

the call. This permits the financial institution to verify the customer biometric information at block 424 with biometric information on record, such as may have been supplied with the credentials. In addition, it provides a remotely stored record of the customer's biometric pattern to enable execution of remote identifications. While the location verification and biometric identification each provide assurance that the initiation is being performed by a valid customer, even greater assurance is provided in embodiments where both location verification and biometric identification are used.

[0037] Once the customer has been authenticated, the financial institution downloads software for implementing an account transaction mechanism to the wireless device at block 428. After the software has been loaded, the customer may acknowledge receipt of the software and establish a unique encryption key on the wireless device at block 432. The encryption key may subsequently be used as part of an authentication process performed when executing a transaction as described further below. In some instances, a combination of the private key established by the customer, a timestamp, and a location code derived from the GPS chip 360 may be used to create a unique one-time encryption key that minimizes the risk of possible replay attacks and is used in maintaining an accurate transaction record.

[0038] A similar initiation procedure may be used for credit, debit, prepaid, stored-value, and other types of account transaction mechanisms. In addition, any or all of the accounts may be tied to a loyalty program that permits issuers to provide loyalty rewards or to enhance existing programs by allowing the customer to customize offerings. Thus, for example, a customer may be able to select a particular account transaction mechanism to be associated with a particular loyalty program.

[0039] As indicated at block 440 of FIG. 4B, execution of a transaction with an account transaction mechanism loaded on the wireless device begins with the customer visiting a merchant. The customer selects goods and/or services to be purchased at block 444 and transaction information is input into a point-of-sale device 204 having the capabilities described above. Entry of the transaction information is typically performed by a clerk, but may be performed in an automated fashion for certain merchant layouts. It should be understood that the range of devices comprised by the point-of-sale device 204 may be somewhat extended so that execution of the transaction need not require that the customer be physically at the station, although in some instances a merchant may structure its premises for security reasons to require such presence. Examples of merchants that may find it advantageous to use the extended range of the point-of-sale device include restaurants so that a customer may settle a bill without leaving the table. Furthermore, by making use of the wireless device in this way, there is a complete elimination of the risk that an employee who takes a card away from the table to execute a transaction will steal the account information or otherwise commit fraud involving the card.

[0040] For any of these configurations, the point-of-sale device transmits transaction information wirelessly to the wireless device at block 448. The wireless device that is to receive the transmission may be identified using the RFID chip 364. A display on the wireless device permits the customer to review the transaction information for correct-

ness, ensuring that such things as the identification of the items to be purchased and their cost are correctly identified. In addition, the display permits the customer to review a list of account transaction mechanisms that have been loaded onto the wireless device. Display of logos for the various account transaction mechanisms from graphical information that has been loaded onto the wireless device may simplify the selection of the desired account transaction mechanism by the customer at block 456.

[0041] After the customer has selected the desired account transaction mechanism using functionality provided on the wireless device to make menu selections, steps may be taken to complete the transaction. In some cases, the identity of the customer may be verified prior to completing such steps, as indicated at block 460. In one embodiment, a local biometric verification is performed by using the biometric system 376 to read a biometric feature from the person using the wireless device and to compare that feature with a feature stored on the wireless device itself. In other embodiments, the biometric feature may be read using the biometric system 376 and bundled with a packet to transmit account information and the cryptographic key, as is otherwise done at block 464. In such instances, the biometric identification may be performed remotely as part of the transaction authorization.

[0042] In most instances, the account information and key are transmitted to the point-of-sale device 204, which bundles the information with a specification of the transaction parameters, including the cost for the transaction, for transmission as an approval request at block 468. An approval request transmitted from the point-of-sale device 204 may be sent wirelessly or may be sent over physical connections as described for different embodiments in connection with FIG. 2. In some alternative embodiments, the wireless device itself may bundle the transaction information with the account and cryptographic information and transmit the bundle as an approval request directly to the host system 218 of the financial institution 216. It is noted that in either instance there is no need to include an acquirer as an intermediary in coordinating transmissions, although nothing in the arrangement precludes the presence of an intermediary acquirer either.

[0043] At block 472, the financial institution 216 determines whether to authorize the transaction in accordance with its normal authorization practices and perhaps also by verifying the identity of the customer with a remote biometric comparison. If the transaction is a debit transaction, the financial institution 216 initiates an immediate transfer of funds at block 476 from the identified customer account to the merchant's account. Such a transfer of funds may involve transmission over the financial network 212 discussed in connection with FIG. 2 if the customer and merchant have accounts at different institutions. If the transaction is a credit transaction, the authorization may be generated with the transaction conveniently being held at block 480 by the financial institution 216 for batch funding with other transactions payable to the merchant account at a later time. If the transaction is authorized, the authorization is communicated back to the point-of-sale device 204. In addition to permitting the system to operate without an acquirer, this arrangement may also function without the need for individual credit companies to maintain their own networks.