

WHAT IS CLAIMED IS:

1. A system that aggregates client data and cyber indicators to authenticate a client, the system comprising:

a memory that stores and maintains a plurality of client profiles; and

a computer server comprising at least one computer processor and coupled to the memory, the computer server programmed to:

receive, via an electronic input, an authorization request from a requester for access to an account and to perform one or more actions related to the account;

identify a client identifier associated with the authorization request;

using the client identifier, retrieve, from the memory, a client profile, wherein the client profile is based on an aggregation of client data, client device data, claims data and cyber data;

the client data comprises client account data, client behavior data and transaction activity data;

the client device data comprises a device print associated with the authorization request;

the claims data comprises pending and prior data relating to one or more reports of improper activity; and

the cyber data comprises an indication of whether the client's personally identifiable information has been compromised;

generate a risk score based on an aggregated combination of the client data, client device data, claims data and cyber data to determine whether the requester is authenticated to access the account;

generate an arrangement of tiered user actions grouped by relative risk levels, wherein higher tiers include user actions with relative risk levels greater than those actions in lower tiers,

as well as all of the user actions from any lower tiers;

determine, based on the risk score, an approved tier of user actions;

automatically apply an authentication determination to the request to perform one or more actions related to the requested account; and

apply machine learning to the authentication determination, wherein the machine learning (1) analyzes the requestor's behavior and transaction history to determine if the requestor's behavior is outside of an expected behavior range and updates the risk score based on the determination, and (2) applies feedback to reduce improper denials of authorization requests.

2. The system of claim 1, wherein the account comprises an account with a financial institution.

3. The system of claim 1, wherein the computer processor is programmed to:
automatically adjust the risk score based on subsequent customer data and cyber data.

4. The system of claim 1, wherein cyber data comprises data relating to authentication activity from one or more separate and distinct third party entities in a common industry.

5. The system of claim 1, wherein cyber data comprises data relating to authentication activity from one or more other lines of businesses within a common company entity.

6. The system of claim 1, wherein the authentication determination comprises one or more responsive actions permitted to the requester based on the risk score.

7. The system of claim 1, wherein the cyber data comprises an originating IP address.

8. The system of claim 1, wherein the cyber data comprise malware indicators.

9. The system of claim 1, wherein the cyber data comprises voice biometrics.

10. The system of claim 1, wherein the computer processor is further programmed to: apply learning analytics to predict client acceptable behavior.

11. A method that aggregates client data and cyber indicators to authenticate a client, the method comprising the steps of:

receiving, via an electronic input, an authorization request from a requester for access to an account and performing one or more actions related to the account;

identifying, via a computer processor, a client identifier associated with the authorization request;

using the client identifier, retrieving, from a memory component, a client profile, wherein the client profile is based on an aggregation of client data, client device data, claims data and cyber data;

the client data comprises client account data, client behavior data and transaction activity data;

the client device data comprises a device print associated with the authorization request;

the claims data comprises pending and prior data relating to one or more reports of improper activity; and

the cyber data comprises an indication of whether the client's personally identifiable information has been compromised;

generating, via the computer processor, a risk score based on an aggregated combination of the client data, client device data, claims data and cyber data to determine whether the requester is authenticated to access the account;

generating an arrangement of tiered user actions grouped by relative risk levels, wherein higher tiers include user actions with relative risk levels greater than those actions in lower tiers,

as well as all of the user actions from any lower tiers;

determining based on the risk score, an approved tier of user actions;

automatically applying, via the computer processor, an authentication determination to the request to perform one or more actions related to the requested account; and

applying machine learning to the authentication determination, wherein the machine learning (1) analyzes the requestor's behavior and transaction history to determine if the requestor's behavior is outside of an expected behavior range and updates the risk score based on the determination, and (2) applies feedback to reduce improper denials of authorization requests.

12. The method of claim 11, wherein the account comprises an account with a financial institution.

13. The method of claim 11, further comprising the step of:

automatically adjusting the risk score based on subsequent customer data and cyber data.

14. The method of claim 11, wherein cyber data comprises data relating to authentication activity from one or more separate and distinct third party entities in a common industry.

15. The method of claim 11, wherein cyber data comprises data relating to authentication activity from one or more other lines of businesses within a common company entity.

16. The method of claim 11, wherein the authentication determination comprises one or more responsive actions permitted to the requester based on the risk score.

17. The method of claim 11, wherein the cyber data comprises an originating IP address.

18. The method of claim 11, wherein the cyber data comprise malware indicators.

19. The method of claim 11, wherein the cyber data comprises voice biometrics.
20. The method of claim 11, wherein the computer processor is further programmed to: apply learning analytics to predict client acceptable behavior.