

**METHOD AND SYSTEM FOR PROVIDING
TRANSACTION NOTIFICATION AND MOBILE
REPLY AUTHORIZATION**

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention generally relates to processing commercial transactions, and in particular, to a system for detecting and preventing fraudulent use of credit and debit cards.

[0003] 2. Description of the Related Art

[0004] The number of consumers using the Internet to make online purchases continues to increase. In such credit card transactions, because consumers are making the transactions by inputting information from a remote location, merchants cannot check for picture identification and/or compare the purchaser's signature with a signature on the card to verify that the purchaser is an authorized card user. Moreover, because it is not even necessary to have the physical credit card itself when transactions are made from remote locations, a credit card thief may be able to make an unauthorized charge simply by finding a sales slip with someone else's account number and expiration date. Fraudulent and unauthorized use of credit cards is a concern for all those involved in credit card transactions, including the card users, banks and financial institutions that provide credit cards. It has been estimated that credit card fraud losses may be in the range of billions of dollars a year, which is ultimately paid by the consumers through higher credit card charges and higher purchase prices.

[0005] Systems employing smart cards have been disclosed. Smart cards include a microprocessor with a memory element embedded within a physical card or device and may contain various information, such as the amount of funds in a particular account, a transaction history, account numbers and other customer data. Although various smart card systems have been proposed which attempt to provide security against fraudulent transactions, they do not address the problem of fraudulent use of conventional transaction cards (e.g., credit or debit cards having non-secure magnetic stripe data memories). Furthermore, there are a number of disadvantages associated with smart card systems. For one thing, smart cards require a smart card reader which is specifically configured to read the smart cards. Therefore, authentication or security features of smart card systems may not be performed when such smart card readers are unavailable.

**BRIEF SUMMARY OF EMBODIMENTS THE
INVENTION**

[0006] Described herein are various embodiments of a system and a correspond method for providing a notification of a pending transaction to an authorized cardholder and obtaining a reply from the cardholder indicating either approval or denial of the notified transaction. The system may be configured to transmit a transaction notification message to a mobile device associated with an account requesting a transaction. In response to receiving the transaction notification message, a user of the mobile device may generate and send a reply message to indicate approval or denial of the transaction.

[0007] According to an embodiment, the system includes the functionality to enable each of the authorized cardholders to designate a phone number of a mobile device for receiving authorization request messages and for transmitting mobile reply authorization messages. The phone number information is associated with a corresponding account number and stored in a cardholder information database. The information stored in the cardholder information database may be searchable by a phone number retrieving program executed within a server. In one embodiment, the phone number retrieving program is provided and the information arranged in the cardholder information database such that an account number search will locate the relevant phone number information designated to handle authorization request messages for the account.

[0008] According to an embodiment, a transaction authorization server is used to perform a mobile reply authorization process ("MRAP") to provide transaction notification and mobile reply authorization services. The MRAP requires that transaction requests submitted by merchants, payment servers and/or transaction computers be reviewed and authorized by the cardholder before a transaction authorization message is returned to the respective merchants, payment servers and/or transaction computers. The MRAP begins by examining a transaction request to identify the account number and determine a phone number of a mobile device assigned to receive authorization request messages. The server generates an authorization request message based on information contained in the transaction request and transmits the authorization request message to the mobile device assigned to the account requesting the transaction. A user of the mobile device receiving the authorization request message can utilize a software program executed in the mobile device to view the message and generate and send a reply message. Once the reply message is received from the mobile device, the server examines the reply message to determine if the user of the mobile device approves or denies the transaction request.

[0009] According to an embodiment, the transaction authorization server also includes the functionality to validate reply messages received from mobile devices. In one embodiment, the server includes a pending transaction database which contains information pertaining to pending transaction requests. Identifying information uniquely identifying each of the pending transaction requests is stored in the pending transaction database. Upon being presented with a reply message, the server may retrieve from the database a pending transaction record corresponding to the reply message by matching the unique identifying information specified in the reply message with corresponding information stored in the database. Then, the server may verify that the reply message is sent from a proper mobile device by matching the phone number transmitting the reply message with the phone number included in the retrieved record.

[0010] According to an embodiment, the transaction authorization server further includes the functionality to enable a card provider and/or a card holder to select one or more conditions for triggering execution of the MRAP for a particular transaction. The selected trigger conditions are associated with a corresponding account number and stored in a cardholder information database. When a transaction request is received for a particular account, trigger condition information pertaining to the requesting account is retrieved