

step of said VPN server instructing said first user's financial institution to initiate a transfer of available funds from said first pooled funds account to said second pooled funds account using an automated clearing house (ACH) commercial credit draft.

13. A method of preventing fraud in an electronic financial transaction as claimed in claim **11**, further comprising the step of presenting to said first user a visual animated display representing said withdrawal of available funds from said first user's DDA account in said first user's financial institution as e-cache, said first user's placing said e-cache in said first user's virtual account, and said first user transferring said e-cache to said second user;

said animated display comprising an icon representing an electronic automated teller machine (eATM), cash-like authentication tokens representing said e-cache, an icon representing a repository for holding said first user's e-cache, one or more icons representing potential recipients of said e-cache including an icon representing said second user, and at least one icon representing a pointer by which said first user can select and move said e-cache;

said animated display visually depicting said user's moving said pointer to withdraw e-cache from said eATM, moving said pointer to place e-cache from said eATM into said repository for holding said first user's e-cache, and moving said pointer to transfer e-cache out of said first user's repository and to said icon representing said second user.

14. A method of preventing fraud in a financial transaction as claimed in claim **13**, in which said first pooled funds account and said second pooled funds account are the same pooled funds account.

15. A method of preventing fraud in a financial transaction as claimed in claim **13** in which said first user's financial institution and said second user's financial institution are the same financial institution.

16. A method of preventing fraud in electronic financial transactions comprising the steps of:

establishing a proprietary network including at least the internet and one or more cellular wireless networks interconnecting a proprietary network server, one or more financial institutions, and at least one user, said user having a demand deposit account (DDA) in one of said financial institutions and having a virtual monetary account maintained by said proprietary network server and associated with said DDA, said user being authorized to use said proprietary network and having a cellular telephone that is connected to said one or more cellular wireless networks such that said cellular telephone can communicate with said proprietary network server,

said user being identified and authenticated to said proprietary network server through said cellular telephone;

said user providing instructions to said proprietary network server to prepare a transfer of funds from said user's virtual monetary account to an identified entity;

said proprietary network server notifying said user that all conditions necessary to initiate said transfer of funds have been satisfied;

said user providing instructions via said cellular telephone and said one or more cellular wireless network to said proprietary network server to transfer said funds to said identified entity.

17. A method of preventing fraud in electronic financial transactions as claimed in claim **16**, said step of said user being identified and authenticated to said proprietary network server through said cellular telephone further comprising the steps of:

said proprietary network server sending information to said user through a short message service (SMS) message sent to said user's cellular telephone;

said user sending an SMS message to said proprietary network server, said user's SMS message including identifying information authenticating said user's identity and authorization to access said proprietary network server;

said proprietary network server receiving said user's SMS message and comparing said identifying information with corresponding identifying information previously provided by said user;

and if said comparison of identifying information authenticates said user's identity and authorization to conduct transactions using said proprietary network server, accepting instructions from said user.

18. A method of preventing fraud in electronic financial transactions as claimed in claim **17** further comprising said cellular telephone having means for reading encoded identifying information stored on a machine-readable object, and said user providing a machine-readable object to said cellular telephone whereby said user's SMS message to said proprietary network server includes said encoded identifying information.

19. A method of preventing fraud in electronic financial transactions as claimed in claim **17** further comprising said cellular telephone communicating to said proprietary network server that a physical authenticating object is present.

20. A method of preventing fraud in electronic financial transactions comprising the steps of:

establishing a proprietary network using the internet;

connecting to said proprietary network a proprietary network server, one or more financial institutions, one or more commercial merchants, at least one purchaser having at least one demand deposit account in one of said one or more financial institutions, and a plurality of terminals whereby each user of said proprietary network can communicate with said proprietary network server;

authorizing said purchaser to conduct financial transactions using said proprietary network;

said one or more commercial merchants and said at least one purchaser having virtual monetary accounts maintained by said proprietary network server;

one of said one or more commercial merchants establishing an internet site through which said commercial merchant offers products or services for purchase over the internet;

said commercial merchant displaying information on said internet site notifying prospective purchasers that financial transactions may be conducted with said commercial merchant using said proprietary network and including a proprietary network icon to be selected when a purchase is to be made using said proprietary network;

said purchaser selecting products or services to be purchased from said commercial merchant;