

CLAIMS

What is claimed is:

1. A method comprising:

receiving, by a processor via a computer network and from a user computing device, a payment request wherein the payment request comprises sender data, receiver data, and a payment amount;

retrieving, by the processor via the computer network and from the user computing device, one or more settings associated with the user computing device; and

executing, by the processor, a payment risk analysis on the payment request, wherein the payment risk analysis analyses, with a machine learning model, the one or more settings associated with the user computing device to perform a risk assessment associated with the user computing device,

wherein when the risk assessment indicates that the user computing device is not a fraudulent computing device and that a sender account comprises sufficient funds to complete the payment request based on the payment amount, the method further comprises:

transmitting, by the processor a debit pull to a sender bank indicated in the sender data to debit the payment amount from the sender account indicated in the sender data, and

transmitting, by the processor a credit push to a receiver bank indicated in the receiver data to credit the payment amount to a receiver account indicated in the receiver data,

wherein when the risk assessment indicates that the user computing device is a fraudulent computing device or that the sender account comprises insufficient funds to complete the payment request based on the payment amount, the method further comprises:

transmitting, by the processor, an authentication challenge;

receiving, by the processor, an authentication challenge response based on the authentication challenge; and

validating, by the processor, the authentication challenge response by comparing the authentication challenge to the authentication challenge response, and

wherein when the risk assessment indicates that the user computing device is a fraudulent computing device and that the sender account comprises insufficient funds to complete the payment request based on the payment amount, the method further comprises

declining, by the processor, the payment request.

2. The method of claim 1, wherein the debit pull and the credit push are transmitted simultaneously or near simultaneously.

3. The method of claim 1, wherein the executing the payment risk analysis comprises validating, by the processor, sender bank data from the sender data, wherein the sender bank data is validated by verifying sender bank login information from the sender bank data and validating that the sender account comprises sufficient funds to complete the payment request based on the payment amount.

4. The method of claim 1, wherein the executing the payment risk analysis comprises:

determining, by the processor, the risk assessment by comparing the one or more settings associated with the user device to device data characteristics known to originate from fraudulent sources.

5. The method of claim 1, further comprising assigning, by the processor, a unique identifier to the payment request.

6. The method of claim 5, wherein the unique identifier comprises a legacy identifier compatible with a legacy payment system, and wherein the legacy identifier comprises a checking account number, a savings account number, a credit card number, a commercial account number a commercial charge card number, or a direct deposit account number.

7. The method of claim 1, further comprising approving, by the processor, the payment request in response to receiving a debit notification from the sender bank and a credit notification from the receiver bank.

8. The method of claim 7, wherein the payment request is initiated between a customer and a merchant as payment for a transaction, and wherein in response to the debit pull and the credit push being transmitted the merchant completes the transaction with the customer.

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:

receiving, by the processor via a computer network and from a user computing device, a payment request wherein the payment request comprises sender data, receiver data, and a payment amount;

retrieving, by the processor via the computer network and from the user computing device, one or more settings associated with the user computing device; and

executing, by the processor, a payment risk analysis on the payment request, wherein the payment risk analysis analyzes, with a machine learning model, the one or more settings associated with the user computing device to perform a risk assessment associated with the user computing device;

wherein when the risk assessment indicates that the user computing device is not a fraudulent computing device and that a sender account comprises sufficient funds to complete the payment request based on the payment amount, the operations further comprise:

transmitting, by the processor, a debit pull to a sender bank indicated in the sender data to debit the payment amount from the sender account indicated in the sender data, and

transmitting, by the processor, a credit push to a receiver bank indicated in the receiver data to credit the payment amount to a receiver account indicated in the receiver data,

wherein when the risk assessment indicates that the user computing device is a fraudulent computing device or that the sender account comprises insufficient funds to complete the payment request based on the payment amount, the operations further comprise:

transmitting, by the processor, an authentication challenge;

receiving, by the processor, an authentication challenge response based on the authentication challenge; and

validating, by the processor, the authentication challenge response by comparing the authentication challenge to the authentication challenge response, and

wherein when the risk assessment indicates the user computing device is a fraudulent computing device and that the sender account comprises insufficient funds to complete the payment request based on the payment amount, the operations further comprise

declining, by the processor, the payment request.

