

CLAIMS:

1. A computer-implemented method comprising:
 - receiving a first authentication parameter from a user, the first authentication parameter being associated with a user payment account;
 - receiving a first iteration of a transaction request from a merchant server, the transaction request including an identifier of the user payment account and a merchant identifier;
 - determining that the merchant identifier is associated with an untrustworthy merchant;
 - transmitting a request to re-submit the transaction request to the merchant server;
 - in response to determining that the merchant identifier is associated with an untrustworthy merchant, transmitting an authentication request to a computing device associated with the user payment account;
 - receiving a second authentication parameter from the computing device in response to the authentication request;
 - determining that the second authentication parameter matches the first authentication parameter;
 - receiving a second iteration of the transaction request from the merchant server in response to the request to re-submit the transaction request; and
 - approving the second iteration of the transaction request based on the determination that the second authentication parameter matches the first authentication parameter;
- wherein the method is performed using one or more processors.
2. The method of claim 1, wherein the first and second authentication parameters are a fingerprint of the user.
3. The method of claim 1, wherein the first and second authentication parameters are a facial recognition of the user.
4. The method of claim 1, wherein the first and second authentication parameters are a password.
5. The method of claim 1, wherein the authentication request is configured to trigger a notification on the computing device.

6. The method of claim 5, wherein the authentication request is configured to receive an authentication confirmation from the user.

7. The method of claim 1, wherein the request to re-submit the transaction request is transmitted using one or more ISO MTI codes.

8. The method of claim 7, wherein the one or more ISO MTI codes include a code indicating a request to re-submit the transaction request.

9. A computer-implemented method comprising:
receiving a first iteration of a transaction request including an identifier of a user payment account;

determining that the transaction request includes a likelihood of fraud that exceeds a predetermined fraud threshold;

based on the determination that the transaction request includes a likelihood of fraud that exceeds the predetermined fraud threshold, transmitting an authentication request to a computing device associated with the user payment account and transmitting a request to re-submit the transaction request;

in response to the authentication request, receiving an authentication parameter from the computing device;

determining that the authentication parameter matches an authentication parameter associated with the user payment account;

in response to the request to re-submit the transaction request, receiving a second iteration of the transaction request; and

approving the second iteration of the transaction request based on the determination that the authentication parameter received from the computing device matches the authentication parameter associated with the user payment account;

wherein the method is performed using one or more processors.

10. The method of claim 9, wherein the authentication parameters are a fingerprint of a user associated with the user payment account.

11. The method of claim 9, wherein the authentication parameters are a facial recognition of a user associated with the user payment account.

12. The method of claim 9, wherein the authentication parameters are a password.

13. The method of claim 9, wherein the authentication request is configured to trigger a notification on the computing device.

14. The method of claim 13, wherein the authentication request is configured to receive an authentication confirmation from a user associated with the user payment account.

15. The method of claim 9, wherein the transaction request further comprises receiving a merchant identifier, and wherein determining that the transaction request includes a likelihood of fraud that exceeds the predetermined fraud threshold includes determining that a merchant associated with the merchant identifier is an untrustworthy merchant.

16. A computer-implemented method comprising:
receiving a first iteration of a transaction request including an identifier of a user payment account from a merchant server;

in response to receiving the first iteration of the transaction request, transmitting an authentication request to a computing device associated with the user payment account and transmitting a request to re-submit the transaction request to the merchant server;

receiving an authentication parameter from the computing device in response to the authentication request;

determining that the authentication parameter received from the computing device matches an authentication parameter associated with the user payment account;

receiving a second iteration of the transaction request from the merchant server;
and

based on the determination that the authentication parameter received from the computing device matches the authentication parameter associated with the user payment account, approving the second iteration of the transaction request;

wherein the method is performed using one or more processors.

17. The method of claim 16, wherein the request to re-submit the transaction request is transmitted using one or more ISO MTI codes.

18. The method of claim 17, wherein the one or more ISO MTI codes include a code indicating a request to re-submit the transaction request.

19. The method of claim 16, wherein the authentication parameters are a fingerprint of a user associated with the user payment account.

20. The method of claim 16, wherein the authentication parameters are a facial recognition of a user associated with the user payment account.

