[0006] Recently, the Credit/Debit card purchase industry has launched technologies to solve security-related issues and also ease-of-use issues. Examples of these new technologies include Payment Gateway, 3-D Secure, Digital Wallet, Controlled Payment Number, and Online Authentication.

[0007] Each of these technologies is associated with messages, which are sometimes referred to as "E-commerce messages" and are used in conjunction with purchases. These e-commerce messages as well as containing a PAN may also contain the following "e-commerce message attributes": addresses (e.g. billing and shipping), email addresses, phone numbers, and application account id (e.g. wallet id). In addition, because the E-commerce messages are online messages, the IP Address, and fingerprint of the device used may readily be determined if not contained directly in the messages. The E-commerce "Transaction Trust Score" (ETTS) is a function of its attributes pairing history and in some aspects its attributes reputation.

[0008] Some known real-world systems purport to return a "trust score" on an E-commerce transaction, which is typically based on establishing a track record of usage of the device (as identified by one or more device fingerprints wherein the device can be any mobile device, for example a laptop, a mobile phone, or tablet with other E-commerce attributes, such as, an address or an IP address. The trust score may also include an attribute reputation, for example, but, not limited to a compromised IP address or a compromised email address, which may be obtained from offline input. However, these systems can only return an E-commerce Transaction Trust Score (ETTS) on a particular E-commerce Transaction if queried with a device fingerprint and one or more other message attributes used in the same transaction.

[0009] Accordingly, it would be desirable to improve the ability to determine a risk of fraud and trustworthiness of the account information using device fingerprints in combination with other message attributes.

SUMMARY

[0010] According to an aspect, there is provided a computer-implemented method for creating an assurance level based on authentication data attributes electronically captured by a merchant computing device, the method implemented using a computer device coupled to a memory device, the method comprising: receiving, from a sender, an authentication request message associated with a financial transaction initiated by a

cardholder, wherein the authentication request message includes authentication data attributes relating to the cardholder's interaction with the merchant computing device; performing an authentication routine for authenticating the cardholder as the actual cardholder using the authentication data attributes; transmitting an authentication response to the sender including results of the authentication routine; receiving an authorization request message associated with the financial transaction from the sender, the authorization request message including a fraud risk assessment of the financial transaction determined using the authentication response, the authorization request message including one or more reason codes associated with fraud risk assessment; and transmitting the received authorization request message to an issuer associated with the cardholder.

[0011] According to another aspect, there is provided a risk-based decisioning system for creating an assurance level based on authentication data attributes electronically captured by a merchant computer device, said system comprising the merchant computer device coupled to a payment network, said merchant computer device configured to: transmit an authentication request message to the payment network when a cardholder interacting with a merchant website is attempting to perform activities inconsistent with at least one of a transaction history of the cardholder and a profile of the cardholder; receive, from the payment network, an authentication response that indicates a trustworthiness of the cardholder; perform a secondary authentication evaluation that generates the merchant assessment of the trustworthiness of the cardholder based on the secondary authentication evaluation, wherein the secondary authentication evaluation is based at least partially upon the authentication response received from the payment network; transmit an authorization request message onto the payment network if the generated merchant assessment of trustworthiness indicates the cardholder is trustworthy; receive an authorization approval or denial based at least partially on the generated merchant assessment of trustworthiness; and complete a financial transaction based on the received authorization approval or denial.

[0012] According to yet another aspect, there is provided one or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by at least one processor, the computer-executable instructions cause the processor to: receive, from a sender, an authentication request message associated with a financial transaction initiated by a cardholder, wherein the authentication request message includes authentication data attributes relating to the

cardholder's interaction with a merchant computing device; perform an authentication routine for authenticating the cardholder as the actual cardholder using the authentication data attributes; transmit an authentication response to the sender including results of the authentication routine; receive, from the sender, an authorization request message associated with the financial transaction, the authorization request message including a fraud risk assessment of the financial transaction determined using the authentication response, the authorization request message including one or more reason codes associated with the fraud risk assessment; and transmit the received authorization request message to an issuer associated with the cardholder.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIGS. 1-8 show example embodiments of the methods and systems described herein.

[0014] FIG. 1 is a schematic diagram illustrating an example multi-party payment card industry system having a sender trust assessment module and that enables payment transactions between merchants and cardholders.

[0015] FIG. 2 is a simplified block diagram of an example payment processing system including a plurality of computer devices including the sender trust assessment module shown in FIG. 1 for influencing a fraud determination in a financial transaction based on a sender confidence level in accordance with an example embodiment of the present disclosure.

[0016] FIG. 3 is an expanded block diagram of an example embodiment of a server architecture of the payment processing system shown in FIG. 2 in accordance with one example embodiment of the present disclosure.

[0017] FIG. 4 illustrates an example configuration of a user system operated by a user, such as cardholder shown in FIG. 1.

[0018] FIG. 5 illustrates an example configuration of a server system such as server system shown in FIGS. 2 and 3.

[0019] FIG. 6 illustrates a data flow diagram of a risk-based decisioning process that uses input from a sender, for example, but not limited to the merchant, that represents the sender's perception of the fraud risk in a transaction with a cardholder.

