Claims

1. A system for preventing electronic transaction fraud, comprising:

a plurality of network-connected data processing terminals, including at least one server;

means for receiving an electronic authorisation request at the server from a first data processing terminal, wherein the request is for authorising the processing of an electronic transaction associated with a cardholder's card data or account data;

means for filtering the received request according to predetermined filtering criteria;

means for identifying at least a second data processing terminal as a cardholder device;

means for sending the request to the cardholder device, to notify the cardholder that processing of an electronic transaction is proposed, a parameter of which is said cardholder's card data or account data; and

means for receiving interrupt data from the second terminal and for interrupting processing of the, or any further, electronic transaction with that card data or account data;

wherein the first data processing terminal is selected from the group comprising an electronic point of sale terminal, an electronic card processing terminal, an automatic teller machine, a telephone, a cellular telephone, a radiotelephone, a portable computing device, a desktop computing device.

2. A system for preventing electronic transaction fraud, comprising:

a plurality of network-connected data processing terminals, including at least one server;

means for receiving an electronic authorisation request at the server from a first data processing terminal, wherein the request is for authorising the processing of an electronic transaction associated with a cardholder's card data or account data;

means for filtering the received request according to predetermined filtering criteria;

means for identifying at least a second data processing terminal as a cardholder device;

means for sending the request to the cardholder device, to notify the cardholder that processing of an electronic transaction is proposed, a parameter of which is said cardholder's card data or account data; and

means for receiving interrupt data from the second terminal and for interrupting processing of the, or any further, electronic transaction with that card data or account data;

wherein the first or second network is selected from the group comprising a public switched telephone network, a cellular telecommunication network, a wide area network, a local area network, a wireless local area network, a virtual private network and an interbank network.

3. A system for preventing electronic transaction fraud, comprising:

a plurality of network-connected data processing terminals, including at least one server;

means for receiving an electronic authorisation request at the server from a first data processing terminal, wherein the request is for authorising the processing of an electronic transaction associated with a cardholder's card data or account data;

means for filtering the received request according to predetermined filtering criteria;

means for identifying at least a second data processing terminal as a cardholder device;

means for sending the request to the cardholder device, to notify the cardholder that processing of an electronic transaction is proposed, a parameter of which is said cardholder's card data or account data; and

means for receiving interrupt data from the second terminal and for interrupting processing of the, or any further, electronic transaction with that card data or account data;

wherein the plurality of network-connected data processing terminals includes at least one security terminal operated by a state, official or private security organisation and further comprising means to automatically communicate interrupt data to the security terminal whenever interrupt data is received from a second terminal for an electronic transaction, wherein the means to automatically communicate further comprises aggregating means for receiving the interrupt data and generating fraud reporting data.

4. The system according to claim 3, wherein the plurality of network-connected data processing terminals includes at least one security terminal operated by a state, official or private security organisation and further comprising means to automatically communicate interrupt data to the security terminal, whenever interrupt data is received from a second terminal for an electronic transaction and wherein the fraud reporting data corresponds to at

least one selected from the group comprising a geographical position, a first data processing terminal type, a financial institution identifier, a merchant identifier, image data, audio data and video data, as a function of whether any such data is stored at the first data processing terminal and/or at the server in connection with the reported transaction.

5. The system according to claim 3, wherein the plurality of network-connected data processing terminals includes at least one security terminal operated by a state, official or private security organisation and further comprising means to automatically communicate interrupt data to the security terminal, whenever interrupt data is received from a second terminal for an electronic transaction and wherein the fraud reporting data corresponds to a combination of some or all of data corresponding to a geographical position, a first data processing terminal type, a financial institution identifier, a merchant identifier, image data, audio data and/or video data, as a function of whether any such data is stored at the first data processing terminal and/or at the server in connection with the reported transaction.

