27 and a validation agent's computer 28 participating in a secure transaction according to the embodiment of the invention;

Figure 2 shows an information exchange between the customer's computer 25, an authorization agent's computer 27 and a validation agent's computer 28 during a registration phase;

Figure 3 shows an information exchange between the customer's computer 25, and a validation agent's computer 28 during a transaction window request phase; and

Figure 4 shows an information exchange between a customer's computer 25, a merchant's computer 26, an authorization agent's computer 27 and a validation agent's computer 28 a payment authorization phase.

Best Mode(S) For Carrying Out The Invention

The embodiment is directed towards a system for preventing unauthorised online transactions using payment instruments such as credit cards. Although the

embodiment is described with reference to credit cards and with a validation agent as a separate entity to the authorization agent, it should be appreciated that the invention is not limited to such arrangements.

The consumer, the merchant, and the authorization agent play the primary roles in the conventional online commerce transaction. The customer and merchant may represent individual people, entities, or businesses. The authorization agent may represent different types of payment instrument-issuing institutions, such as credit card issuing banks, credit card companies, card sponsoring companies, credit card associations, or third party issuers under contract with financial institutions.

The validation agent is an organization or individual, that utilizes the system for preventing unauthorised online transactions of the embodiment to facilitate secure online commerce. It should be appreciated that in alternative embodiments of this invention, the function performed by the validation agent can be fully or partially performed by the authorization agent. For example, the validation agent may forward copies of transaction windows to the authorization agent, who keeps a local cache of the transaction windows.

Further, in alternative embodiments of this invention, additional participants such as the merchant's bank, and a payment gateway may be involved in some phases of a transaction. For simplicity, these additional participants are not shown or described in this embodiment, however it should be appreciated that the invention is not limited to arrangements omitting these participants.

In this embodiment, each participant is equipped with a computer to facilitate online commerce transactions. The customer has a computer 25 in the form of a personal computer, although other types of computing units may be used including laptops, notebooks, handheld computers, set-top boxes, mobile communication equipments, and the like. The merchant has a computer 26 implemented in the form of a computer server. The authorization agent has a computer 27 shown as a mainframe computer, however, the authorization agent's computer 27 may be implemented in other forms, such as a minicomputer, a PC

server, a networked set of computers, and the like. The validation agent has a computer 28 implemented in the form of a computer server.

The computers 25, 26, 27 and 28 are able to communicate with each other via a data communication network 29. The network 29 is a public network which, in the embodiment, is the Internet. In this context, the computers 25, 26, 27 and 28 may or may not be connected to the network 29 at all times. For instance, the customer's computer 25 may employ a modem to occasionally connect to the network 29, whereas the authorization agent's computer 27 may maintain a permanent connection to the network 29. It is noted that other types of networks may be used, such as an interactive television (ITV) network or a wireless telecommunication network.

In the embodiment, the merchant's computer 26 and the authorization agent's computer 27 are interconnected via a second network 30, referred to hereafter as a "payment network" 30. The payment network 30 represents existing proprietary networks that presently accommodate transactions for payment instruments such as credit cards and debit cards. The payment network 30 is a closed network. One example of the payment network 30 is the VisaNet™ network.

Similarly, in the embodiment the authorization agent's computer 27 and the validation agent's computer 28 are interconnected via a third network 31, referred to as a "validation network" 31. The validation network 31 is a closed network, which can be the same network as payment network 30, a dedicated communication link between the authorization agent's computer 27 and the validation agent's computer 28 or a secure network implemented over the public network 29 using technology such as Virtual Private Network (VPN).

In the preferred embodiment, the system is implemented as a registration software module 33, a transaction window software module 34, and client and transaction window databases loaded onto the validation agent's computer 28. The system is accessed during transaction processing by an authorization software module 35 operating on the authorization agent's computer 27. The customer's computer 25 and the merchant's computer 26 do not require any

additional software to participate in the online commerce transaction supported by the embodiment.

General Operation

There are three distinct phases supported by the embodiment: a registration phase, a transaction window request phase, and a payment authorization phase.

In the registration phase, the customer registers their payment instrument such as a credit card with the system, the validation agent's computer 28 in the embodiment. As part of the registration phase, the system confirms that the payment instrument issued from an authorization agent approved by the validation agent. The system also validates information received from the customer with information in its own database as well as the authorization agent.

