

WHAT IS CLAIMED IS:

1. A computer-implemented method for authenticating devices, comprising:

generating, with a transaction processing system comprising at least one processor, a virtual authenticator comprising at least one authentication input, at least one account identifier associated with at least one payment account, and at least one device identifier of at least one client device, the virtual authenticator associated with a virtual authenticator identifier, the virtual authenticator comprising a graph data structure comprising a plurality of nodes representing the at least one authentication input, the at least one account identifier, and the at least one device identifier;

receiving, with the transaction processing system, a transaction request message associated with a transaction between a user and a merchant made using an authentication input of the at least one authentication input and a client device of the at least one client device, the transaction request message comprising a second account identifier different than the at least one account identifier of the virtual authenticator, wherein the at least one account identifier corresponds to a first payment account, and wherein the second account identifier corresponds to a second payment account different than the first payment account;

linking, with the transaction processing system, the second account identifier to the virtual authenticator in response to receiving the transaction request;

communicating, with the transaction processing system, an authorization request message to an issuer system, the authorization request message comprising the virtual authenticator identifier, wherein the issuer system generates an authorization response message based on the virtual authenticator;

receiving, with the at least one processor of the transaction processing system, the authorization response message; and

updating, with the at least one processor of the transaction processing system, the virtual authenticator based on the authorization response message, resulting in an updated virtual authenticator.

2. The computer-implemented method of claim 1, wherein the transaction request message further comprises a merchant identifier, and wherein the virtual authenticator further comprises the merchant identifier.

3. The computer-implemented method of claim 1, further comprising:

receiving, with at least one processor of the transaction processing system, a plurality of additional transaction requests associated with a plurality of subsequent transactions between the user and the merchant, wherein at least one additional transaction request of the plurality of additional transaction requests comprises the second account identifier and a second authentication input.

4. The computer-implemented method of claim 1, further comprising:

associating an authentication identifier with the virtual authenticator, wherein the authentication identifier uniquely identifies the virtual authenticator and is not communicated to the issuer system.

5. The computer-implemented method of claim 1, further comprising:

generating, with the issuer system comprising at least one processor, a registration code based on account data associated with the payment account;

receiving, with the issuer system, a confirmation message generated by the client device based on the registration code, the least one device identifier, and the at least one authentication input;

communicating, with the issuer system, authentication data to the transaction processing system, the authentication data comprising the account identifier, at least one device identifier, and the at least one authentication input;

generating, with the at least one processor of a transaction processing system, an authentication graph based on the authentication data;

receiving, with the at least one processor of the transaction processing system, a transaction request message associated with a transaction between the user and the merchant, the transaction request message comprising the account identifier;

determining, with at least one processor, an authentication result based on the transaction request message and the authentication graph; and

updating, with at least one processor, the authentication graph based on the authentication result.

6. A system for authenticating devices, the system comprising:
at least one processor programmed or configured to:

generate a virtual authenticator comprising at least one authentication input, at least one account identifier associated with at least one payment account, and at least one device identifier of at least one client device, the virtual authenticator associated with a virtual authenticator identifier, the virtual authenticator comprising a graph data structure comprising a plurality of nodes representing the at least one authentication input, the at least one account identifier, and the at least one device identifier;

receive a transaction request message associated with a transaction between a user and a merchant made using an authentication input of the at least one authentication input and a client device of the at least one client device, the transaction request message comprising a second account identifier different than the at least one account identifier of the virtual authenticator, wherein the at least one account identifier corresponds to a first payment account, and wherein the second account identifier corresponds to a second payment account different than the first payment account;

link the second account identifier to the virtual authenticator in response to receiving the transaction request;

communicate an authorization request message to an issuer system, the authorization request message comprising the virtual authenticator identifier, wherein the issuer system generates an authorization response message based on the virtual authenticator;

receive the authorization response message; and

update the virtual authenticator based on the authorization response message, resulting in an updated virtual authenticator.

