Claims

1. A payment network server for processing an electronic commerce (e-commerce) transaction initiated by a customer, the server comprising at least a computer processor and a data storage device, the data storage device comprising instructions operative by the processor to:

receive, from a merchant server, an authentication request, the authentication request comprising at least a payment card identifier associated with a payment card;

generate an authentication code associated with the e-commerce transaction for authenticating the customer, a portion of the authentication code comprising a unique identifier;

store, in a payment network database, the authentication code as a stored authentication code;

transmit, the unique identifier to the merchant server, wherein the merchant server presents the unique identifier to the consumer via a merchant website associated with the merchant server;

transmit, the authentication code ~~for transmission to the customer~~ and an indication of the payment card to an issuer server, wherein the issuer server communicates the authentication code to the customer;

receive, from the merchant server, a customer entered authentication code which was entered by the customer into ~~a merchant website associated with~~ the merchant ~~server~~ website;

determine if the customer entered authentication code matches the stored authentication code; and

if the customer entered authentication code matches the stored authentication code:

generate an authentication indication;

store, in the payment network database, the authentication indication as a stored authentication indication; and

transmit, to the merchant server, an authentication response comprising the authentication indication.

2. The server of claim 1, wherein the processor is further configured to:

receive, from the merchant server, a transaction request comprising a received authentication indication, the payment card identifier and a payment amount associated with the e-commerce transaction;

determine if the received authentication indication matches the stored authentication indication;

generate an on-behalf service message if the received authentication indication matches the stored authentication indication, the on-behalf service message indicating that the e-commerce transaction has been authenticated;

transmit, to the issuer server, an authorisation request comprising the on-behalf service message, the indication of the payment card and the payment amount;

receive, from the issuer server, an authorisation response indicating if the e-commerce transaction is authorised or refused; and

transmit, to the merchant server, a transaction response indicating whether the e-commerce transaction is approved or refused, the e-commerce transaction is approved if it is authorised.

3. The server of claim 1 ~~or claim 2~~, wherein the merchant website is designed using an application programming interface associated with the payment network server.
4. The server of ~~any one of the preceding~~ claim~~s~~ 1, wherein the payment card identifier comprises a payment card number of the payment card.
5. The server of ~~any one of~~ claim~~s~~ 1 ~~to 3~~, wherein the payment card identifier comprises a token, the processor is further configured to identify, using the payment network database, a payment card number associated with the token, and the indication of the payment card.
6. The server of ~~any one of the preceding~~ claim~~s~~ 1, wherein the authentication code is a one-time password.
7. The server of ~~any one of the preceding~~ claim~~s~~ 1, wherein the authentication code is valid for a predetermined authentication code time period.
8. The server of ~~any one of the preceding~~ claim~~s~~ 1, wherein the authentication indication is valid for a predetermined authentication indication time period.
9. The server of claim 8, wherein the predetermined authentication indication time period is determined by the issuer server.
10. The server of ~~any one of the preceding~~ claim~~s~~ 1, wherein the authentication indication is an accountholder authorisation value (AAV) or a cardholder authentication verification value (CAVV).
11. A computerised method for processing an e-commerce transaction initiated by a customer, the method comprising:

receiving, from a merchant server, an authentication request, the authentication request comprising at least a payment card identifier;

generating an authentication code associated with the e-commerce transaction for authenticating the customer, a portion of the authentication code comprising a unique identifier;

storing, in a payment network database, the authentication code as a stored authentication code;

transmitting, the unique identifier to the merchant server, wherein the merchant server presents the unique identifier to the consumer via a merchant website associated with the merchant server;

transmitting, the authentication code ~~for transmission to the customer~~ and an indication of the payment card to an issuer server, wherein the issuer server communicates the authentication code to the customer;

receiving, from the merchant server, a customer entered authentication code which was entered by the customer into a merchant website associated with the merchant server;

determining if the customer entered authentication code matches the stored authentication code; and

if the customer entered authentication code matches the stored authentication code:

generating an authentication indication;

storing, in the payment network database, the authentication indication as a stored authentication indication; and

transmitting, to the merchant server, an authentication response comprising the authentication indication.

12. The method of claim 11 further comprising:

receiving, from the merchant server, a transaction request comprising a received authentication indication, the payment card identifier and a payment amount associated with the e-commerce transaction;

determining if the received authentication indication matches the stored authentication indication;

generating an on-behalf service message if the received authentication indication matches the stored authentication indication, the on-behalf service message indicating that the e-commerce transaction has been authenticated;

transmitting, to the issuer server, an authorisation request comprising the on-behalf service message, the indication of the payment card and the payment amount;

receiving, from the issuer server, an authorisation response indicating if the e-commerce transaction is authorised or refused; and

transmitting, to the merchant server, a transaction response indicating whether the e-commerce transaction is approved or refused, the e-commerce transaction is approved if it is authorised.

13. The method of claim 11 ~~or claim 12~~, wherein the merchant website is designed using an application programming interface associated with the payment network server.

14. The method of ~~any one of~~ claim~~s~~ 11 ~~to 13~~, wherein the payment card identifier comprises a payment card number associated with the payment card.

15. The method of ~~any one of~~ claim~~s~~ 11 ~~to 13~~, wherein the payment card identifier is in the form of a token, the method further comprises identifying, using the payment network database, a payment card number associated with the token, and the indication of the payment card.

16. The method of ~~any one of~~ claim~~s~~ 11 ~~to 15~~, wherein the authentication code is a one-time password.

17. The method of ~~any one of~~ claim~~s~~ 11 ~~to 16~~, wherein the authentication code is valid for a predetermined authentication code time period.

18. The method of ~~any one of~~ claim~~s~~ 11 ~~to 17~~, wherein the authentication indication is valid for a predetermined authentication indication time period.

19. The method of claim 18, wherein the predetermined authentication indication time period is determined by the issuer server.

20. A non-transitory computer-readable medium having stored thereon program instructions for causing at least one processor to; ~~perform the method according to any one of claims 11 to 19.~~

receive, from a merchant server, an authentication request, the authentication request comprising at least a payment card identifier;

generate an authentication code associated with the e-commerce transaction for authenticating the customer, a portion of the authentication code comprising a unique identifier;

store, in a payment network database, the authentication code as a stored authentication code;

transmit the unique identifier to the merchant server, wherein the merchant server presents the unique identifier to the consumer via a merchant website associated with the merchant server;

transmit the authentication code and an indication of the payment card to an issuer server, wherein the issuer server communicates the authentication code to the customer;

receive, from the merchant server, a customer entered authentication code which was entered by the customer into a merchant website associated with the merchant server;

determine if the customer entered authentication code matches the stored authentication code; and

if the customer entered authentication code matches the stored authentication code:

generate an authentication indication;

store, in the payment network database, the authentication indication as a stored authentication indication; and

transmit, to the merchant server, an authentication response comprising the authentication indication.