If the validation is positive, the system assigns a permanent customer identification number and a PIN security code to the customer. The permanent customer identification number, the PIN and the payment instrument information are retained in a data record stored in the database on the validation agent's computer 28. The registration phase is described below in more detail with reference to Figure 2.

The transaction window request phase occurs when the customer requests a transaction window for their registered payment instrument in order to allow a proposed transaction to be approved. The customer issues the transaction window request by invoking a software module, which can be residing on the validation agent's computer 28, or alternatively may be accessible on other computers on the public network 29 to be dynamically downloaded to the customer's computer 25 as needed. The software module allows the registered customer to request a transaction window for a specific payment instrument that is registered with the validation agent's computer 28. The transaction window can be tied to a specific purchase merchant ID, a particular amount and a short expiration term. Since the transaction window is issued with such constraints, a thief that intercepts the payment instrument information is prevented from using it for illicit

gain. The transaction window request phase is described below in more detail with reference to Figure 3.

The payment authorization phase occurs when the merchant submits an authorization request containing payment instrument information over the conventional payment network 30 to the authorization agent for approval of a transaction. The authorization agent's computer 27 identifies the authorization request as resulting from an online transaction and seeks extra validation from the validation agent's computer 28 by forwarding the full or partial authorization request to the validation agent's computer 28. In operation, this is achieved by software modules that are executing on the authorization agent's computer 27. The validation agent's computer 28 references the transaction window data record in the database associated with the payment instrument, using the payment instrument number as a full or partial index to the appropriate data record. The validation agent's computer 28 validates the authorization request against the transaction window data records, and once validated, sends the authorization reply to the requesting authorization agent's computer 27. Depending on the result of the validation agent's authorization, the authorization agent's computer 27 processes the authorization request using its conventional processing system. After the processing, the authorization agent's computer 27 sends an authorization reply to the merchant's computer 26. In this manner, only the authorization agent's computer 27 needs to be aware that the transaction is an online transaction, which requires special validation by the validation agent's computer 28. The merchant's computer 26 need not be aware of this, but simply handles the online transaction as it would any other transaction. The authorization phase is described below in more detail with reference to Figure 4.

Registration Phase

Figure 2 shows the flow of information between the customer's computer 25, the validation agent's computer 28 and the authorisation agent's computer 27 during the registration phase.

To register with the validation agent, the customer accesses the validation agent's website via the public network 29, such as by entering the appropriate URL or by clicking the validation agent's promotional banner icon with a mouse pointer. This action submits a request for a membership registration application. In response, the registration software module 33 on the validation agent's computer 28 is invoked and sends a membership application to the customer's computer 25 via the public network 29. The membership application, which may be an HTML (hypertext markup language) form, is displayed on the customer's computer 25. This initial registration step is illustrated by flow arrow 1 from the validation agent's computer 28 via the public network 29 to the customer's computer 25.

The customer fills out various fields related to personal matters, such as name, address, telephone number, identification number (e.g. social security number), and the like. The customer also provides information regarding the payment instrument, such as payment instrument number, the issuing institution, and the like.

The customer completes the membership application and submits the application to the validation agent's computer 28 as illustrated by flow arrow 2. The registration software module 33 on the validation agent's computer 28 analyses the application to determine whether the customer is genuine and thus whether to grant or deny a membership. In the embodiment, the analysis includes verifying the customer and the payment instrument information with the issuing institution of the payment instrument, which is the authorization agent in this embodiment. The communication between the validation agent's computer 28 and the authorization agent's computer 27 for this purpose is illustrated by flow arrow 3. Although this link is illustrated as a link between computers, this step can be performed in an automated fashion or otherwise. In the embodiment, this step is performed using the validation network 31.

If membership is denied, the registration software module 33 returns a message to the customer's computer 25 indicating that the application has been denied and the payment instrument(s) will not be accepted.

Conversely, if membership is granted, the registration software module 33 returns a message, as illustrated by flow arrow 4, indicating that membership will be granted.

Assuming that a membership is granted, the registration software module 33 creates a temporary customer membership record in the customer database stored on the validation agent's computer 28 and assigns a customer identification number (CID) and a PIN (personal identification number), which are used to logon to the validation agent's website. The CID uniquely associates all relevant database records to a specific customer. In the preferred implementation, the registration software module 33 also assigns a separate activation code for each submitted payment instrument. This is a security feature to prevent unauthorized holders of payment instrument information to register the payment instrument with the validation agent. The validation agent supplies the CID, PIN, activation codes and any additional information needed to complete the formal application process to the customer. In the preferred implementation, the validation agent supplies the CID, PIN and activation codes using some means other than online transmission (e.g. mailed to the customer using conventional postal carriers) as illustrated by flow arrow 5.

