

WHAT IS CLAIMED IS:

1. A system that combines payment data and cyber fraud indicators to identify potential fraud in payment requests from a client, the system comprising:

a memory that stores and maintains a list of known fraud characteristics and cyber fraud indicators associated with activities prior to a payment instruction; and

a computer processor, coupled to the memory, programmed to:

receive, via an electronic input, a legitimate payment instruction from the client;

identify one or more cyber fraud indicators, from one or more of a social engineering attack and a business email compromise attack against a client prior to the legitimate payment instruction that caused the client to initiate the legitimate payment instruction on fraudulent grounds, the social engineering attack and the email compromise attack based on leveraging information about the client acquired on a plurality of websites, and the one or more cyber fraud indicators include an IP address associated with prior fraudulent activity, an autonomous system number associated with a high risk that has not been previously visited by a device used by the victim to initiate the payment instruction, a malware indicator originating from the victim's device indicating a risk of fraud, an automatic number identification that determines an origination telephone number associated with fraudulent activity, and a look alike domain accessed by the device used by the victim prior to the payment instruction;

apply payment decisioning, based on learning analytics, to correlate the one or more cyber fraud indicators to the legitimate payment instruction, whereby identified characteristics of potentially fraudulent activities are applied to downstream decisioning;

apply learning analytics, based on one or more of known fraudulent activity and suspected fraudulent activity involving both a payor and a payment beneficiary, to the correlated

one or more cyber fraud indicators and legitimate payment instruction to determine that the legitimate payment instruction is likely originating from fraudulent activity;

generate a risk score based on the applied learning analytics to determine whether the payment instruction should be executed;

determine an action based on the risk score, the actions comprising one of completing a payment, denying a payment, and allowing a payment with continued monitoring of the payment;

add one or more new cyber fraud indicators identified in the received payment instruction to the list of known fraud characteristics and cyber fraud indicators; and

perform feedback analysis via the learning analytics on known good transactions, known fraud, and the one or more new cyber fraud indicators to further train, refine, and improve the functioning of the learning analytics.

2. The system of claim 1, wherein the one or more cyber fraud indicators comprise an originating IP address.

3. The system of claim 1, wherein the one or more cyber fraud indicators comprise malware indicators.

4. The system of claim 1, wherein the one or more cyber fraud indicators comprise look alike domain names.

5. The system of claim 1, wherein the one or more cyber fraud indicators comprise voice biometrics.

6. The system of claim 1, further comprising an interactive user interface that enables the client to view the risk score and determine a payment action in response.

7. The system of claim 1, wherein the computer processor is further programmed to:

apply learning analytics from a first user of the client to a second user of the client.

8. The system of claim 1, wherein the computer processor is further programmed to: apply learning analytics from a first user of the client to a second user of a second client different from the client.

9. The system of claim 1, wherein the payment instruction further comprises a request for access to client sensitive information.

10. The system of claim 1, wherein the computer processor is further programmed to leverage a separate and distinct risk score generated based on beneficiary account data elements.

11. A method that combines payment data and cyber fraud indicators to identify potential fraud in payment requests from a client, the method comprising the steps of:

storing and maintaining, in a memory, a list of known fraud characteristics and cyber fraud indicators associated with activities prior to a payment instruction;

receiving, via an electronic input, a legitimate payment instruction from the client;

identifying, via a programmed computer processor, one or more cyber fraud indicators, from one or more of a social engineering attack and a business email compromise attack against a client prior to the legitimate payment instruction that caused the client to initiate the legitimate payment instruction on fraudulent grounds, the social engineering attack and the email compromise attack based on leveraging information about the client acquired on a plurality of websites, and the one or more cyber fraud indicators include an IP address associated with prior fraudulent activity, an autonomous system number associated with a high risk that has not been previously visited by a device used by the victim to initiate the payment instruction, a malware indicator originating from the victim's device indicating a risk of fraud, an automatic number identification that determines an origination telephone number associated with fraudulent

activity, and a look alike domain accessed by the device used by the victim prior to the payment instruction;

applying, via the programmed computer processor, payment decisioning, based on learning analytics, to correlate the one or more cyber fraud indicators to the legitimate payment instruction, whereby identified characteristics of potentially fraudulent activities are applied to downstream decisioning;

applying learning analytics, based on one or more of known fraudulent activity and suspected fraudulent activity involving both a payor and a payment beneficiary, to the correlated one or more cyber fraud indicators and legitimate payment instruction to determine that the legitimate payment instruction is likely originating from fraudulent activity;

generating, via the programmed computer processor, a risk score based on the applied learning analytics to determine whether the payment instruction should be executed;

determining an action based on the risk score, the actions comprising one of completing a payment, denying a payment, and allowing a payment with continued monitoring of the payment;

adding one or more new cyber fraud indicators identified in the received payment instruction to the list of known fraud characteristics and cyber fraud indicators; and

performing feedback analysis via the learning analytics on known good transactions, known fraud, and the one or more new cyber fraud indicators to further train, refine, and improve the functioning of the learning analytics.

12. The method of claim 11, wherein the one or more cyber fraud indicators comprise an originating IP address.

13. The method of claim 11, wherein the one or more cyber fraud indicators comprise

malware indicators.

14. The method of claim 11, wherein the one or more cyber fraud indicators comprise look alike domain names.

15. The method of claim 11, wherein the one or more cyber fraud indicators comprise voice biometrics.

16. The method of claim 11, further comprising the step of:
enabling, via an interactive user interface, the client to view the risk score and determine a payment action in response.

17. The method of claim 11, further comprising the step of:
applying learning analytics from a first user of the client to a second user of the client.

18. The method of claim 11, further comprising the step of:
applying learning analytics from a first user of the client to a second user of a second client different from the client.

19. The method of claim 11, wherein the payment instruction further comprises a request for access to client sensitive information.

20. The method of claim 1, further comprising the step of:
leveraging a separate and distinct risk score generated based on beneficiary account data elements.