CLAIMS:

1. A computer-implemented method comprising:

receiving, at an authentication server, a first authentication parameter from a user, the first authentication parameter being associated with a user payment account;

receiving, at the authentication server, a first iteration of a transaction request from a merchant server associated with a merchant, the transaction request including an identifier of the user payment account and a merchant identifier;

determining, by the authentication server via one or more processors, that the merchant identifier is associated with an untrustworthy merchant;

in response to determining that the merchant identifier is associated with an untrustworthy merchant:

transmitting, to the merchant server from the authentication server, an ISO message type indicator (MTI) file populated with a code requesting that the merchant server re-submit the transaction request to provide an opportunity to authenticate the transaction request, and

transmitting, from the authentication server, an authentication request to a computing device associated with the user payment account, the authentication request including a merchant name associated with the merchant;

receiving, at the authentication server, a second authentication parameter from the computing device in response to the authentication request, the second authentication parameter indicating that the transaction request from the merchant server is legitimate;

determining, by the authentication server via the one or more processors, that the second authentication parameter matches the first authentication parameter;

receiving, at the authentication server, a second iteration of the transaction request from the merchant server in response to the code requesting that the merchant server request to re-submit the transaction request; and

approving, by the authentication server via the one or more processors, the second iteration of the transaction request based on the determination that the second authentication parameter matches the first authentication parameter.

2. The method of claim 1, wherein the first and second authentication parameters are a fingerprint of the user.

3. The method of claim 1, wherein the first and second authentication parameters are a facial recognition of the user.

4. The method of claim 1, wherein the first and second authentication parameters are a password.
5. The method of claim 1, wherein the authentication request is configured to trigger a notification on the computing device.
6. The method of claim 5, wherein the authentication request is configured to receive an authentication confirmation from the user.
7. A computer-implemented method comprising:
 - receiving, at an authentication server, a first iteration of a transaction request including an identifier of a user payment account;
 - determining, at the authentication server via one or more processors, that the transaction request includes a likelihood of fraud that exceeds a predetermined fraud threshold;
 - based on the determination that the transaction request includes a likelihood of fraud that exceeds the predetermined fraud threshold, transmitting, from the authentication server:
 - an authentication request to a computing device associated with the user payment account, and
 - an ISO message type indicator (MTI) file populated with a code requesting re-submission of transaction request;
 - in response to the authentication request, receiving, at the authentication server, an authentication parameter from the computing device;
 - determining, by the authentication server via the one or more processors, that the authentication parameter matches an authentication parameter associated with the user payment account;
 - in response to the code requesting re-submission of the transaction request, receiving, at the authentication server, a second iteration of the transaction request; and
 - approving, by the authentication server via the one or more processors, the second iteration of the transaction request based on the determination that the authentication parameter received from the computing device matches the authentication parameter associated with the user payment account.
8. The method of claim 7, wherein the authentication parameters are a fingerprint of a user associated with the user payment account.
9. The method of claim 7, wherein the authentication parameters are a facial recognition of a

user associated with the user payment account.

10. The method of claim 7, wherein the authentication parameters are a password.

11. The method of claim 7, wherein the authentication request is configured to trigger a notification on the computing device.

12. The method of claim 11, wherein the authentication request is configured to receive an authentication confirmation from a user associated with the user payment account.

13. The method of claim 7, wherein the transaction request further comprises receiving a merchant identifier, and wherein determining that the transaction request includes a likelihood of fraud that exceeds the predetermined fraud threshold includes determining that a merchant associated with the merchant identifier is an untrustworthy merchant.

14. A computer-implemented method comprising:

receiving, at an authentication server, a first iteration of a transaction request including an identifier of a user payment account from a merchant server associated with a merchant;

in response to receiving the first iteration of the transaction request, transmitting, by the authentication server:

an authentication request to a computing device associated with the user payment account, and

an ISO message type indicator (MTI) file populated with a code requesting that the merchant server re-submit the transaction request;

receiving, at the authentication server, an authentication parameter from the computing device in response to the authentication request;

determining, by the authentication server via one or more processors, that the authentication parameter received from the computing device matches an authentication parameter associated with the user payment account;

receiving, at the authentication server, a second iteration of the transaction request from the merchant server; and

based on the determination that the authentication parameter received from the computing device matches the authentication parameter associated with the user payment account, approving, by the authentication server via one or more processors, the second iteration of the transaction request.

15. The method of claim 14, wherein the authentication parameters are a fingerprint of a user associated with the user payment account.

16. The method of claim 14, wherein the authentication parameters are a facial recognition of a user associated with the user payment account.