While the merchant is capable of collecting data about the cardholder associated with an online payment transaction, the constraints of many known payment processing systems limit the amount of data that may be provided to the issuing bank or the payment processing network. There exists a need for more advanced fraud detection systems.

BRIEF DESCRIPTION OF THE DISCLOSURE

In an aspect, there is a computer-implemented method for detecting fraud in an online payment transaction, the method implemented using an assurance exchange (AE) computer device including a processor in communication with a memory device, the AE computer device in communication with a merchant computer device and a payment processing network, the method comprising:

receiving, from a merchant, authentication data associated with a candidate payment transaction being conducted by a cardholder via a website associated with the merchant;

storing, in the memory device, the authentication data;

generating an initial assurance score based on the authentication data;

transmitting, to the merchant, the initial assurance score;

receiving, from a computer device associated with the payment processing network, an authorization request message for the candidate online payment transaction, wherein the authorization request message originated at the merchant computer device and includes the transaction identifier;

retrieving, from the memory, the authentication data for the candidate online payment transaction that matches the transaction identifier included in the authorization request message;

calculating, by the AE computer device, an assurance level score based on the authentication data and the authorization request message, wherein the

assurance level score represents a level of confidence that the candidate payment transaction is not fraudulent; and

transmitting, to an issuer processor computer device, the authorization request message including the assurance level score.

In an aspect there is an assurance exchange (AE) computer device used to detect fraud in an online payment transaction, said AE computer device comprising a processor communicatively coupled to a memory device, said AE computer device in communication with a merchant computer device and a payment processing network, said processor programmed to:

receive, from a merchant, authentication data associated with a candidate payment transaction being conducted by a cardholder via a website associated with the merchant;

store, in the memory device, the authentication data;

generate an initial assurance score based on the authentication data;

transmit, to the merchant, the initial assurance score;

receive, from a computer device associated with the payment processing network, an authorization request message for the candidate online payment transaction, wherein the authorization request message originated at the merchant computer device and includes the transaction identifier;

retrieve, from the memory device, the authentication data for the candidate online payment transaction that matches the transaction identifier included in the authorization identifier included in the authorization request message;

calculate an assurance level score based on the authentication data and the authorization request message, wherein the assurance level score represents a level of confidence that the candidate online payment transaction is not fraudulent; and

transmit, to an issuer processor computer device, the authorization request message including the assurance level score.

In an aspect there is at least one non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by an assurance exchange (AE) computer device having at least one processor coupled to at least one memory device, the computer-executable instructions cause the processor to:

receive, from a merchant, authentication data associated with a candidate payment transaction being conducted by a cardholder via a website associated with the merchant;

store, in the memory device, the authentication data;

generate an initial assurance score based on the authentication data;

transmit to the merchant, the initial assurance score;

receive, from a computer device associated with payment processing network, an authorization request message for the candidate payment transaction, wherein the authorization request message originated at the merchant computer device and includes the transaction identifier;

retrieve, from the memory device, the authentication data for the candidate online payment transaction that matches the transaction identifier; calculate an assurance level score based on the authentication data and the authorization request message, wherein the assurance level score represents a level of confidence that the candidate payment transaction is not fraudulent; and

transmit, to an issuer processor computer device, the authorization request message including the assurance level score. A computer-implemented method for determining a level of confidence that a payment transaction is not fraudulent is provided. The method is implemented using an assurance exchange (AE) computer device in communication with a memory. The method includes receiving, from a merchant, authentication data associated with a candidate payment transaction being conducted by a cardholder via a website associated with the merchant, storing, in the memory, the authentication

data, receiving, from a payment processor, an authorization request message for the candidate payment transaction, retrieving, from the memory, the authentication data for the candidate payment transaction based on the authorization request message, and calculating, by the AE computer device, an assurance level score based on the authentication data and the authorization request message. The assurance level score represents a level of confidence that the candidate payment transaction is not fraudulent. The method also includes transmitting, to an issuer processor, the authorization request message including the assurance level score.

An assurance exchange (AE) computer device used to determine a level of confidence that a payment transaction is not fraudulent is provided. The AE computer device includes a processor communicatively coupled to a memory device. The processor is programmed to receive, from a merchant, authentication data associated with a candidate payment transaction being conducted by a cardholder via a website associated with the merchant, store, in the memory device, the authentication data, receive, from a payment processor, an authorization request message for the candidate payment transaction, retrieve, from the memory device, the authentication data for the candidate payment transaction based on the authorization request message, and calculate an assurance level score based on the authentication data and the authorization request message. The assurance level score represents a level of confidence that the candidate payment transaction is not fraudulent. The processor is also programmed to transmit, to an issuer processor, the authorization request message including the assurance level score.

At least one non-transitory computer-readable storage media having computer-executable instructions embodied thereon is provided. When executed by an assurance exchange (AE) computer device having at least one processor coupled to at least one memory device, the computer-executable instructions cause the processor to receive, from a merchant, authentication data associated with a candidate payment transaction being conducted by a cardholder via a website associated with the merchant, store, in the memory device, the authentication data, receive, from a payment processor, an authorization request message for the candidate payment transaction, retrieve, from the memory device, the authentication data for the candidate payment transaction based on the authorization request message, and

calculate an assurance level score based on the authentication data and the authorization request message. The assurance level score represents a

WHAT IS CLAIMED IS:

1. A computer-implemented method for detecting fraud in an online payment transaction, the method implemented using an assurance exchange (AE) computer device including a processor in communication with a memory device, the AE computer device in communication with a merchant computer device and a payment processing network, the method comprising:

receiving, from a merchant, authentication data associated with a candidate payment transaction being conducted by a cardholder via a website associated with the merchant;

storing, in the memory device, the authentication data;

generating an initial assurance score based on the authentication data;

transmitting, to the merchant, the initial assurance score;

receiving, from a computer device associated with the payment processing network, an authorization request message for the candidate online payment transaction, wherein the authorization request message originated at the merchant computer device and includes the transaction identifier;

retrieving, from the memory, the authentication data for the candidate online payment transaction that matches the transaction identifier included in the authorization request message;

calculating, by the AE computer device, an assurance level score based on the authentication data and the authorization request message, wherein the assurance level score represents a level of confidence that the candidate payment transaction is not fraudulent; and

transmitting, to an issuer processor computer device, the authorization request message including the assurance level score.

