CLAIMS

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

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

(b) a fraud analysis engine with at least one computer processor, wherein the fraud analysis engine is in data communication with the network, the fraud database, and the cyber database, and the at least one computer processor of the fraud analysis engine is programmed to:

(i) receive, via an electronic input, a legitimate payment instruction from the client system via the network;

(ii) 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:

(1) an IP address associated with prior fraudulent activity;

(2) 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;

(3) a malware indicator originating from the victim's device indicating a risk of fraud;

(4) an automatic number identification that determines an origination telephone number associated with fraudulent activity;

(5) a look alike domain accessed by the device used by the victim prior to the payment instruction; and

(6) one or more voice biometrics;

(iii) apply logic rules by a logic rules module of the fraud analysis engine to determine look alike domain names by comparing one or more registered domain names to a list of known legitimate domain names;

(iv) collect, to the extent not protected by a privacy shield, associated information relevant to each look alike domain name registration comprising a registration entity, and when the registration was made;

(v) determine if each look alike domain name registration is fraudulent, the determination depending at least in part on the associated information for each look alike domain name registration;

(vi) apply the look alike domain registrations as one of the plurality of cyber fraud indicators relevant to the business email compromise attack against the client prior to the legitimate payment instruction, and by applying the look alike domain name as one of the plurality of cyber fraud indicators:

(1) determine whether to release a transaction or proceed with a transaction; and

(2) determine whether a requesting domain name associated with the received legitimate payment instruction from the client has been potentially compromised;

(vii) 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;

(viii) apply learning analytics by a learning engine module of the fraud analysis engine, based on one or more of known fraudulent activity and suspected fraudulent activity involving both a payor and a payment beneficiary, including fraud-based information from a plurality of payment instructions from one or more other clients, 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, the determination made by the learning analytics is also based on a historical set of behavior for the client;

(ix) generate a risk score based on the applied learning analytics to determine whether the legitimate payment instruction will result in an illegitimate payment, wherein the accuracy of the risk score is based on a number of indicators considered in the analysis and the number of indicators considered is determined based on the payment instruction, the client providing the payment instruction, and a geographic location for the payment instruction;

(x) 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;

(xi) 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

(xii) 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, further comprising an interactive user interface that enables the client to view the risk score and determine a payment action in response.

3. 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.

4. 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.

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

6. 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.