

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:
 - receiving, by a processing computer from a transport computer or a resource provider computer, an authorization request message for a transaction and a session identifier, the session identifier generated by the resource provider computer and associated with data for one or more interactions by a user associated with the transaction and stored in a supplemental database;
 - obtaining, by the processing computer and from the supplemental database, a portion of pre-analyzed data about the user and the one or more interactions based at least in part on the session identifier;
 - performing, by the processing computer, a risk analysis for the transaction using the portion of the pre-analyzed data to generate a value, the value representing a likelihood of a fraudulent transaction for the transaction;
 - modifying, by the processing computer, the authorization request message to include the portion of the pre-analyzed data and the valuescore;
 - transmitting, by the processing computer and to an authorizing computer, the modified authorization request message; and
 - transmitting, by the processing computer to the transport computer, an authorization response message from the authorizing computer, the authorizing computer generating the authorization response message based on the modified authorization request message, the authorization response message approving or declining the transaction.
2. The computer-implemented method of claim 1, further comprising transmitting, by the processing computer and to the resource provider computer, the portion of pre-analyzed data and the value.
3. The computer-implemented method of claim 1, wherein the portion of the pre-analyzed data is selected from the supplemental database based at least in part on preferences specified by the authorizing computer.
4. The computer-implemented method of claim 1, wherein modifying the authorization request message to include the portion of pre-analyzed

data and the value includes modifying a data field in the authorization request message.

5. The computer-implemented method of claim 1, further comprising updating the supplemental database with updated interactions by the user by utilizing an application programming interface (API) call by the resource provider computer to the supplemental database.

6. The computer-implemented method of claim 1, wherein the session identifier includes at least a key or a unique user identifier.

7. The computer-implemented method of claim 1, wherein generating the authorization response message by the authorizing computer includes the authorizing computer not performing an analysis of the transaction based at least in part on the modified authorization request message.

8. A server comprising:
a processor; and
a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, to implement a method comprising:

receiving, by the server ~~computer~~ and from a transport computer or a resource provider computer, an authorization request message for a transaction and a session identifier, the session identifier generated by an authentication requestor and associated with data for one or more interactions by a user associated with the transaction and stored in a database;

obtaining, by the server ~~computer~~ and from the database, a portion of pre-analyzed data about the user and the one or more interactions based at least in part on the session identifier;

performing, by the server ~~computer~~, a risk analysis for the transaction using the portion of the pre-analyzed data to generate a value, the value representing a likelihood of a fraudulent transaction for the transaction;

modifying, by the server ~~computer~~, the authorization request message to include the portion of the pre-analyzed data and the value; and

transmitting, by the server ~~computer~~ and to an authorizing computer, the modified authorization request message.

9. The server of claim 8, wherein the method further comprises transmitting, by the server ~~computer~~ to the transport computer, an authorization response message from the authorizing computer, the authorizing computer generating the authorization response message based on the modified authorization request message, the authorization response message approving or declining the transaction.

10. The server of claim 8, wherein the pre-analyzed data is analyzed by one or more authentication risk models associated with a plurality of authentication requestors.

11. The server of claim 8, wherein the pre-analyzed data includes one or more of a device identifier associated with the transaction, transaction detail information, personal information for the user, internet protocol (IP) address information, web site traffic, or web site interaction information.

12. The server of claim 8, wherein modifying the authorization request message includes setting one or more flags associated with the authorization request message for the transaction.

13. The server of claim 8, wherein the method further comprises transmitting, by the server ~~computer~~ and to the transport computer, the portion of pre-analyzed data and the valuescore.

14. The server of claim 8, wherein the portion of the pre-analyzed data is selected from the supplemental database based at least in part on preferences specified by the authorizing computer.

15. A processor computer comprising:
a processor; and
computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, to implement a method comprising:
receiving, by the processor computer and from a transport computer or a resource provider computer, an authorization request message for a transaction and a session identifier, the session identifier generated by an authentication

requestor and associated with data for one or more interactions by a user associated with the transaction and stored in a database;

obtaining, by the processor computer and from the database, a portion of pre-analyzed data about the user and the one or more interactions based at least in part on the session identifier;

performing, by the processor computer, a risk analysis for the transaction using the portion of the pre-analyzed data to generate a value, the value representing a likelihood of a fraudulent transaction for the transaction;

modifying, by the processor computer, the authorization request message to include the portion of the pre-analyzed data and the value; and

transmitting, by the processor computer and to an authorizing computer, the modified authorization request message.

16. The processor computer of claim 15, wherein the method further comprises transmitting, by the processor computer to the transport computer, an authorization response message from the authorizing computer, the authorizing computer generating the authorization response message based on the modified authorization request message, the authorization response message approving or declining the transaction.

17. The processor computer of claim 15, wherein the method further comprises transmitting, by the processor computer and to a resource provider associated with the transport computer, the portion of pre-analyzed data and the value.

18. The processor computer of claim 15, wherein the portion of the pre-analyzed data is selected from the supplemental database based at least in part on preferences specified by the authorizing computer.

19. The processor computer of claim 15, wherein modifying the authorization request message to include the portion of pre-analyzed data and the value includes modifying a data field in the authorization request message.

20. The processor computer of claim 15, wherein the method further comprises generating, by the authorizing computer, the authorization response

message by performing an additional analysis of the transaction based at least in part on the modified authorization request message.