10. The system of claim 9, wherein the executing the payment risk analysis comprises validating, by the processor, sender bank data from the sender data, wherein the sender bank data is validated by verifying sender bank login information from the sender bank data and validating that the sender account comprises sufficient funds to complete the payment request based on the payment amount.

11. The system of claim 9, wherein the executing the payment risk analysis comprises:
determining, by the processor, the risk assessment by comparing the one or more settings associated with the user device to device data characteristics known to originate from fraudulent sources.

12. The system of claim 9, further comprising approving, by the processor, the payment request in response to transmitting the debit pull and the credit push.

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

receiving, by the processor via a computer- network and from a user computing device, a payment request wherein the payment request comprises sender data, receiver data, and a payment amount;

retrieving, by the processor via the computer network and from the user computing device, one or more settings associated with the user computing device; and

executing, by the processor, a payment risk analysis on the payment request, wherein the payment risk analysis analyses, with a machine learning model, the one or

more settings associated with the user computing device to perform a risk assessment associated with the user computing device,

wherein when the risk assessment indicates that the user computing device is not a fraudulent computing device and that a sender account comprises sufficient funds to complete the payment request based on the payment amount, the operations further comprise:

transmitting, by the processor, a debit pull to a sender bank indicated in the sender data to debit the payment amount from the sender account indicated in the sender data, and

transmitting, by the processor, a credit push to a receiver bank indicated in the receiver data to credit the payment amount to a receiver account indicated in the receiver data,

wherein when the risk assessment indicates that the user computing device is a fraudulent computing device or that the sender account comprises insufficient funds to complete the payment request based on the payment amount, the operations further comprise:

transmitting, by the processor, an authentication challenge;

receiving, by the processor, an authentication challenge response based on the authentication challenge; and

validating, by the processor, the authentication challenge response by comparing the authentication challenge to the authentication challenge response, and

wherein when the risk assessment indicates that the user computing device is a fraudulent computing device and that the sender account comprises insufficient funds to complete the payment request based on the payment amount, the operations further comprise

declining, by the processor, the payment request.

14. The article of manufacture of claim 13, wherein the debit pull is transmitted at a first time and the credit push is transmitted at a second time, and wherein the first time is the same or proximate the second time.

15. The article of manufacture of claim 14, further comprising approving, by the processor, the payment request in response to transmitting the debit pull and the credit push, wherein in

response to the payment request being approved the credited payment amount is available for use by a receiver associated with the receiver account.

16. The article of manufacture of claim 13, wherein the executing the payment risk analysis comprises:

validating, by the processor, sender bank data from the sender data, wherein the sender bank data is validated by verifying sender bank login information from the sender bank data and validating that the sender account comprises sufficient funds to complete the payment request based on the payment amount;

capturing, by the processor, a user computing device characteristic from a user device;

comparing, by the processor, the one or more settings associated with the user device to device data characteristics known to originate from fraudulent sources; and

determining, by the processor, the risk assessment based on at least one of the validated sender bank data or a result of the compared one or more settings to the device data characteristics.

17. The method of claim 1, wherein a medium risk is determined for the payment risk by validating that the sender account comprises sufficient funds to complete the payment request based on the payment amount and determining that a user of the user device is not an owner of the user device.

18. The method of claim 1, wherein a medium risk is determined for the payment risk by validating that the sender account comprises sufficient funds to complete the payment request based on the payment amount and determining that the payment request is fraudulent.

19. The system of claim 9, wherein a medium risk is determined for the payment risk by validating that the sender account comprises sufficient funds to complete the payment request based on the payment amount and determining that a user of the user device is not an owner of the user device.

20. The system of claim 9, wherein a medium risk is determined for the payment risk by validating that the sender account comprises sufficient funds to complete the payment request based on the payment amount and determining that the payment request is fraudulent.