WHAT IS CLAIMED IS:

1. A server computer comprising:

a processor; and

a computer readable medium coupled to the processor, wherein the computer readable medium includes code executable by the processor for implementing a method comprising:

receiving a first authorization request message comprising a first verification value;

determining whether the first verification value is valid;

creating a second authorization request message comprising a second verification value; and

sending the second authorization request message to an issuer computer.

2. The system of claim 1, wherein the first verification value is a dynamic verification value.

3. The system of claim 1, wherein the second verification value is a static verification value.

4. The system of claim 1, further comprising:

sending a validation indicator in the second authorization request message to the server computer, wherein the validation indicator indicates whether the first verification value is valid.

5. The system of claim 1, wherein the server computer is a first server computer, and wherein the method further comprises:

receiving a duplicate copy of the first verification value from a second server computer, wherein the second server computer is operated by an IP Gateway.

6. The system of claim 5, wherein determining whether the first verification value is valid further comprises comparing the first verification value from the first authorization request message with the verification value received from the server computer operated by the IP Gateway.

7. The system of claim 1, wherein the second verification value is generated based on the transaction data in the first authorization request message

8. The system of claim 1, wherein the second verification value is associated with a portable device.

9. The system of claim 1, wherein the first authorization request message includes data associated with a portable device.

10. The system of claim 9, wherein the portable device is a payment card.

11. The system of claim 9, wherein the portable device is a mobile phone.

12. The system of claim 1, wherein the second authorization request message is in a magnetic stripe data format.

13. The system of claim 1, further comprising:

determining whether the first authorization request message includes a static verification value associated with a portable device when the first verification value is not valid.

14. A method comprising:

receiving a first authorization request message comprising a first verification value;

determining whether the first verification value is valid;

creating a second authorization request message comprising a second verification value; and

sending the second authorization request message to a server computer.

15. The method of claim 14, further comprising:

determining whether the first authorization request message includes a static verification value associated with a portable device when the first verification value is not valid.

16. The method of claim 14, further comprising:

sending a validation indicator in the second authorization request message to the server computer, wherein the validation indicator indicates whether the first verification value is valid.

17. The method of claim 14, wherein the first verification value is a dynamic verification value and wherein the second verification value is a static verification value.

18. The method of claim 14, wherein the second verification value is generated based on the data in the first authorization request message.

19. A method comprising:

receiving an authorization request message associated with a payment transaction from a first server computer;

receiving a validation indicator from the first server computer, wherein the validation indicator indicates whether a verification value associated with the payment transaction is valid; and

generating an authorization response message based on the validation indicator.

20. The method of claim 19, wherein the verification value is further associated with a portable device.

21. The method of claim 20, where in the portable device is a payment card.

22. The method of claim 20, wherein the portable device is a mobile phone.

CLAIMS:

1. A server computer comprising:

a processor; and

a computer readable storage medium coupled to the processor, having code stored thereon which is executable by the processor for implementing a payment transaction authentication method, the method comprising:

receiving a first authorization request message, associated with a credit or debit account, the authorization request message comprising a first verification value;

determining whether the first verification value is valid;

creating a second authorization request message comprising a second verification value, wherein the second authorization request message is created by replacing the first verification value with the second verification value after determining that the first verification value is valid;

including a validation indicator in the second authorization request message after validating the first verification value, wherein the validation indicator indicates whether the first verification value is valid; and

sending the second authorization request message to an issuer computer.

2. The server computer of claim 1, wherein the first verification value is a dynamic verification value.

3. The server computer of claim 2, wherein the second verification value is a static verification value.

4. The server computer of claim 1, wherein the server computer is a first server computer, and wherein the method further comprises:

receiving a duplicate copy of the first verification value from a second server computer, wherein the second server computer is operated by an IP Gateway.

5. The server computer of claim 4, wherein determining whether the first verification value is valid further comprises comparing the first verification value from the first authorization request message with the duplicate copy of the first verification value received from the server computer operated by the IP Gateway.

6. The server computer of claim 1, wherein the second verification value is generated based on transaction data in the first authorization request message.

7. The server computer of claim 1, wherein the second verification value is associated with a portable device.

8. The server computer of claim 1, wherein the first authorization request message includes data associated with a portable device.

