

WHAT IS CLAIMED IS:

1 1. A computer-implemented method comprising:
2 receiving, by an access control server via a directory server from an
3 authentication requestor, an authentication process message associated with an
4 authentication request comprising an account identifier, and information regarding a
5 prior authentication method on the account identifier and a current authentication
6 method for the account identifier associated with a transaction, wherein the information
7 regarding the prior authentication method on the account identifier and the current
8 authentication method for the account identifier are represented by one or more values
9 that are appended to the authentication process message, a value of the one or more
10 values representing a unique type of authentication provided by a processing network;
11 performing, by the access control server, a risk analysis for the transaction
12 based at least in part on the information and a threshold;
13 authenticating, by the access control server, a user of the account
14 identifier using the information, the account identifier, and a result of the risk analysis;
15 generating, by the access control server, an authentication response;
16 modifying, by the access control server, the an-authentication response to
17 include an authentication indicator by setting a value in the authentication response that
18 represents a strength of a verification result for the transaction based at least in part on
19 the prior authentication method on the account identifier and the current authentication
20 method for the account identifier; and
21 transmitting, by the access control server, the authentication response to
22 the authentication requestor.

1 2. The computer-implemented method of claim 1, wherein the
2 information further includes transaction data for the transaction and personal
3 information for the user associated with the transaction.

1 3. The computer-implemented method of claim 1 further comprising
2 generating, by a service provider application associated with the account identifier, a set
3 intent message that includes a user identifier, a service provider payment account
4 identifier, and transaction data for the transaction.

1 4. The computer-implemented method of claim 3, further comprising
2 generating, by a service provider computer associated with the service provider

3 application, an attestation signature for the transaction based at least in part on input
4 provided by the user associated with the transaction.

1 ~~5. The computer-implemented method of claim 1, wherein the~~
2 ~~information regarding the prior authentication method on the account identifier and the~~
3 ~~current authentication method for the account identifier are represented by one or more~~
4 ~~values that are appended to a message associated with the authentication request.~~

~~6. The computer-implemented method of claim 5, wherein a value of the one or more value represents a unique type of authentication provided by a processing network.~~

~~7. The computer-implemented method of claim 1, wherein modifying the authentication response to include the authentication indicator comprises setting a value in the authentication response that represents a strength of a verification result for the transaction based at least in part on the prior authentication method on the account identifier and the current authentication method for the account identifier.~~

58. The computer-implemented method of claim 1, wherein the current authentication method for the account identifier associated with the transaction is performed by a service provider application associated with the account identifier and the transaction.

69. The computer-implemented method of claim 1, wherein the current authentication method includes at least one of a first login to an account using an authorizing entity authentication process, a second login to the account through a service provider application authentication process, or a third login to the account using a third party authentication process.

710. The computer-implemented method of claim 1, wherein the prior authentication method includes at least one of a billing address verification process, a online authentication process risk based analysis using device information from a user device associated with the transaction process, a online authentication process challenge process that includes a username and password login provisioning, a tokenization process, or an issuer inline provisioning process.

811. The computer-implemented method of claim 1, wherein the result of the risk analysis includes a negative verification of the transaction in response to a determination that the risk analysis for the transaction is less than the threshold, or a positive verification of the transaction in response to a determination that the risk analysis for the transaction is greater than the threshold.

912. An access control server comprising:
a processor; and

3 a computer readable medium coupled to the processor, the computer
4 readable medium comprising code, executable by the processor, to implement a
5 method comprising:

6 receiving, by ~~the~~ an access control server via a directory server from an
7 authentication requestor, an authentication process message associated with an
8 authentication request comprising an account identifier, and information regarding a
9 prior authentication method on the account identifier and a current authentication
10 method for the account identifier associated with a transaction, wherein the information
11 regarding the prior authentication method on the account identifier and the current
12 authentication method for the account identifier are represented by one or more values
13 that are appended to the authentication process message, a value of the one or more
14 values representing a unique type of authentication provided by a processing network;

15 performing, by the access control server, a risk analysis for the transaction
16 based at least in part on the information and a threshold;

17 authenticating, by the access control server, the user of the account
18 identifier using the information, the account identifier, and a result of the risk analysis;

19 generating, by the access control server, an authentication response;

20 modifying, by the access control server, ~~the~~ an authentication response to
21 include an authentication indicator by setting a value in the authentication response that
22 represents a strength of a verification result for the transaction based at least in part on
23 the prior authentication method on the account identifier and the current authentication
24 method for the account identifier; and

25 transmitting, by the access control server, the authentication response to
26 the authentication requestor.

