

example at an ATM, or by a merchant for example at a retail store. The third party then inputs their system identification number **74**, followed by a biological identifier **76**, such as a fingerprint. The third party then picks from a menu the account to access **78**. The account menu may, for example, list Account #1, Account #2, etc. or Checking Account #1, Credit Card #1, Credit Card #2, etc.

[**0057**] The amount, fingerprint, and system identification number are then transmitted to the central database **80**. The combination of the biological identifier and the system identification number uniquely identifies the third party **82**. If the person is not identified, the transaction is declined **84**. If the identity is confirmed, the third party's authorization to access the account is processed **86**. If the third party is not authorized to access the account chosen, the transaction is declined **88**. If the individual is authorized, the authorization parameters are compared **90**. If the transaction meets the authorization parameters the transaction is approved **94**, and a receipt is printed by the terminal **96**. If however, any parameter is exceeded, the transaction is declined and the process ends **92**.

[**0058**] As noted above, this process is preferably also used to limit account access by the primary account holder himself during the course of foreign or domestic travel, in order to limit the potential for fraud.

[**0059**] As described above, the central database functions both as a storehouse for biological identification information, and as an authorization authority that makes the automated decision (based on the primary account holder's previously recorded instructions) on transaction authorization. However, both functions need not be centralized. Instead one or both of these functionalities is optionally distributed among other devices in a network.

[**0060**] According to a hybrid embodiment, the central database continues to function as a storehouse for biological identification information. However, this central facility does not conduct transaction authorization processing. The authorization processing is handled locally at or near the location of the transaction so that the authorization processing burden is distributed around the network. When the third party initiates the transaction, providing their system identification number and their fingerprint, only the system identification number is transmitted across the network to the central database, which returns to the local server the appropriate biological identification data for comparison to the fingerprint the third party has just provided. That local server actually makes the comparison and applies the conditions previously set by the primary account holder under which the value account may be accessed. Thus authorization is distributed while ID data is stored centrally.

[**0061**] It is also an alternate embodiment of the present invention for both authorization processing and biological ID information storage to be distributed. Operationally, this embodiment is very similar to the one previously described where authorization is distributed and ID data is stored centrally. One difference is that in the event the merchant server has the third party's biological ID information stored locally, then the merchant server proceeds directly to performing authorization processing. The only transmission to the central database server is to indicate occurrence and disposition (approved/denied) of the transaction. This data is then used for notification of the primary account holder.

However, in the event that the merchant server does not have the third party's biological ID information stored locally, the merchant server then sends out a request for the information to the central database. The central database then broadcasts this request for the relevant data across the network to other facilities that store such data. The appropriate storage device responds by returning to the central database the appropriate biological identification data for relay to the merchant server or, in the alternative, transmits it directly to the merchant server. Once the biological ID information is obtained, the merchant server makes a comparison to the fingerprint the third party has just provided. Thus, both authorization processing and storage of ID information are distributed.

[**0062**] According to another hybrid embodiment, the central database stores no biological identification information but conducts all authorization processing for the system. The storage of biological identification information is handled locally at or near the location of the transaction so that the data storage burden is distributed around the network. When the third party initiates the transaction, providing their system identification number and their fingerprint, the merchant server transmits a package of information across the network to the central database. The package of information contains the system identification number provided, an extract of biological ID data from the fingerprint proffered, and (if available in the merchant server's own database) the biological identification data corresponding to the that third party, as previously recorded. In the event that the merchant server local to where the transaction is being initiated does not have a copy of that third party's biological identification data, then the central database sends out a request for the relevant data across the network to other facilities that store such data. The appropriate storage device responds by returning to the central database the appropriate biological identification data for comparison to the fingerprint the third party has just provided. That central database actually makes the comparison and applies the conditions previously set by the primary account holder under which the value account may be accessed. Thus authorization is done centrally while ID data is distributed.

[**0063**] An additional feature of the present invention is wireless notification of the primary account holder that an authorized third party has accessed an account. The wireless message (sent, for example, to a cell phone, PDA, or pager) is preferably an alphanumeric message that indicates at least the name of the party who accessed the account, and the amount of the transaction. This provides a near real time notification to the primary account holder of activity on the account.

[**0064**] Such notification is optionally made via an email message addressed to the primary account holder. Although email is not always as immediately accessible as a pager carried on one's person, the medium of email easily permits the message to include a detailed accounting of all relevant facts about the transaction, including (if desired) a listing of items bought from a merchant.

[**0065**] Another aspect of the present invention is real time authorization by the primary account holder of transactions involving the value account. This means that the transaction completion is contingent upon real time assent by the primary account holder, rather than a rule-based, automated approval/disapproval as described above. At the primary