9. The server computer of claim 8, wherein the portable device is a payment card.

10. The server computer of claim 8, wherein the portable device is a mobile phone.

11. The server computer of claim 1, wherein the second authorization request message is in a magnetic stripe data format.

12. The server computer of claim 1, further comprising:

determining whether the first authorization request message includes a static verification value associated with a portable device when the first verification value is not valid.

13. The server computer of claim 1, wherein the first authorization request message is received from a first communication channel.

14. The server computer of claim 13, wherein the second authorization request message is sent via a second communication channel different from the first communication channel to the issuer computer.

15. The server computer of claim 13, wherein the first communication channel is configured to establish communication between a client computer and an IP Gateway server computer coupled to a payment processing network.

16. The server computer of claim 14 wherein the second communication channel is configured to establish communication between a payment processing network and the issuer computer.

17. The server computer of claim 14, wherein the first authorization request message received from the first communication channel includes dynamic verification value, and wherein the second authorization request message sent to the issuer computer includes static verification value.

18. The server computer of claim 2, wherein the dynamic verification value is placed in a field of the first authorization request message reserved for the static verification value.

19. The server computer of claim 3, wherein the static verification value in the second authorization request message is generated in a format that can be processed by the issuer computer.

20. The server computer of claim 2, further comprising a comparison module operable to determine whether the dynamic verification value in the first authorization request message is valid by comparing it with a duplicate copy of the dynamic verification value received from a server computer operated by an IP Gateway.

21. The server computer of claim 18, further comprising a counter operable to keep track of a number of transactions that are conducted by the user using the dynamic verification value and to cause it to change with each transaction.

22. A method comprising:

receiving a first authorization request message at a server computer, associated with a credit or debit account, the authorization request message comprising a first verification value;

determining whether the first verification value is valid;

creating a second authorization request message comprising a second verification value at the first server computer, wherein the second authorization request message is created by replacing the first verification value with the second verification value after determining that the first verification value is valid;

including a validation indicator in the second authorization request message after validating the first verification value, wherein the validation indicator indicates whether the first verification value is valid; and

sending the second authorization request message including the second verification value and the validation indicator to a second server computer operated by an issuer of the credit or debit account when the first verification value is valid.

23. The method of claim 22, further comprising:

determining whether the first authorization request message includes a static verification value associated with a portable device when the first verification value is not valid.

24. The method of claim 22, further comprising:

sending a validation indicator in the second authorization request message to the second server computer, wherein the validation indicator indicates whether the first verification value is valid.

25. The method of claim 22, wherein the first verification value is a dynamic verification value and wherein the second verification value is a static verification value.

26. The method of claim 22, wherein the second verification value is generated based on the data in the first authorization request message.

27. A computer implemented method comprising:

receiving an authorization request message associated with a payment transaction from a first server computer associated with a payment processing entity, wherein the payment transaction is associated with a credit or debit account, wherein the authorization request message is received using a second server computer associated with an issuer of the credit or debit account;

receiving, using the second server computer, a validation indicator from the first server computer, wherein the validation indicator indicates whether a verification value associated with the payment transaction is valid, wherein validation of the verification value comprises validating a dynamic verification value and replacing the dynamic verification value with a static verification value known to the second server computer associated with an issuer of the credit or debit account; and

generating, using the second server computer an authorization response message based on the validation indicator; and

sending the authorization response message to the first server computer of the payment processing entity.

28. The method of claim 27, wherein the verification value is further associated with a portable device.

29. The method of claim 28, where in the portable device is a payment card.

30. The method of claim 28, wherein the portable device is a mobile phone.

31. A server computer comprising:

a processor; and

a computer readable storage medium, coupled to the processor, having code stored thereon which is executable by the processor for implementing a payment transaction authentication method, the method comprising:

receiving an authorization request message associated with a payment transaction from a second server computer associated with a payment processing entity, wherein the payment

transaction is associated with a credit or debit account, wherein the server computer is associated with an issuer of the credit or debit account;

receiving a validation indicator from the second server computer, wherein the validation indicator indicates whether a verification value associated with the payment transaction is valid, wherein validation of the verification value comprises validating a dynamic verification value and replacing the dynamic verification value with a static verification value known to the server computer; and

generating an authorization response message based on the validation indicator; and

sending the authorization response message to the second server computer.