6. A system for preventing electronic transaction fraud, comprising:

a plurality of network-connected data processing terminals, including at least one server;

a server component configured to receive an electronic authorisation request at the server from a first data processing terminal, wherein the request is for authorising the processing of an electronic transaction associated with a cardholder's card data or account data;

a server component configured to filter the received request according to predetermined filtering criteria;

a server component configured to identify at least a second data processing terminal as a cardholder device;

a server component configured to send the request to the cardholder device, to notify the cardholder that processing of an electronic transaction is proposed, a parameter of which is said cardholder's card data or account data; and

a server component configured to receive interrupt data from the second terminal and to interrupt processing of the, or any further, electronic transaction with that card data or account data;

wherein the first data processing terminal is selected from the group comprising an electronic point of sale terminal, an electronic card processing terminal, an automatic teller machine, a telephone, a cellular telephone, a radiotelephone, a portable computing device, a desktop computing device.

7. A system for preventing electronic transaction fraud, comprising:

a plurality of network-connected data processing terminals, including at least one server;

a server component configured to receive an electronic authorisation request at the server from a first data processing terminal, wherein the request is for authorising the processing of an electronic transaction associated with a cardholder's card data or account data;

a server component configured to filter the received request according to predetermined filtering criteria;

a server component configured to identify at least a second data processing terminal as a cardholder device;

a server component configured to send the request to the cardholder device, to notify the cardholder that processing of an electronic transaction is proposed, a parameter of which is said cardholder's card data or account data; and

a server component configured to receive interrupt data from the second terminal and to interrupt processing of the, or any further, electronic transaction with that card data or account data;

wherein the plurality of network-connected data processing terminals includes at least one security terminal operated by a state, official or private security organisation and further comprising means to automatically communicate interrupt data to the security terminal, whenever interrupt data is received from a second terminal for an electronic transaction and wherein the fraud reporting data corresponds to a combination of some or all of data corresponding to a geographical position, a first data processing terminal type, a financial institution identifier, a merchant identifier, image data, audio data and/or video data, as a function of whether any such data is stored at the first data processing terminal and/or at the server in connection with the reported transaction.

Claims

1. An apparatus for preventing electronic transaction fraud, comprising

a plurality of network – connected data processing terminals, including at least one server,

means for receiving an electronic authorisation request at the server from a first data processing terminal, wherein the request is for authorising the processing of an electronic transaction associated with a cardholder's card data or account data;

means for filtering the received request according to predetermined filtering criteria;

means for identifying at least a second data processing terminal as a cardholder device;

means for sending the request to the cardholder device, to notify the cardholder that processing of an electronic transaction is proposed, a parameter of which is said cardholder's card data or account data; and

means for receiving interrupt data from the second terminal and for interrupting processing of the, or any further, electronic transaction with that card data or account data.

2. Apparatus according to claim 1, further comprising means for allowing processing of the electronic transaction.

3. Apparatus according to claim 1 or 2, wherein the plurality of network – connected data processing terminals includes at least the first and second data processing terminals and the server.

4. Apparatus according to any one of claims 1 to 3, wherein the first data processing terminal data and the server are connected by a first network, and the second data processing terminal data and the server are connected by the first or a second network.

5. Apparatus according to any one of claims 1 to 3, wherein the first or second network is selected from the group comprising a public switched telephone network, a

cellular telecommunication network, a wide area network, a local area network, a wireless local area network, a virtual private network and an interbank network.

6. Apparatus according to any one of claims 1 to 5, wherein the first data processing terminal is selected from the group comprising an electronic point of sale terminal, an electronic card processing terminal, an automatic teller machine, a telephone, a cellular telephone, a radiotelephone, a portable computing device, a desktop computing device.

7. Apparatus according to any one of claims 1 to 6, wherein the at least second data processing terminal is selected from the group comprising a telephone, a cellular telephone, a radiotelephone, a pager, a personal digital assistant, a portable computing device, a desktop computing device.

8. Apparatus according to any one of claims 1 to 7, wherein the means for identifying the at least second data processing terminal comprises a database storing at least, for each cardholder, card or account data associated with a network address of at least a second data processing terminal.