1 ~~1013~~. The access control server of claim ~~912~~, wherein the information
2 further includes transaction data for the transaction and personal information for a user
3 associated with the transaction.

1 ~~1114~~. The access control server of claim ~~912~~, wherein the method further
2 comprises generating, by a service provider application associated with the account
3 identifier, a set intent message that includes a user identifier, a service provider
4 payment account identifier, and transaction data for the transaction, the service provider
5 application associated with a service provider computer, the service provider application
6 and the service provider computer separate from the access control server and in
7 communication with the access control server.

1 ~~12~~¹⁵. The access control server of claim ~~11~~¹⁴, wherein the method
2 further comprises generating, by the service provider computer associated with the
3 service provider application, an attestation signature for the transaction based at least in
4 part on input provided by a user associated with the transaction.

1 ~~16.~~ The access control server of claim ~~12~~, wherein the information
2 regarding the prior authentication method on the account identifier and the current
3 authentication method for the account identifier are represented by one or more values
4 that are appended to a message associated with the authentication request.

1 ~~17.~~ The access control server of claim 12, wherein a value of the one
2 ~~or more value represents a unique type of authentication provided by a payment~~
3 ~~processing network.~~

1 ~~18.~~ The access control server of claim 12, wherein modifying the
2 ~~authentication response to include the authentication indicator comprises setting a value~~
3 ~~in the authentication response that represents a strength of a verification result for the~~
4 ~~transaction based at least in part on the prior authentication method on the account~~
5 ~~identifier and the current authentication method for the account identifier.~~

1 ~~1319.~~ The access control server of claim ~~912~~, wherein the result of the
2 risk analysis includes a negative verification of the transaction in response to a
3 determination that the risk analysis for the transaction is less than the threshold, or a
4 positive verification of the transaction in response to a determination that the risk
5 analysis for the transaction is greater than the threshold.

1 ~~1420.~~ A directory server comprising:
2 a processor; and
3 a computer readable medium coupled to the processor, the computer
4 readable medium comprising code, executable by the processor, to implement a
5 method comprising:
6 receiving, by the directory server from an authentication requestor, an
7 authentication process message associated with an authentication request comprising
8 an account identifier, and information regarding a prior authentication method on the
9 account identifier and a current authentication method for the account identifier
10 associated with a transaction, the current authentication method for the account
11 identifier including a signature for the transaction, the information regarding the prior
12 authentication method on the account identifier and the current authentication method
13 for the account identifier are represented by one or more values that are appended to
14 the authentication process message, a value of the one or more values representing a
15 unique type of authentication provided by a processing network;

16 verifying, by the directory server, the signature of the information;

17 modifying, by the directory server, an authentication response to include
18 the verification of the signature; and

19 transmitting, by the directory server, the authentication response to the
20 authentication requestor thereby bypassing an access control server for the transaction.

1 ~~1521~~. A method comprising:
2 receiving, by a directory server from an authentication requestor, an
3 authentication process message associated with an authentication request comprising
4 an account identifier, and information regarding a prior authentication method on the
5 account identifier and a current authentication

6 method for the account identifier associated with a transaction, the current
7 authentication method for the account identifier including a signature for the transaction,
8 the information regarding the prior authentication method on the account identifier and
9 the current authentication method for the account identifier are represented by one or
10 more values that are appended to the authentication process message, a value of the
11 one or more values representing a unique type of authentication provided by a
12 processing network;
13 verifying, by the directory server, the signature of the information;
14 modifying, by the directory server, an authentication response to include
15 the verification of the signature; and
16 transmitting, by the directory server, the authentication response to the
17 authentication requestor thereby bypassing an access control server for the transaction.