tion, which may correspond to Block **240** of FIG. **2**. In particular, referring to FIG. **4**, the location of the credit card transaction terminal **130** that is being used for the prospective credit card transaction may be provided by the credit card transaction terminal **130** itself, using pre-stored longitude and latitude coordinates. Alternatively, a credit card issuer **120** and/or a merchant may provide these coordinates along with a request for authorization of the prospective credit card transaction. In other embodiments, as illustrated at Block **410**, the credit card transaction terminal **130** may only provide an identification of the merchant. For example, there may a large number of credit card transaction terminals at a "big box" retailer or other large merchant, and the individual location of the credit card terminal may be less important than the fact that it is located at the given big box retailer. Accordingly, an identification of the merchant may be provided.

[0054] Then, at Block **420**, a determination is made as to whether multiple merchant locations are present within a given geographic area, such as a city. Thus, a determination may be made as to whether multiple sites of the big box retailer are present in a given city. If not, then a geographic information system, such as Google® Maps or MapQuest® may be queried with the merchant name, to obtain the merchant location at Block **430**. This single merchant location can then be correlated with the location of the wireless terminal(s) **150** at Block **440**, as was already described.

[0055] Alternatively, if multiple merchant locations are present within a given geographic region, the geographic information system may be queried at Block **450** and multiple locations may be obtained, as shown by multiple arrows **452**. The multiple merchant locations may be correlated with the locations of the wireless terminal(s) **150**, to determine, for example, whether one of the big box retailer locations corresponds to the location of the wireless terminal(s) **150**.

[0056] FIG. **5** is a flowchart of operations that may be performed by a credit card transaction authorization processor, such as the credit card transaction authorization processor **116** of FIG. **1**, according to other embodiments of the present invention. These embodiments may correspond to embodiments of FIG. **2**, except that at Block **240'**, an additional correlation is made of user credit card history. For example, the history of past credit card transactions for the credit card that took place prior to the prospective credit card transaction may be included in the correlation. Accordingly, credit card profiling that is conventionally used to determine authenticity of a transaction based on past buying habits of a user and/or other concurrent transactions by the user may be correlated with the location of the credit card transaction terminal and the location(s) of the user wireless terminal(s) in generating the authorization information at Block **250**.

[0057] FIG. **6** is a flowchart of operations that may be performed to generate authorization information according to various embodiments of the present invention, which may correspond to Block **250** of FIGS. **2** and **5**. Referring to FIG. **6**, at Block **610**, in some embodiments, the authorization information may be generated by transmitting a message to the at least one wireless terminal **150** that is associated with the user **160** of the credit card **162** for the prospective credit card transaction. The message may state, for example, "Please provide the clerk with the following authorization code XXX", and the authorization code may also be simultaneously transmitted to the credit card transaction terminal **130** and/or another merchant terminal. If desired, the authorization code message transmitted to the wireless terminal **150** may be protected by a password or PIN known only to the legitimate user, such that the user must input their PIN to view the authorization code. Alternatively, or in addition, at Block **620**, a message may be transmitted to the credit card transaction terminal **130** itself. This message may indicate, for example, "Please verify additional identification from the credit card holder". Alternatively, the transmission to the credit card transaction terminal **130** may include a picture of the credit card holder and the message, "Please verify that this is the credit card holder". The obtaining of a picture of the credit card holder will be described in greater detail below in connection with FIG. **7**.

[0058] Finally, at Block **630**, in addition, or alternatively, a message may be transmitted to a merchant terminal that is separate from the credit card transaction terminal **130**. In particular, the credit card transaction terminal **130** may be visible to the user **160** of the credit card **162**, particularly in a checkout line. Accordingly, a message may be sent to a separate merchant terminal, for example, a wireless terminal (e.g., cell phone) of a clerk that is operating the credit card transaction terminal **130**, to another merchant terminal in a different location, or even to a merchant security terminal (not shown). This separate message may include a picture of the user and an audible and/or text message that states, "Please verify that this is the credit card holder". Accordingly, embodiments of the present invention may obtain additional authorization information by transmitting a message to the wireless terminal (Block **610**), to the credit card transaction terminal (Block **620**) and/or to a separate merchant terminal (Block **630**).

[0059] FIG. **7** is a flowchart of operations that may be performed to obtain user authentication using a picture, according to some embodiments of the present invention. These operations may be performed, for example, using the messages that are transmitted at Block **610**, **620** and/or **630** and/or at other times.

[0060] Referring to FIG. **7**, at Block **710**, a picture of the user **160** of the credit card **162** is obtained. For example, the credit card issuer **120** may have obtained the picture of the user when the credit card **160** was issued. Alternatively, the wireless network provider **140** may have a picture of the user that in some cases may be stored for use on the wireless terminal **150** home screen, for caller identification, text messaging and/or other applications on the user's wireless terminal **150** and/or for other purposes. The picture may have a date stamp indicating when it was taken. The obtaining of a picture of a user of a credit card or a wireless terminal, along with a date stamp, is well known to those having skill in the art and need not be described further herein.

[0061] Still referring to FIG. **7**, at Block **720**, in order to reduce the likelihood of intentional fraud, a determination is made as to whether the picture is sufficiently old by comparing the date stamp to the current date. In some embodiments, "sufficiently old" may be any day that is prior to the current date. However, in other embodiments, a picture that is, for example, at least several days old, at least a week old or older, may be used. If, at Block **720**, the picture is not sufficiently old, then it may be discarded at Block **730**. On the other hand, if the picture is sufficiently old at Block **720**, it may be transmitted at Block **740**, for example as part of any of the operations of Blocks **610**, **620** and/or **630** of FIG. **6**.

[0062] Embodiments of FIG. **7** may arise from recognition that a thief who desires to spoof a credit card authorization system may fraudulently obtain another wireless terminal and