

[0104] In either event, (System platform or desktop/laptop built database) the subscriber will enter (or for an established subscriber, modify) user information, actual account information and account alias (e.g. how the account will be referenced or named on the mobile device, such as VISA \*\*\*\*4195) the account access rules (such as PIN assignment, or biometric information needed to access account information, e.g. voice sample, or other biometric measure used as a security feature); personal preference or personal account information (for instance, airline mileage accounts, hotel preferred user identifications, etc).

[0105] Information is stored in three general areas of the database: financial account information, Subscriber personal information; and Subscriber preferences. The Subscriber can also enable CTC transactions and enter information for CTC transactions. When the database is stored on the System, the mobile device also contains a database, but that database contains very limited information as the mobile device in this embodiment is used primarily a non-intelligent input device. For instance, account aliases would be stored, but not actual account information. The data storage on such a non-intelligent device can be further reduced by pushing input selections (such as aliases) from the System platform to the mobile device during each transaction.

[0106] Once the database is built and configurations established, they are saved on the laptop/desktop or System platform. The saved database (or a portion of it) and mobile application software must be transferred to the mobile communications device(s). Several alternatives can be used to transfer data and vary depending on where the data is initially located. First, the mobile system application program must be installed on the mobile device. This can be accomplished by interfacing the mobile device with the desktop, or to the System platform and downloading directly to the mobile's Internet features. Alternatively, the mobile could be interfaced with a storage device (such as a USB flash memory) having the software stored thereon transferred and installed on the mobile device. One embodiment can allow transfer (possibly including the mobile system application program) from the desktop/laptop to the mobile device, through an interface program designed to communicate with the mobile AMS, using a mobile docking station or USB interface (if the mobile device is so equipped). For instance, some mobile communications devices, such as the Blackberries, already have software for syncing data files through a USB connection.

[0107] Another option is to download to the mobile device through the System Server through an established system mobile application program. For instance, to update an existing mobile database, the System mobile application is already installed. It is also possible to input information into the mobile device directly through preloaded software, but this is not preferred due to limitations on mobile device keyboards and processing limitations.

[0108] Once the mobile device is configured, it is desirable to exercise the account information to ensure accuracy of the information. For instance, the System platform can request that the subscriber pay a charge through each of the listed accounts using the System to assist in the transaction (the merchant in this event would be the System itself) in order to fully activate the account.

[0109] An active account can be reconfigured, edited or modified using similar procedures, such as displayed in

**FIG. 9** As shown in **FIG. 9** (see 9.4) the System can provide an option to "wipe" or erase the stored mobile databases. This feature is activated by the Subscriber through the Server web based portal and can be used to erase data on the mobile device in the event the device is lost or stolen. The subscriber will log into the subscriber's account and request the data wipe.

[0110] As described, the Subscriber's sensitive account information can be stored in the System or the mobile device databases (and possibly, a backup desktop database). Further, it is preferred that the certain sensitive data stored in the mobile database (if any) be stored encrypted. The Subscriber personal information may be stored in the mobile and encrypted using a different key or algorithm than that of the encrypted sensitive account information. Even if the mobile device is stolen or the desktop hacked, the account information remains secure unless the encryption scheme can be broken.

[0111] In the current embodiment, the System platform 4 has the ability to decrypt the information stored on the mobile device, as the System platform 4 provides the encryption scheme. In future embodiments, the ability of the System platform 4 to decrypt account information can be eliminated by having the issuing bank platform 3 (e.g. the bank or credit card company) load account information on the System platform database, mobile device database or desktop built database using the issuing bank's encryption scheme, thereby providing additional security measures. For instance, the Subscriber could access the issuing bank through the issuing banks web portal and request the issuing bank to download encrypted account information into the database under construction or the mobile device. Alternatively, encrypted information could be passed from the issuing bank to the System platform database 4 for storage of download to the mobile device database. This embodiment is generally only applicable if the mobile device stores the actual account information. When the subscriber account database is stored on the System, encryption is not usually needed as the System database will be protected by firewalls and other security devices, although encryption on the System database could be used for security redundancy.

#### [0112] B. Merchant Account

[0113] Finally, for each merchant using the system, the merchant will enroll as a merchant subscriber with the System, and have data associated with the merchant (merchant data). See generally **FIG. 4**. The merchant platform will be configured to interface the System (such as receive the merchant software module designed or be informed of transfer request formats for web services). The enrolled Merchant will be given a merchant subscriber ID and associated with the System Processor if the System will process the account information (see generally 4.3) (e.g. credit card information) for this merchant or the merchant subscriber account data will indicate that a Merchant Processor will be the processing party. Details of the Merchant Processor may be included in the System database, if needed. The merchant will configure the merchant's system data, particularly, merchant data that interfaces with subscriber's PI or preference data. For instance, the merchant data can interface certain subscriber PI or preference data to determine pricing options, availability options, service upgrades, etc for a particular transaction. For example, the