The customer receives the mail and, upon receiving the CID, PIN and/or activation codes, the customer invokes the registration software module 33 and proceeds to activate the membership account with the CID and PIN, and the payment instrument with the activation code. If the validation agent 28 still desires to grant a membership to the customer, the registration software module 33 converts the temporary customer membership record to a permanent membership record in the customer database.

In some implementations, when the CID and the PIN are not considered sufficient to authenticate the customer, other forms of authentication can be used to replace or complement the CID and the PIN. These alternative forms of authentication include but are not limited to the server-side and client-side authentication using Secure Socket Layer (SSL) and authentication using Secure Electronic Transaction (SET).

Transaction Window Request Phase

Figure 3 shows information flow when the customer engages in an online commerce transaction with the merchant. As part of the process, the customer requests a transaction window from the validation agent to be used in the commerce transaction. This request can be performed prior to or during the online commerce interaction with the merchant. The information exchange between the customer's computer 25, the merchant's computer 26, and the validation agent's computer 27 during the transaction phase are illustrated as enumerated lines.

In the embodiment, the customer will typically use a browser application 32 on their computer 25 to 'surf' the World Wide Web for a particular product or service, or to visit a World Wide Web site of a particular merchant. When the customer decides to commence an online transaction with the merchant, such as purchasing a product from the merchant, the customer accesses an order form from merchant's computer 26. The order form is typically configured as an HTML (hypertext markup language) form. The customer fills out the order form to purchase a desired product from the merchant. The order form includes a payment section that requires the customer to enter a payment instrument number for payment of the goods. This is illustrated by flow arrow 1 in Figure 3.

Prior to sending the completed order form to the merchant's computer 26, the customer accesses the validation agent's website in a separate browser 32 window by typing the website URL directly or by clicking the URL link on the merchant's website to invoke the transaction window module 34 as illustrated by flow arrow 2. The transaction window module 34 is employed to guide the customer through a request for a transaction window.

A dialog box is presented to the customer informing them that they have requested a transaction window. The customer is prompted by the dialog box to input their CID and PIN for identification purposes. This information is sent to the validation agent's computer 28 via the public network 29 for authentication as illustrated by flow arrow 3. If the transaction window module 34 approves the

customer's CID and PIN, the transaction window module 34 creates a new transaction window record in the database. The transaction window record is keyed by a unique key, which in the embodiment comprises the payment instrument number and a system-generated number. The transaction window record includes the unique key, the CID, and the payment instrument number. The transaction window record is then written to the transaction window database on the validation agent's computer 28.

The transaction window request has a finite life in the embodiment, as determined by the customer or the transaction window module 34. The shorter the duration of the transaction window request, the less the likelihood of fraud resulting from the stolen payment instrument information and used prior to the end of the transaction window request's life. In the embodiment, this is accomplished by an expiration data field in the transaction window record. The customer can specify an expiration date and time into the dialog box, or leave it empty in which case the a default life is defined by the transaction window module 34.

The chief requirement of the expiration term is that it be sufficiently greater than the anticipated worst-case time for returning the authorization request response to the merchant, plus overhead to account for customer and merchant handling prior to submittal of the authorization request. The networks operated by Visa and MasterCard allegedly handle submission and return of an authorization request (round trip from the merchant to the authorization agent and back to the merchant) in less than four seconds, which is essentially negligible compared to the time reserved for customer and merchant handling. Accordingly, a suitable expiration term for a transaction window can be one-half hour to two hours. When the expiration term lapses, the transaction window is no longer valid.

Each transaction window is normally valid for only one transaction. For added security, the transaction window can be linked to transaction information to ensure that the transaction window is only used for one specific transaction. The transaction window module 34 may require the customer to enter information pertaining to the purchase, such as the purchase price, the merchant name, and the like. The transaction window module 34 can then tie the transaction window

to this specific transaction data. In the preferred embodiment, the transaction window will have a finite life of less than 2 hours and can only be used for a specific merchant.

Once the transaction window record is created, the transaction window module 34 sends a confirmation to the customer's computer 25 as illustrated by flow arrow 4. Upon receiving the confirmation, the customer continues to complete the online commerce transaction as in any conventional transaction. The customer then submits the completed order form over the Internet 29 to the merchant's computer 26 as illustrated by flow arrow 5.