CLAIMS

1. A computer-implemented method for creating an assurance level based on authentication data attributes electronically captured by a merchant computing device, the method implemented using a computer device coupled to a memory device, the method comprising:

receiving, from a sender, an authentication request message associated with a financial transaction initiated by a cardholder, wherein the authentication request message includes authentication data attributes relating to the cardholder's interaction with the merchant computing device;

performing an authentication routine for authenticating the cardholder as the actual cardholder using the authentication data attributes;

transmitting an authentication response to the sender including results of the authentication routine;

receiving an authorization request message associated with the financial transaction from the sender, the authorization request message including a fraud risk assessment of the financial transaction determined using the authentication response, the authorization request message including one or more reason codes associated with fraud risk assessment; and

transmitting the received authorization request message to an issuer associated with the cardholder.

2. The computer-based method of claim 1, further comprising generating an authentication response based on a correlating at least some of the authentication data attributes with previously authenticated cardholder data.

3. The computer-based method of claim 1, further comprising:

performing the authentication routine based on correlating a device identifier of a device used by the cardholder to interact with a website associated with the merchant to a primary account number (PAN) associated with an account of the cardholder.

4. The computer-based method of claim 1, wherein the information relating to a cardholder interaction with the sender comprises information relating to the cardholder navigating a webpage of the merchant.

5. The computer-based method of claim 1, wherein the historical transaction data of the cardholder includes an indication of a longevity of the account of the cardholder.

6. The computer-based method of claim 1, wherein the fraud risk assessment is determined using an

age of a cardholder profile with the merchant, wherein the age of the cardholder profile indicates a last update of the cardholder profile with the merchant.

7. The computer-based method of claim 1, further comprising:

receiving at least one of an authorization approval and an authorization denial from the issuer, the at least one of the authorization approval and the authorization denial based at least in part on the fraud risk assessment by the sender; and

transmitting the received at least one of the authorization approval and the authorization denial to the sender.

8. The computer-based method of claim 1, wherein the one or more reason codes include an indication of at least one of a longevity of the account of the cardholder, a time period since the profile of the cardholder has been updated, and a similarity of non-financial transaction interactions with the sender.

9. The computer-based method of claim 1, further comprising receiving a message from the sender relating to the financial transaction prior to receiving the authorization request message associated with the financial transaction, the message including a predefined sender confidence level data field that includes a fraud assessment of the financial transaction by the sender.

10. The computer-based method of claim 1, wherein the historical transaction data of the cardholder relates to a longevity of an account of the cardholder.

11. The computer-based method of claim 1, wherein the fraud risk assessment by the sender comprises determining an amount of time since an update of a profile of the cardholder with the sender.

12. The computer-based method of claim 1, further comprising:

receiving at least one of an authorization approval message and an authorization denial message from the issuer, the at least one of the authorization approval message and the authorization denial message based at least in part on the fraud risk assessment determined by at least one of the sender and the merchant; and

transmitting the received at least one of the authorization approval message and the authorization denial message to the sender.

13. The computer-based method of claim 1, wherein the sender and the merchant are the same.

14. A risk-based decisioning system for creating an assurance level based on authentication data attributes electronically captured by a merchant computer device, said system comprising the merchant computer device coupled to a payment network, said merchant computer device configured to:

transmit an authentication request message to the payment network when a cardholder interacting with a merchant website is attempting to perform activities inconsistent with at least one of a transaction history of the cardholder and a profile of the cardholder;

receive, from the payment network, an authentication response that indicates a trustworthiness of the cardholder;

perform a secondary authentication evaluation that generates the merchant assessment of the trustworthiness of the cardholder based on the secondary authentication evaluation, wherein the secondary authentication evaluation is based at least partially upon the authentication response received from the payment network;

transmit an authorization request message onto the payment network if the generated merchant assessment of trustworthiness indicates the cardholder is trustworthy;

receive an authorization approval or denial based at least partially on the generated merchant assessment of trustworthiness; and

complete a financial transaction based on the received authorization approval or denial.

15. The risk-based decisioning system of claim 14, wherein said merchant computer device is further configured to determine from interactions between the cardholder and the merchant website whether the cardholder is attempting to perform activities inconsistent with at least one of a transaction history of the cardholder and a profile of the cardholder.

16. The risk-based decisioning system of claim 14, wherein said secondary authentication evaluation comprises analyzing answers made by the cardholder to at least one of predetermined security questions and security questions determined in approximately real-time.

17. The risk-based decisioning system of claim 14, wherein the generated merchant assessment of trustworthiness indicates the cardholder is trustworthy when the generated merchant assessment of trustworthiness indicates the cardholder is not fraudulent.

18. One or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by at least one processor, the computer-executable instructions cause the processor to:

receive, from a sender, an authentication request message associated with a financial transaction initiated by a cardholder, wherein the authentication request message includes

authentication data attributes relating to the cardholder's interaction with a merchant computing device;

perform an authentication routine for authenticating the cardholder as the actual cardholder using the authentication data attributes;

transmit an authentication response to the sender including results of the authentication routine;

receive, from the sender, an authorization request message associated with the financial transaction, the authorization request message including a fraud risk assessment of the financial transaction determined using the authentication response, the authorization request message including one or more reason codes associated with the fraud risk assessment; and

transmit the received authorization request message to an issuer associated with the cardholder.

19. The computer-readable storage media of claim 18, wherein the computer-executable instructions further cause the processor to receive interaction data relating to the cardholder navigating a webpage of the merchant.

20. The computer-readable storage media of claim 18, wherein the computer-executable instructions further cause the processor to generate a plurality of trust scores during the cardholder interaction with the merchant computing device, each successive trust score of the plurality of trust scores superseding all previous trust scores generated during the cardholder interaction with the merchant.