2. A method in accordance with Claim 1, wherein calculating an assurance level score is further based on a cost of a false positive, a cost of a false negative, and a probability that the candidate payment transaction is fraudulent.

3. A method in accordance with Claim 1, wherein calculating the assurance level score is further based on the initial assurance score.

4. A method in accordance with Claim 1, wherein the authentication data includes a merchant fraud grading of the cardholder and the candidate online payment transaction performed by the merchant.

5. A method in accordance with Claim 5, wherein the authentication data includes one or more merchant reason codes that each represent a reason for the merchant fraud grading, and wherein when the authorization request message is transmitted to the issuer processor computer device, the authorization request message includes at least one of the one or more merchant reason codes.

6. A method in accordance with Claim 1, further comprising:

generating, by the AE computer device, one or more reason codes based on the authentication data, the authorization request message, and the assurance level score, wherein each of the one or more reason codes represents a reason for the assurance level score; and

transmitting at least one of the one or more generated reason codes to the issuer processor computer device in the authorization request message.

7. A method in accordance with Claim 7, further comprising transmitting, to the merchant, the assurance level score and the one or more reason codes.

8. A method in accordance with Claim 1, wherein communication with the merchant is executed via API calls between a computer device associated with the merchant and the AE computer device.

9. An assurance exchange (AE) computer device used to detect fraud in an online payment transaction, said AE computer device comprising a processor communicatively coupled to a memory device, said AE computer device in

communication with a merchant computer device and a payment processing network, said processor programmed to:

receive, from a merchant, authentication data associated with a candidate payment transaction being conducted by a cardholder via a website associated with the merchant;

store, in the memory device, the authentication data;

generate an initial assurance score based on the authentication data;

transmit, to the merchant, the initial assurance score;

receive, from a computer device associated with the payment processing network, an authorization request message for the candidate online payment transaction, wherein the authorization request message originated at the merchant computer device and includes the transaction identifier;

retrieve, from the memory device, the authentication data for the candidate online payment transaction that matches the transaction identifier included in the authorization identifier included in the authorization request message;

calculate an assurance level score based on the authentication data and the authorization request message, wherein the assurance level score represents a level of confidence that the candidate online payment transaction is not fraudulent; and

transmit, to an issuer processor computer device, the authorization request message including the assurance level score.

10. An AE computer device in accordance with Claim 9, wherein the assurance level score is further based on a cost of a false positive, a cost of a false negative, and a probability that the candidate payment transaction is fraudulent.

11. An AE computer device in accordance with Claim 9, wherein the authentication data includes a merchant fraud grading of the cardholder and the candidate online payment transaction performed by the merchant.

12. An AE computer device in accordance with Claim 11, wherein the authentication data includes one or more merchant reason codes that each represent a reason for the merchant fraud grading, and wherein when the authorization request message is transmitted to the issuer processor computer device, the authorization request message includes at least one of the one or more merchant reason codes.

13. An AE computer device in accordance with Claim 10, wherein said processor is further programmed to:

generate one or more reason codes based on the authentication data, the authorization request message, and the assurance level score, wherein each of the one or more reason codes represents a reason for the assurance level score; and

transmit at least one of the one or more generated reason codes to the issuer processor computer device in the authorization request message.

14. An AE computer device in accordance with Claim 14, wherein said processor is further programmed to transmit, to the merchant, the assurance level score and the one or more reason codes.

15. At least one non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by an assurance exchange (AE) computer device having at least one processor coupled to at least one memory device, the computer-executable instructions cause the processor to:

receive, from a merchant, authentication data associated with a candidate payment transaction being conducted by a cardholder via a website associated with the merchant;

store, in the memory device, the authentication data;

generate an initial assurance score based on the authentication data;

transmit to the merchant, the initial assurance score;

receive, from a computer device associated with payment processing network, an authorization request message for the candidate payment transaction, wherein the authorization request message originated at the merchant computer device and includes the transaction identifier;

retrieve, from the memory device, the authentication data for the candidate online payment transaction that matches the transaction identifier;

calculate an assurance level score based on the authentication data and the authorization request message, wherein the assurance level score represents a level of confidence that the candidate payment transaction is not fraudulent; and

transmit, to an issuer processor computer device, the authorization request message including the assurance level score.

16. The computer-readable storage medium of Claim 15, wherein the assurance level score is further based on a cost of a false positive, a cost of a false negative, and a probability that the candidate online payment transaction is fraudulent.

17. The computer-readable storage medium of Claim 15, wherein the authentication data includes a merchant fraud grading of the cardholder and the candidate online payment transaction performed by the merchant.

18. The computer-readable storage medium of Claim 15, wherein the authentication data includes one or more merchant reason codes that each represent a reason for the merchant fraud grading, and wherein when the authorization request message is transmitted to the issuer processor computer device, the authorization request message includes at least one of the one or more merchant reason codes.

19. The computer-readable storage medium of Claim 15, the computer-executable instructions further cause the processor to:

generate one or more reason codes based on the authentication data, the authorization request message, and the assurance level score, wherein each of the one or more reason codes represents a reason for the assurance level score; and

transmit at least one of the one or more generated reason codes to the issuer processor computer device in the authorization request message.