In this embodiment, the transaction window commences immediately upon creation of the transaction window record and expires at the end of the term specified in the expiration data field. In alternative embodiments, the transaction window record may facilitate a commencement data field and a recurrence data field to specify a start date and time, and an interval between recurrences of the transaction window, respectively.

Authorization Phase

Figure 4 shows the information exchange between the merchant's computer 26, the authorization agent's computer 27 and the validation agent's computer 28 during the authorization phase. This phase involves the merchant seeking authorization from the authorization agent and the validation agent to honour the customer's payment information received by the merchant in the commerce transaction with the customer, for example when the customer submits the order form to the merchant's computer 26. The merchant's computer 26 does not need to have any direct link with the validation agent's computer 28 during this phase.

The merchant's computer 26 receives the payment information and other information regarding the transaction from the customer's computer 25 via the public network 29, as illustrated by flow arrow 1 in Figure 4. The merchant's computer 26 processes the information using its existing systems. There is no software components added to the merchant's computer 26. Rather, the merchant's computer 26 treats the secure online transaction no differently than it

treats the other online transactions that are not using the system of the embodiment. In fact, the merchant's computer 26 most likely will not be able to distinguish between the two types of transactions.

Next, the merchant's computer 26 submits an authorization request over the payment network 30 to the authorization agent's computer 27, as illustrated by flow arrow 2. This illustration is simplified for discussion purposes, as other participants will most likely be involved. For instance, the merchant's computer 26 typically submits the authorization request to its acquiring bank (not shown) by conventional means. The acquiring bank (not shown) validates the authorization request by verifying that the merchant is a valid merchant and that the credit card number represents a valid number. The acquiring bank (not shown) then forwards the authorization request to the authorization agent. The routing to the authorization agent via the payment network is handled through conventional techniques.

When the authorization agent's computer 27 receives the authorization request, it first performs some preliminary validation such as checking the validity of the payment instrument number. A special authorization module 35 executing at the authorization agent's computer 27 examines all incoming requests to segregate online transactions from non-online transactions. On a daily basis, the authorization agent's computer 27 will likely handle many authorization requests on the order of tens or hundreds of thousands. Most of the requests are expected to come from non-online transactions. A smaller percentage is anticipated to come from online transactions. In the continuing example, the special authorization module 35 recognizes the request submitted by the merchant computer 26 as a result of an online transaction.

The special authorization module 35 passes the full or partial authorization request to the validation agent's computer 28 via the validation network 31 as illustrated by flow arrow 3. The transaction window module 34 uses the payment instrument number as a full or partial key to locate any transaction window records in the transaction window database for that payment instrument number.

If no records are found, the payment instrument number is deemed invalid and the validation agent's computer 28 returns a reply disapproving the transaction to the authorization agent's computer 27, which in turn sends the reply to the merchant's computer 26.

If a record is found, the transaction window module 34 examines any extra transaction information, such as the expiry date of the transaction window and merchant ID, which is typically included in the authorization request to double check the accuracy of the request. If the information does not match, the number is deemed invalid and the validation agent's computer 28 returns a reply disapproving the transaction to the authorization agent's computer 27, which in turn sends the reply to the merchant's computer 26.

If the information matches, namely if the authorization request is received by the validation agent's computer 28 while a transaction window request for the payment instrument is active, and any other criteria specified in the transaction window record such as the merchant ID and payment amount match that in the authorization request, the transaction window module 34 then returns a positive reply to the authorization agent's computer 27 as illustrated by flow arrow 4. The authorization agent's computer 27 then submits the authorization request to the authorization agent's traditional processing system for normal authorization processing (e.g., confirm account status, credit rating, credit line, etc.). After the request is processed, the authorization agent's computer 27 then returns the authorization reply to the merchant's computer 26 via the payment network 30 as illustrated by flow arrow 5.

If the authorization request was successful, the credit limit of the customer's account is drawn down in the amount of the authorization, and the transaction is logged for future posting. From this point onwards, all processing such as settlement is as per normal.

The system has many advantages. One advantage is that it substantially reduces the value of a stolen number since the number is valid only if the transaction window is present. Stealing the number would not greatly benefit a thief because

it cannot be repeatedly used for other purchases or transactions. Another benefit is that the system integrates with existing card verification and settlement protocols. All the conventional parties, except the authorization agent, are able to treat the online transaction in the same manner in which they process a payment transaction today. No additional processing hardware or software is needed at the merchants or settlement participants.

