

[0024] A storage device **121** is in communication with the server **122** for storing cardholder information database **124**. The cardholder information database **124** may include account information of each cardholder such as the cardholder identification, account number, billing address, phone numbers and other information such as the credit limit and account balance associated with each account. When an applicant applies to open an account (e.g., credit card account) with a card provider, the card provider may request that the applicant provide a phone number of a mobile device to which the applicant desires to receive authorization request messages. The phone number information is associated with the account number and stored in the cardholder information database **124**.

[0025] The transaction processing system **120** is coupled to a wireless network **128** via a data transport interface, such as Short Message Service (“SMS”) gateway **126**. In one embodiment, text messages between the system **120** and mobile devices **130-1** through **130-N** are transmitted and received using SMS text messaging. In this regard, SMS gateway **126** facilitates communication between the system **120** and the wireless network using SMS protocol. Although SMS text messaging protocol is used in one embodiment to send authorization request messages to and receive reply messages from mobile devices, other types of communication protocol may be employed to transmit and receive the messages, including protocols that can convey sound, data, images or any combination of thereof. Wireless network **128** may be a Global System for Mobile communications (“GSM”) network or any other appropriate network that facilitates wireless communication to and from mobile devices **130-1** through **130-N**.

[0026] Each mobile device **130** is preferably a wireless communication device capable of sending and receiving messages over a wireless network and displaying the messages to a user. Mobile device can be cellular phones, personal digital assistants (PDAs) and/or other types of mobile devices. The mobile device **130** may include a client message handling program (“CMHP”) **132** that enables the user to access the authorization request message sent by the server **122** and to respond to the authorization request message by generating a reply message (e.g., approval or denial of the transaction). In one embodiment, the CMHP **132** executed by the mobile device is a text messaging program which enables the user to generate a reply message by attaching a response (indication of approval or denial) to at least a portion of the authorization request message.

[0027] In another embodiment, the CMHP **132** executed by the mobile device **130** is a message handling application which is specifically configured to handle authorization request messages from the server **122** and to generate and transmit reply message to the server **122**. In one implementation, the CMHP **132** recognizes the format of authorization request messages sent from the server **122**. Similarly, the message analyzing program **40** provided on the server **122** recognizes the format of reply messages generated by the CMHP **132**. The CMHP **132** executed by the mobile device **130** includes the functionality to display transaction information included in an authorization request message to the user, which may include (i) the merchant name, (ii) the date of the transaction, (iii) the merchant location, and (iv) the purchase amount. Another function provided by the CMHP **132** is to prompt the user to input a response (e.g., approval

or denial of the transaction) by pressing designated buttons on the mobile device. In one implementation, one of the buttons on the mobile device is designated for accepting the charge and another one of the buttons is designated for declining the charge. Accordingly, the user may respond to the authorization request message by simply pressing a button that corresponds with a desired response. Based on the user’s input, the CMHP **132** generates a reply message which includes information regarding whether or not the user of the mobile device approves the transaction and sends the reply message to the system **120**.

[0028] In accordance with one embodiment, the transaction processing system **120** facilitates detection and prevention of fraudulent credit card charges without employing “smart card” type device embedded within a transaction card or incorporated within a message handling mobile device. Accordingly, in one embodiment, the system **100** does not require that the message handling mobile devices contain or have access to information regarding credit card account numbers or other credit card related information regarding cardholders.

[0029] FIG. 2 shows simplified representation of a transaction authorization server coupled to a cardholder information database according to an embodiment of the present invention. The transaction authorization server **122** includes a first communication interface (“FCI”) **205** to establish communication with payment servers **118** and/or transaction computers **119** and a second communication interface (“SCI”) **210** to establish communication with mobile devices **130**. The server **122** further includes a manager program **215**, a transaction request processing program **220**, a phone number retrieving program **225**, a message generating program **230**, a message analyzing program **240** and a pending transaction database **123** accessible by programs **215**, **220**, **225**, **230** and **240**. Although the software programs **215**, **220**, **225**, **230** and **240** are shown as separate software programs, it should be noted that any suitable arrangement of software components can be employed to provide the functionalities described herein. For example, software programs **215**, **220**, **225**, **230** and **240** can be integrated into one or more software applications executed by the server **122**. Further, in various embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the functionalities described herein. Thus, the embodiments of the present invention are not limited to any specific combination or arrangements of hardware circuitry and software components.

[0030] The pending transaction database **123** is used to maintain records of pending transaction requests, which are waiting for a reply from cardholders. In one embodiment, the pending transaction request records are generated from transaction requests and each record includes a transaction identification code or number (“transaction ID”) uniquely identifying the transaction. More specifically, in the illustrated embodiment, each record **260-1** through **260-N** of the database **123** includes (i) a Transaction ID column **251** to store a transaction ID that has been assigned to a corresponding transaction request, (ii) an Account # column **252** to store an account number requesting the transaction request, (iii) a Phone # column **253** to store a phone number of a mobile device associated with the account number, (iv) a Time of message Transmission column to record the time when the authorization request message was transmitted,