7. The system of claim 6, wherein the transaction request message further comprises a merchant identifier, and wherein the virtual authenticator further comprises the merchant identifier.

8. The system of claim 6, wherein the at least one processor is further programmed or configured to:

receive a plurality of additional transaction requests associated with a plurality of subsequent transactions between the user and the merchant, wherein at least one additional transaction request of the plurality of additional transaction requests comprises the second account identifier and a second authentication input.

9. The system of claim 6, wherein the at least one processor is further programmed or configured to:

associate an authentication identifier with the virtual authenticator, wherein the authentication identifier uniquely identifies the virtual authenticator and is not communicated to the issuer system.

10. The system of claim 6, further comprising the issuer system configured to:

generate a registration code based on account data associated with the payment account;

receive a confirmation message generated by the client device based on the registration code, the least one device identifier, and the at least one authentication input;

communicate authentication data to a transaction processing system, the authentication data comprising the account identifier, at least one device identifier, and the at least one authentication input,

wherein the at least one processor is further programmed or configured to:

generate an authentication graph based on the authentication data;

receive a transaction request message associated with a transaction between the user and the merchant, the transaction request message comprising the account identifier;

determine an authentication result based on the transaction request message and the authentication graph; and

update the authentication graph based on the authentication result.

11. A computer program product for authenticating devices, the computer program product comprising at least one non-transitory computer-readable medium comprising one or more program instructions that, when executed by at least one processor cause the at least one processor to:

generate a virtual authenticator comprising at least one authentication input, at least one account identifier associated with at least one payment account, and at least one device identifier of at least one client device, the virtual authenticator associated with a virtual authenticator identifier, the virtual authenticator comprising a graph data structure comprising a plurality of nodes representing the at least one authentication input, the at least one account identifier, and the at least one device identifier;

receive a transaction request message associated with a transaction between a user and a merchant made using an authentication input of the at least one authentication input and a client device of the at least one client device, the transaction request message comprising a second account identifier different than the at least one account identifier of the virtual authenticator, wherein the at least one account identifier corresponds to a first payment account, and wherein the second account identifier corresponds to a second payment account different than the first payment account;

link the second account identifier to the virtual authenticator in response to receiving the transaction request;

communicate an authorization request message to an issuer system, the authorization request message comprising the virtual authenticator identifier, wherein the issuer system generates an authorization response message based on the virtual authenticator;

receive the authorization response message; and

update the virtual authenticator based on the authorization response message, resulting in an updated virtual authenticator.

12. The computer program product of claim 11, wherein the transaction request message further comprises a merchant identifier, and wherein the virtual authenticator further comprises the merchant identifier.

13. The computer program product of claim 11, wherein the program instructions further cause the at least one processor to:

receive a plurality of additional transaction requests associated with a plurality of subsequent transactions between the user and the merchant, wherein at least one additional transaction request of the plurality of additional transaction requests comprises the second account identifier and a second authentication input.

14. The computer program product of claim 11, wherein the program instructions further cause the at least one processor to:

associate an authentication identifier with the virtual authenticator, wherein the authentication identifier uniquely identifies the virtual authenticator and is not communicated to the issuer system.

15. The computer program product of claim 11, wherein the program instructions further cause the issuer system in communication with the at least one processor to:

generate a registration code based on account data associated with the payment account;

receive a confirmation message generated by the client device based on the registration code, the least one device identifier, and the at least one authentication input;

communicate authentication data to a transaction processing system, the authentication data comprising the account identifier, at least one device identifier, and the at least one authentication input,

wherein the program instructions further cause the at least one processor to:

generate an authentication graph based on the authentication data;

receive a transaction request message associated with a transaction between the user and the merchant, the transaction request message comprising the account identifier;

determine an authentication result based on the transaction request message and the authentication graph; and

update the authentication graph based on the authentication result.