It should be appreciate that this invention is not limited to the particular embodiment described above.

Claims

1. A method for preventing unauthorized transactions over a telecommunications network among a merchant, a buyer who will make a purchase from the merchant using a payment instrument, and an authorization agent that is at least partly responsible for providing authorizations regarding the payment instrument, comprising the steps of:

an authorised user of the payment instrument registering the payment instrument with a validation agent;

the authorization agent registering with the validation agent;

an authorised user of the payment instrument submitting a transaction window request to the validation agent concerning a proposed transaction using the payment instrument;

the buyer making a purchase from the merchant, including providing the merchant with payment instrument identification information during said purchase;

the authorization agent receiving a request that originated from the merchant to provide authorization that the payment instrument is able to honour the transaction to the merchant, and determining from said request whether the transaction was provided over the telecommunications network; and

if said authorization agent determines that said transaction was performed over said telecommunications network, said authorization agent then determines from the validation agent whether said transaction satisfies the criteria of at least one transaction window for that payment instrument, and if all such criteria are not met for any of said transactions windows, rejecting the transaction.

* C L M S *

2. A method as claimed in claim 1, wherein the step of registering the payment instrument with a validation agent comprises the validation agent receiving registration information regarding the payment instrument, said registration information including verification information regarding the authorized user of the payment instrument.

3. A method as claimed in claim 2, wherein said step of submitting a transaction window request to the validation agent includes the step of the validation agent validating the transaction window request using the verification information, whereby said transaction window request is disregarded if said validation is not correct.

4. A method as claimed in any one of claims 1 to 3, wherein said criteria includes a transaction window duration, after which the transaction window expires.

5. A method as claimed in any one of claims 1 to 4, wherein said criteria include the identity of the merchant.

6. A method as claimed in any one of claims 1 to 5, wherein said criteria include a transaction value.

7. A method as claimed in any one of claims 1 to 5, wherein said criteria include a transaction value range.

8. A method as claimed in any one of claims 1 to 7, wherein said criteria includes repeat transaction period data, specifying a period after which the transaction window again becomes valid.

9. A method as claimed in any one of claims 1 to 8, wherein said validation agent provides the authorization agent with access to validated transaction windows from authorized users of payment instruments relating to that authorization agent, and said step of the authorization agent determining from the validation agent whether said transaction satisfies the criteria of at least one transaction

* C L M S *

window comprises the authorization agent performing said determination by directly accessing the transaction windows.

10. A method as claimed in any one of claims 1 to 9, wherein said authorization agent comprises the issuing institution of the payment instrument.

11. A method as claimed in any one of claims 1 to 9, wherein said authorization agent comprises a credit card association responsible for the payment instrument.

12. A method as claimed in any one of claims 1 to 11, wherein said authorization agent performs at least some of the steps of the validation agent in place of the validation agent.

13. A method as claimed in any one of claims 1 to 11, wherein said authorization agent performs all of the steps of the validation agent in place of the validation agent.

14. Computer software, embodied on a computer-readable medium that, when executed on an authorization agent's computer and a validation agent's computer executes method steps for preventing unauthorized transactions over a telecommunications network among a merchant, a buyer who will make a purchase from the merchant using a payment instrument, and an authorization agent that is at least partly responsible for providing authorizations regarding the payment instrument, the method steps comprising:

registering an authorised user of the payment instrument with the validation agent;

registering the authorization agent with the validation agent;

the validation agent receiving a transaction window request from the authorised user of the payment instrument concerning a proposed transaction using the payment instrument;

the buyer making a purchase from the merchant, including providing the merchant with payment instrument identification information during said purchase;

the authorization agent receiving a request that originated from the merchant to provide authorization that the payment instrument is able to honour the transaction to the merchant, and determining from said request whether the transaction was provided over the telecommunications network; and

if said authorization agent determines that said transaction was performed over said telecommunications network, said authorization agent then determines from the validation agent whether said transaction satisfies the criteria of at least one transaction window for that payment instrument, and if all such criteria are not met for any of said transactions windows, rejecting the transaction.

15. Computer software as claimed in claim 14, wherein the step of registering the payment instrument with a validation agent comprises the validation agent receiving registration information regarding the payment instrument, said registration information including verification information regarding the authorized user of the payment instrument.

16. Computer software as claimed in claim 15, wherein said step of submitting a transaction window request to the validation agent includes the step of the validation agent validating the transaction window request using the verification information, whereby said transaction window request is disregarded if said validation is not correct.

