

PAYMENT AUTHORIZATION SYSTEM

BACKGROUND

[0001] 1. Field of the Invention

[0002] This invention relates to the field of electronic payment approval and authorization. More particularly, this invention relates an improved credit or similar account authorization system and method.

[0003] 2. Description of the Problem

[0004] As society evolves, it continues to seek more convenient ways of paying for goods and services. The first system to replace the use of hard currency was based on drafts or "checks", as we know them today. While checks have proved more convenient than carrying cash, the security of a check has sometimes been questionable in that any suitable document that specified the appropriate account and bore the account holder's signature could be legally presented as a draft on the account. In practice today, the use of pre-printed checks with security papers has provided a way to limit access to only those authorized.

[0005] The twentieth century saw the rise of the credit card and the credit card account. In the early days of credit cards, the user was required to present a physical card and sign a charge slip bearing an imprint of the card. More industrious criminals could forge a card, but it was difficult enough, and the convenience of credit cards was great enough, that the credit card industry flourished. Legal restrictions on the use of credit cards and on the liability of the consumer helped. Today, a credit card owner can dispute any use of a credit card when the charge appears on the credit account statement. The card issuer is then liable for most losses due to forgery. The use of the magnetic stripe reader has enabled card issuers to prevent forgery through increasingly elaborate security encoding schemes.

[0006] As the twentieth century progressed, telephonic mail order became popular and the physical presentation of credit cards was no longer required. Credit card fraud also increased. The advent of the Internet has added to the problem by making on-line shopping a pleasant experience and thereby encouraging greater use. As electronic commerce evolves, a continually growing percentage of the world's financial transactions will rely on the integrity of the ordering. Schemes for providing encrypted keys which are in use widely today prevent third parties from learning card specifics over the Internet, but dishonest individuals will still be able to obtain card numbers in more traditional ways and simply enter a stolen number on a web page as they order. Again, these losses are primarily felt by the card issuer, but the impact is societal in scope. The biggest threat to the consumer is the advent of debit cards and check cards which allow direct access to the consumer's bank account without an intervening step of verifying the charges.

[0007] The most often used external security measure imposed on the use of a credit account number today is direct, real-time authorization by a credit card processing center. A merchant's computer system is tied into a merchant network, which is in turn connected to a large data center operated by the credit card company or financial institution. When a charge is presented the appropriate transaction and account information is electronically transmitted to the data center and authorization is requested. Before authorizing the

transaction, the data center computer system makes several checks to include whether the card has been lost or stolen as well as review and recount account histories to confirm recent, frequent use which may occur before a cardholder realizes the card is missing. What is needed is a way to enhance the security of financial account transactions, e.g., credit and debit accounts, by providing a way for the legitimate account holder to quickly and easily participate in the approval process whenever and wherever required.

SUMMARY

[0008] The present invention reduces security risks by enhancing the authorization processing at the credit card processing center. An additional test is included in the list of verification tests performed to ensure the transaction is authorized. The test uses the power of modern, mobile telecommunications networks to allow instantaneous, real-time user participation in the authorization process.

[0009] According to one method of the invention, an account payment authorization service is provided by an account processing center. When an authorization request is received from a merchant containing transaction information, the processing center determines if the credit account holder has subscribed to the service. If so, an approval request is sent to the communication device that the user or account holder has specified. An approval response is then processed. In most cases, this involves processing an actual approval response when the user sends an approval response through the specified communication device. However, the response may include an assumed disapproval if there is no response within a specified time. The processing center then sends an appropriate authorization response back to the payee, who is usually a merchant. Essentially, the processing center treats this process as another of the various tests that are performed to determine if the charge should be authorized.

[0010] Note that the request from the payee or merchant and the correlative response is referred to as the "authorization" request and response, and the messages between the processing center and the user or account holder as the "approval" request and response. The transaction information can include the amount of the charge, the name of the payee, the account number or any other similar information needed to process the transaction. The specified communication device on which the user receives the approval request is typically a wireless device so that a user can approve transactions wherever they go. This can include a digital wireless phone, for example, with short text message capability, a wireless personal data assistant, or a laptop computer with a wireless modem. It can also, however, be a stationary device such as a telephone with text messaging capability or a desktop computer.

[0011] Additionally, while it is possible to use only the native capabilities of the specified communication device to implement the invention, it may also be desirable to provide specialized features and a special protocol for the device. The approval protocol can be implemented as a protocol extension to the normal messaging protocol in order to present the information (approval protocol request) to the user and send the response (approval protocol response) from the user without having to exchange details of how to format the information. The specialized features include