

store a picture of the user on the fraudulent wireless terminal, and/or may obtain another credit card with a picture of the user, and then use this credit card to misrepresent the user during the proposed credit card transaction. Accordingly, if the picture is new, it may not be used in performing authentication, because it may have been obtained to commit a fraud. On the other hand, if the picture is sufficiently old, it may be used in performing authentication because it is unlikely to have been obtained by a thief. Generally, an older picture is more trustworthy, as long as it is not so old as to be inaccurate for purposes of current identification.

[0063] Embodiments of FIG. 7 have been described in connection with location based authorization system, methods and/ computer program products. However, other embodiments of the present invention may use picture verification of FIG. 7 independent of location based authentication. Thus, some embodiments of the present invention may obtain a picture of a user 160 of a credit card transaction terminal 130 for a prospective credit card transaction from a wireless network provider 140 and/or credit card issuer 120 that is associated with the user, along with a date stamp for the picture, as was shown in Block 710. The picture may be selectively transmitted to a location near the credit card transaction terminal 130, including transmitted to the credit card transaction terminal 130 itself, to allow an identity of the user to be verified, if the date stamp is sufficiently before the prospective credit card transaction, as was illustrated in Block 720. Accordingly, picture verification may be used only when there is a high likelihood that the picture itself is legitimate.

[0064] FIG. 8 is a flowchart of operations that may be performed to obtain multiple levels of user authentication according to various embodiments of the present invention. These embodiments may be used in connection with location based credit card authorization according to various embodiments of the present invention. Referring to FIG. 8, at Block 810, a determination is made as to whether all wireless terminals 150 that are registered to a user 160 of the credit card 162 for the prospective credit card transaction are sufficiently close to the credit card transaction terminal 130 for the prospective credit card transaction. If so, a first level of authentication may be obtained at Block 820. The first level of authentication may be a signature that is captured at the credit card transaction terminal 130 and is compared with the signature on the back of the credit card 162. On the other hand, if all of the wireless terminals 150 are not near the credit card transaction terminal 130 at Block 810, a second level of authentication, that is greater than the first level, may be obtained at Block 830. For example, in addition to signature capture, the clerk may be instructed to obtain a second form of identification from the user.

[0065] Continuing with the description of FIG. 8, a determination is made at Block 840 as to whether the multiple wireless terminals 150 are also associated with multiple wireless network providers 140. If so, then at Block 850, a third level of authentication, that is greater than the second level of authentication, may be obtained. For example, the third level of user authentication at Block 850 may comprise transmitting a picture of the user 160 that was obtained sufficiently before the prospective credit card transaction to a location near the credit card transaction terminal 130 and verifying an identity of the user 160 from the picture that was transmitted, as was described above in connection with embodiments of FIG. 7. In other embodiments, transmitting a picture of the user and verifying an identity of the user from the picture that

was transmitted may be performed as part of a second level of user authentication, and an even stricter level of authentication may be provided at the third level. Accordingly, multiple levels of authentication may be obtained based on the correlation of the location of the credit card transaction terminal and the user wireless terminal(s), according to some embodiments of the present invention. It will be understood that various types of user authentication may be obtained at the first, second and third levels using authentication techniques well known to those having skill in the art.

[0066] Additional discussion of various embodiments of the present invention will now be provided. In particular, some embodiments of the invention may arise from recognition that it may be desirable to provide a central credit card transaction server that is capable of communicating with multiple credit issuers, multiple merchants and multiple wireless network providers, to provide a location based credit card transaction authorization clearinghouse. However, other embodiments of the present invention may allow a given wireless network provider to provide location information for wireless terminals in its own system to a plurality of credit card issuers and/or merchants. Moreover, in other embodiments, the credit card transaction server may be operated by a given wireless network provider and the credit card transaction server may be configured to identify wireless phones of other wireless network providers that are registered to the user of a prospective credit card transaction. There may be privacy issues and/or regulatory issues that may impact the solicitation or transmission of customer identification information, but these issues may be overcome using appropriate encryption and/or user pseudonyms. For example, in some embodiments, a pseudonym may be used to hash the personal information of a user of another wireless network provider.

[0067] Moreover, any of the embodiments that were described above may be conditioned on the cost of the item being purchased by the credit card transaction, by a metric of prior or concurrent credit card transactions and/or some other indications of a large potential fraud. In other embodiments, however, these factors may need not be considered, because it may be regarded as important to detect any fraud, big or small.

[0068] In the drawings and specification, there have been disclosed embodiments of the invention and, although specific terms are employed, they are used in a generic and descriptive sense only and not for purposes of limitation, the scope of the invention being set forth in the following claims.

What is claimed is:

1. A credit card transaction server comprising:

- a credit card transaction interface that is configured to receive information about credit card transactions that are associated with a plurality of credit card issuers;
- a wireless network interface that is configured to obtain location information for a plurality of wireless terminals that are associated with a plurality of wireless network providers; and
- a credit card transaction authorization processor that is responsive to receipt of information concerning a prospective credit card transaction with one of the plurality of credit card issuers from the credit card transaction interface, to instruct the wireless network interface to obtain location information from the plurality of wireless network providers for at least one wireless terminal that is associated with a user of the credit card for the prospective credit card transaction, to correlate a location of a credit card transaction terminal that is associ-