* C L M S *

17. Computer software as claimed in any one of claims 14 to 16, wherein said criteria includes a transaction window duration, after which the transaction window expires.

18. Computer software as claimed in any one of claims 14 to 17, wherein said criteria include the identity of the merchant.

19. Computer software as claimed in any one of claims 14 to 18, wherein said criteria include a transaction value.

20. Computer software as claimed in any one of claims 14 to 18, wherein said criteria include a transaction value range.

21. Computer software as claimed in any one of claims 14 to 20, wherein said criteria includes repeat transaction period data, specifying a period after which the transaction window again becomes valid.

22. Computer software as claimed in any one of claims 14 to 21, wherein said validation agent provides the authorization agent with access to validated transaction windows from authorized users of payment instruments relating to that authorization agent, and said step of the authorization agent determining from the validation agent whether said transaction satisfies the criteria of at least one transaction window comprises the authorization agent performing said determination by directly accessing the transaction windows.

23. Computer software as claimed in any one of claims 14 to 22, wherein said authorization agent comprises the issuing institution of the payment instrument.

24. Computer software as claimed in any one of claims 14 to 22, wherein said authorization agent comprises a credit card association responsible for the payment instrument.

CLMS

25. Computer software as claimed in any one of claims 14 to 24, wherein said authorization agent performs at least some of the steps of the validation agent in place of the validation agent.

26. Computer software as claimed in any one of claims 14 to 24, wherein said authorization agent performs all of the steps of the validation agent in place of the validation agent.

27. A system for preventing unauthorized transactions over a telecommunications network among a merchant, a buyer who will make a purchase from the merchant using a payment instrument, and an authorization agent that is at least partly responsible for providing authorizations regarding the payment instrument, the buyer making a purchase from the merchant including providing the merchant with payment instrument identification information during said purchase, the system comprising:

a validation agent computer system configured to register an authorised user of the payment instrument;

the validation agent computer system further configured to register the authorization agent;

the validation agent computer system further configured to receive a transaction window request from an authorised user of the payment instrument concerning a proposed transaction using the payment instrument;

an authorization agent computer system configured to receive a request that originated from the merchant to provide authorization that the payment instrument is able to honour the transaction to the merchant, and determining from said request whether the transaction was provided over the telecommunications network; and

if said authorization agent computer system determines that said transaction was performed over said telecommunications network, said authorization agent computer system then determines from the validation agent computer system whether said transaction satisfies the criteria of at least one transaction window for that payment instrument, and if all such criteria are not met for any of said transactions windows, rejecting the transaction.

28. A system as claimed in claim 27, wherein the validation agent computer system receives registration information regarding the payment instrument during registration of the authorized user, said registration information including verification information regarding the authorized user of the payment instrument.

29. A system as claimed in claim 28, wherein upon receipt of a transaction window request the validation agent computer system is configured to validate the transaction window request using the verification information, whereby said transaction window request is disregarded if said validation is not correct.

30. A system as claimed in any one of claims 27 to 29, wherein said criteria includes a transaction window duration, after which the transaction window expires.

31. A system as claimed in any one of claims 27 to 30, wherein said criteria include the identity of the merchant.

32. A system as claimed in any one of claims 27 to 31, wherein said criteria include a transaction value.

33. A system as claimed in any one of claims 27 to 31, wherein said criteria include a transaction value range.

* C L M S *

34. A system as claimed in any one of claims 27 to 32, wherein said criteria includes repeat transaction period data, specifying a period after which the transaction window again becomes valid.

35. A system as claimed in any one of claims 27 to 34, wherein said validation agent computer system provides the authorization agent computer system with access to validated transaction windows from authorized users of payment instruments relating to that authorization agent, whereby said authorization agent computer system is configured to determine from the validation agent computer system whether said transaction satisfies the criteria of at least one transaction window by directly accessing the transaction windows.

36. A system as claimed in any one of claims 27 to 35, wherein said authorization agent comprises the issuing institution of the payment instrument.

37. A system as claimed in any one of claims 27 to 35, wherein said authorization agent comprises a credit card association responsible for the payment instrument.

38. A system as claimed in any one of claims 27 to 37, wherein said authorization agent performs at least some of the steps of the validation agent in place of the validation agent.

39. A system as claimed in any one of claims 27 to 37, wherein said authorization agent performs all of the steps of the validation agent in place of the validation agent, and said authorization agent computer system includes said validation agent computer system.

CLMS