CLAIMS

1. A method, comprising:

identifying, by a risk assessment engine, a primary fraud risk based on a transaction request corresponding to a transaction account;

identifying, by the risk assessment engine, a notification channel for a fraud protection notification;

transmitting, by the risk assessment engine, a notification through the notification channel to a user device in response to identifying the primary fraud risk, the notification comprising a link to the risk assessment engine comprising a confirmation link that confirms the transaction is legitimate;

obtaining, by the risk assessment engine, a response to the notification from the user device, the response comprising the user device accessing the link to the risk assessment engine transmitted through the notification channel to the user device;

executing, by a transaction verification service, a script associated with the link, the script configured to retrieve and capture user device data from the user device accessing the link to the risk assessment engine, wherein the user device data comprises at least one characteristic corresponding to software or physical parameters of the user device;

receiving, by a risk assessment engine, captured user device data from the script;

retrieving, by the risk assessment engine, historical transaction fraud data based on the captured user device data, the historical transaction fraud data comprising a plurality of device data characteristics known to originate from a fraudulent source;

determining, by the risk assessment engine, a secondary fraud risk based on the captured user device data by determining whether the captured user device data matches data from the historical transaction fraud data; and

transmitting, by the risk assessment engine, a fraudulent verification notification to a payment system in response to determining that the captured device data matching data from the historical transaction data.

2. The method of claim 1, further comprising transmitting, by the risk assessment engine, a verification approval to the payment system in response to determining that the captured device data does not significantly match data from the historical transaction data.

3. The method of claim 2, wherein in response to receiving the verification approval the payment system removes a pending fraud status from the transaction account.

4. The method of any one of claims 1 to 3, wherein in response to receiving the fraudulent verification notification the payment system flags the transaction account for a manual fraud resolution.

5. The method of any one of claims 1 to4, wherein the payment system determines a primary fraud risk based on the transaction request, and wherein in response to determining that the primary fraud risk indicates a potential fraud the payment system transmits a fraud protection notification to the user device.

6. The method of claims 1-5, wherein the secondary fraud risk is determined based on if-then logic comparing the captured user device data to a fraud threshold.

7. The method of any one of claims 1 to 6, wherein the secondary fraud risk is determined by inputting the captured user device data into at least one of a statistical model, a machine learning model, or an artificial intelligence model.

8. The method of any one of claims 1-7, wherein the captured user device data comprises at least one of a unique device ID, an internet protocol (IP) address, an operating system type, a web browser type, an enabled language, a screen resolution setting, a scripting setting, or an anonymous IP indicator.

9. A system comprising:

a processor; and

a tangible, non-transitory memory configured to communicate with the processor, the tangible, non-transitory memory having instructions stored thereon that, in response to execution by the processor, cause the processor to perform operations comprising:

identifying, by the processor, a primary fraud risk based on a transaction request corresponding to a transaction account;

identifying, by the processor, a notification channel for a fraud protection notification;

transmitting, by the processor, a notification through the notification channel to a user device in response to identifying the primary fraud risk, the notification comprising a link to

a risk assessment engine comprising a confirmation link that confirms the transaction is legitimate;

obtaining, by the processor, a response to the notification from the user device, the response comprising the user device accessing the link to the risk assessment engine;

executing, by the processor, a script associated with the link, the script configured to retrieve and capture user device data from the user device accessing the link to the risk assessment engine, wherein the user device data comprises at least one characteristic corresponding to software or physical parameters of the user device;

receiving, by the processor, captured user device data from the script;

retrieving, by the processor, historical transaction fraud data based on the captured user device data, the historical transaction fraud data comprising a plurality of device data characteristics known to originate from a fraudulent source;

determining, by the processor, a secondary fraud risk based on the captured user device data by determining whether the captured user device data matches data from the historical transaction fraud data; and

transmitting, by the processor, a fraudulent verification notification to a payment system in response to determining that the captured device data matching data from the historical transaction data.

10. The system of claim 9, further comprising transmitting, by the processor, a verification approval to the payment system in response to determining that the captured device data does not significantly match data from the historical transaction data, wherein in response to receiving the verification approval the payment system is configured to remove a pending fraud status from the transaction account.

11. The system of claims 9 or 10, wherein the secondary fraud risk is determined based on if-then logic comparing the captured user device data to a fraud threshold.

12. The system of any one of claims 9 to 11, wherein the secondary fraud risk is determined by inputting the captured user device data into at least one of a statistical model, a machine learning model, or an artificial intelligence model.

13. The system of any one of claims 9 to 12, wherein the captured user device data comprises at least one of a unique device ID, an internet protocol (IP) address, an operating system type,

a web browser type, an enabled language, a screen resolution setting, a scripting setting, or an anonymous IP indicator.

14. An article of manufacture including a non-transitory, tangible computer readable storage medium having instructions stored thereon that, in response to execution by a computer-based system, cause the computer-based system to perform operations comprising:

identifying, by the computer-based system, a primary fraud risk based on a transaction request corresponding to a transaction account;

identifying, by the computer-based system, a notification channel for a fraud protection notification;

transmitting, by the computer-based system, a notification to a user device in response to identifying the primary fraud risk, the notification sent through the notification channel and comprising a link to a risk assessment engine comprising a confirmation link that confirms the transaction is legitimate;

obtaining, by the computer-based system, a response to the notification from the user device, the response comprising the user device accessing the link to the risk assessment engine;

executing, by the computer-based system, a script associated with the link, the script configured to retrieve and capture user device data from the user device accessing the link to the risk assessment engine, wherein the user device data comprises at least one characteristic corresponding to software or physical parameters of the user device;

receiving, by the computer-based system, captured user device data from the script;

retrieving, by the computer-based system, historical transaction fraud data based on the captured user device data, the historical transaction fraud data comprising a plurality of device data characteristics known to originate from a fraudulent source;

determining, by the computer-based system, a secondary fraud risk based on the captured user device data by determining whether the captured user device data matches data from the historical transaction fraud data; and

transmitting, by the computer-based system, a fraudulent verification notification to a payment system in response to determining that the captured device data matching data from the historical transaction data.

15. The article of manufacture of claim 14, further comprising transmitting, by the computer-based system, a verification approval to the payment system in response to determining that

the captured device data does not significantly match data from the historical transaction data, wherein in response to receiving the verification approval the payment system is configured to remove a pending fraud status from the transaction account.

16. The article of manufacture of claim 14, wherein in response to receiving the fraudulent verification notification the payment system is configured to flag the transaction account for a fraud resolution.

17. The article of manufacture of claim 14, wherein the secondary fraud risk is determined based on if-then logic comparing the captured user device data to a fraud threshold.

18. The article of manufacture of claim 14, wherein the secondary fraud risk is determined by inputting the captured user device data into at least one of a statistical model, a machine learning model, or an artificial intelligence model.

19. The article of manufacture of claim 14, wherein the captured user device data comprises at least one of a unique device ID, an internet protocol (IP) address, an operating system type, a web browser type, an enabled language, a screen resolution setting, a scripting setting, or an anonymous IP indicator.