[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] In one aspect of the disclosure, a computer-implemented method for creating an assurance level based on authentication data attributes using a computer device coupled to a database includes receiving an authorization request associated with the financial transaction from the sender wherein the authorization request includes a fraud risk

assessment of the financial transaction determined by the sender using an authentication response received from the computer device by the sender. The authorization request includes one or more reason codes associated with the sender fraud risk assessment. The method further includes transmitting the received authorization request to an issuer associated with the cardholder.

[0011] In another aspect, a risk-based decisioning system for creating an assurance level based on authentication data attributes includes a merchant computer device coupled to a payment network wherein the computer device is configured to transmit an authentication request from the merchant computer device 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 wherein the authentication request is separate from an authorization request. The computer device is also configured to receive, from the payment network, a response that indicates a trustworthiness of the cardholder, perform a secondary authentication evaluation that generates a merchant assessment of the trustworthiness of the cardholder based on the secondary authentication evaluation, and transmit an authorization request onto the payment network if the generated merchant assessment of trustworthiness indicates the cardholder is trustworthy. The computer device is further configured to receive an authorization approval or denial based at least partially on the generated merchant assessment of trustworthiness, and complete the financial transaction based on the received authorization approval or denial.

[0012] In yet another aspect, one or more non-transitory computer-readable storage media has computer-executable instructions embodied thereon, wherein when executed by at least one processor, the computer-executable instructions cause the processor to receive an authentication request from a sender wherein the authentication request is associated with the financial transaction and includes interaction data relating to a cardholder interaction with the sender. The computer-executable instructions further cause the processor to transmit an authentication response to the sender, the authentication response including results of an authentication routine performed by the computer device using the received interaction data and historical transaction data of the cardholder. The computer-executable instructions also cause the processor to receive an authorization