9. Apparatus according to claim 8, wherein the means for identifying is adapted to identify a plurality of data processing terminals as respective devices of a same cardholder.

10. Apparatus according to any one of claims 1 to 9, wherein the means for filtering the received request according to predetermined filtering criteria comprises a filter engine.

11. Apparatus according to claim 10, wherein the predetermined filtering criteria is selected from data representative of any one, or a combination, of the group comprising a mandatory notification, an optional notification, a transaction amount threshold, a geographical position, a first data processing terminal type, a network type, a financial institution identifier, a merchant identifier.

12. Apparatus according to any one of claims 1 to 11, wherein the means for sending the request to the cardholder device comprises any one, or a combination, selected from the group comprising messaging instructions stored and processed by the at least one server, a cellular messaging server, an interactive voice response apparatus.

13. Apparatus according to any one of claims 1 to 12, wherein the means for receiving interrupt data from the second terminal and interrupting processing of the electronic transaction comprises a combination of at least one selected from the group comprising messaging instructions stored and processed by the at least one server, a cellular messaging server and an interactive voice response apparatus, respectively receiving the interrupt data from the at least second terminal, and a transaction processing terminal.

14. Apparatus according to any one of claims 1 to 13, wherein the interrupt data is any one, or a combination, selected from the group comprising a portion of card data, a portion of account data, a personal identification number, alphanumerical data representative of a user decision, digitized audio data representative of a user decision, a predetermined period of time.

15. Apparatus according to any one of claims 1 to 14, wherein the plurality of network – connected data processing terminals includes at least one security terminal operated by a state, official or private security organisation.

16. Apparatus according to claim 15, further comprising means to automatically communicate interrupt data to the security terminal, whenever interrupt data is received from a second terminal for an electronic transaction.

17. Apparatus according to claim 16, wherein the means to automatically communicate further comprises aggregating means for receiving the interrupt data and generating fraud reporting data.

18. Apparatus according to claim 16, wherein the fraud reporting data corresponds to at least one selected from the group comprising a geographical position, a first data

processing terminal type, a financial institution identifier, a merchant identifier, image data, audio data and video data, as a function of whether any such data is stored at the first data processing terminal and/or at the server in connection with the reported transaction.

19. Apparatus according to claim 16, wherein the fraud reporting data corresponds to a combination of some or all of data corresponding to a geographical position, a first data processing terminal type, a financial institution identifier, a merchant identifier, image data, audio data and/or video data, as a function of whether any such data is stored at the first data processing terminal and/or at the server in connection with the reported transaction.

20. Apparatus according to any one of claims 15 to 19, wherein the at least one security terminal is selected from the group comprising a telephone, a cellular telephone, a radiotelephone, a pager, a personal digital assistant, a portable computing device, a desktop computing device, a personal radio, a two-way radio, a mobile radio or computing device aboard a land vehicle, aircraft or ship, or a combination thereof.

21. A method of preventing electronic transaction fraud in a network comprising a plurality of network – connected data processing terminals, including at least one server, the method comprising the steps of

receiving an electronic authorisation request at the server from a first data processing terminal, wherein the request is for authorising the processing of an electronic transaction associated with a cardholder's card data or account data;

filtering the received request according to predetermined filtering criteria;

identifying at least a second data processing terminal as a cardholder device;

sending the request to the cardholder device, to notify the cardholder that processing of an electronic transaction is proposed, a parameter of which is said cardholder's card data or account data;

receiving interrupt data from the second terminal; and

interrupting processing of the, or any further, electronic transaction with that card data or account data.

22. Method according to claim 21, comprising the further step of allowing processing of the electronic transaction.

23. Method according to claim 21 or 22, comprising the further step of storing a database storing at least, for each cardholder, card or account data associated with a network address of at least a second data processing terminal.

24. Method according to any one of claims 21 to 23, wherein the step of identifying comprises the further step of identifying a plurality of data processing terminals as respective devices of a same cardholder.

