

[0023] FIG. 4 illustrates a flow chart diagram of access to the primary account by an authorized third party.

#### DETAILED DESCRIPTION OF THE INVENTION

[0024] As noted earlier, the present invention is a system and method for allowing a primary account holder to authorize third parties to access a value account subject to flexible limitations set by the primary account holder.

[0025] Referring to FIG. 1, the architecture of the present invention is illustrated. The primary account holder registers for services according to the present invention at a registration kiosk 16. The primary account holder allows authorization by password for Internet access to accounts. The primary account holder has access to a workstation or personal computer 14 that is connected via a network (preferably, but without limitation, including the Internet) to the central database 12.

[0026] Optionally, a biological identification device (BID) 28 is connected to the primary account holder's personal computer 14. This biological identification device is preferably a fingerprint reader, and is alternatively embodied as a voiceprint reader, an iris recognition device, or a retinal recognition device. The BID may be embodied as any suitable biological identification device. For purposes of example only and without limitation, this BID will be discussed as a fingerprint identification device.

[0027] Also connected to the central database 12 via the network is a bank or financial institution 10 in which the primary account holder has his bank account.

[0028] The primary account holder can access and transfer funds in the value account at a financial institution 10 via a number of ways. One way for the primary account holder to gain access is via the PC 14 in conjunction with either the BID 28, or the appropriate password. A second way is for the primary account holder to gain access via the kiosk 16 in conjunction with the BID 30. A third way for the primary account holder to gain access is via the telephone 32 (or a wireless device) in conjunction with either the appropriate password, or the BID 22.

[0029] The primary account holder can also use the PC 14, kiosk 16, telephone 32, or a wireless device 34 to identify a third party (a spouse, a child, an employee, etc.) by their system ID number as being one who is allowed to have access to the value account. The third party shall have registered at a kiosk 16 (or otherwise) to obtain a system ID number. The third party's biological identity indication is represented by their system ID number, which is preferably stored in the central database 12. The third party performs a transaction at a merchant 24, accessing the value account at the financial institution 10, by reading the biological indicator on the merchant 24 BID 26.

[0030] The primary account holder has the option according to the present invention of flexibly designating a variety of parameters associated with access by the third party to the value account at the financial institution 10. For example, the basic limitation is the identification by a BID that the person attempting to gain access is the one that is authorized to access the account. This is preferably enhanced by a specific system ID number for the individual.

[0031] In addition to the basic authentication and limitation of the specific biological indicator, the primary account holder has the option of limiting:

[0032] the amount that can be withdrawn at any particular time by the third party,

[0033] a total amount that can be withdrawn during any particular period of time,

[0034] the geographic locale from which funds may be requested,

[0035] a range of dates over which funds can be requested by the third party,

[0036] specific merchant types where transactions may or may not be requested, and

[0037] other factors over which a primary account holder chooses to exert control.

[0038] For example, such controls enable a parent to limit the amount of money that a child attending college could obtain on a monthly basis. Extending the example, parental controls would further limit the location from which such funds could be withdrawn. If the child is supposed to be in one state, but attempts to withdraw funds from the value account when the child is located in another state, such access is denied.

[0039] In addition to limiting third parties, the primary account holder is empowered to limit his or her own access to the account to allow funds to be withdrawn to prevent fraud from occurring. For example, if the primary account holder is on travel in a foreign country, the primary account holder elects to allow funds to be deducted from the value account for a period of time when the person is on travel in a particular country. Accordingly, if a physical access device for the value account (check, debit card, credit card, check etc.) is lost or stolen, and then used in another country, that use could be denied based upon the geographic limitations placed on the account by the primary account holder and further denied by virtue of the fact that the biological indicator would not allow the unauthorized third party to access the funds in the first instance.

[0040] As part of the present invention, it is anticipated that a BID 18, associated with an ATM 20 (or other locations where funds are dispersed), is also connected via the network to the central database 12.

[0041] It is expected that that wireless communication of biological information will also be used with the present invention. A new generation of wireless communication devices 34 having fingerprint identification exists so that wireless communication fraud can be avoided. These wireless communication devices 34 communicate via their native wireless network and access a broader network on which the central server resides via a WAP interface 38 or other appropriate network connection. Alternatively, a wireless central server is implemented directly on the wireless network as a supplemental mirror facility to the central database. The wireless central server is programmed (for example, using WML or other wireless oriented language) for optimum interface with wireless communication devices 34.

[0042] Using such a wireless communication device 34, the primary account holder has the power to authorize