25. Method according to any one of claims 21 to 24, wherein the step of filtering the received request comprises the further step of selecting data representative of any one, or a combination, of the group comprising a mandatory notification, an optional notification, a transaction amount threshold, a geographical position, a first data processing terminal type, a network type, a financial institution identifier, a merchant identifier.

26. Method according to any one of claims 21 to 25, wherein the step of sending the request to the cardholder device comprises the further step of selecting any one, or a combination, from the group comprising messaging instructions stored and processed by the at least one server, a cellular messaging server, an interactive voice response apparatus.

27. Method according to any one of claims 21 to 26, wherein the step of receiving interrupt data from the second terminal comprises the further steps of inputting interrupt data at the at least second terminal and communicating same.

28. Method according to claim 27, wherein the step of interrupting processing of the electronic transaction comprises the further steps of receiving the interrupt data at any one, or a combination, selected from the group comprising messaging instructions stored and processed by the at least one server, a cellular messaging server and an

interactive voice response apparatus, and communicating same to a transaction processing terminal.

29. Method according to any one of claims 21 to 28, comprising the further step of automatically communicating interrupt data to a security terminal, whenever interrupt data is received from a second terminal for an electronic transaction, wherein the security terminal is operated by a state, official or private security organisation.

30. Method according to claim 29, wherein the step of automatically communicating interrupt data comprises the further steps of receiving the interrupt data and generating fraud reporting data.

31. Method according to claim 30, wherein the generating step generates fraud reporting data from at least one selected from the group comprising a geographical position, a first data processing terminal type, a financial institution identifier, a merchant identifier, image data, audio data and video data, as a function of whether any such data is stored at the first data processing terminal and/or at the server in connection with the reported transaction.

32. Method according to claim 31, wherein the generating step comprises the further step of aggregating a combination of some or all of data corresponding to a geographical position, a first data processing terminal type, a financial institution identifier, a merchant identifier, image data, audio data and/or video data.

33. Method according to any one of claims 29 to 32, wherein the step of automatically communicating fraud reporting data comprises the further step of selecting the recipient security terminal from the group comprising a telephone, a cellular telephone, a radiotelephone, a pager, a personal digital assistant, a portable computing device, a desktop computing device, a personal radio, a two-way radio, a mobile radio or computing device aboard a land vehicle, aircraft or ship, or a combination thereof.

34. A carrier having a set of instructions encoded thereon which, when processed by a data processing apparatus, adapts the apparatus to perform the method of preventing card fraud according to any of claims 21 to 33.

35. A carrier according to claim 34, wherein the carrier is selected from the group comprising read – only memory means, random access memory means, optical data storage means, solid state data storage means, magnetic data storage means, electrical signal, optical signal.

36. A carrier according to claim 34 or 35, wherein the set of instructions is selected from the group comprising source code, object code, compiled code, partially compiled code, executable code.

37. Computer program product encoded on a computer – readable medium which, when processed by a data processing apparatus, adapts the apparatus to perform the method of preventing card fraud according to any of claims 21 to 33.

38. A method of preventing electronic transaction fraud in a network, comprising the steps of

receiving notification of an electronic transaction request

replying to the notification with a SMS message containing a codeword and authentication code,

automatically blocking a cardholder's payment card for future usage upon receipt of the codeword and authentication code.

39. Method according to claim 38, further comprises the step of notifying in real time the cardholder about the blocking of the card from future usage.

40. A method of preventing electronic transaction fraud in a network, comprising the steps of

contacting a phone number,

routing to an interactive voice recognition system,

inputting a code word and authentication by orally recognising the code word and authentication using speech recognition without human interaction, or keying in a selected digit and code combination, and

blocking the cardholder's payment card for future usage in response to the recognised code word and authentication or keyed in selected digit and code combination.

41. An apparatus for preventing electronic transaction fraud substantially as herein described with reference to the accompanying Figures.

42. A method of preventing electronic transaction fraud in a network substantially as herein described with reference to the accompanying Figures.