BRIEF DESCRIPTION OF THE INVENTION

[0009A] Disclosed herein is a computer-based method for evaluating a risk of fraud in a payment card transaction on a payment card interchange network, the method implemented using a computer device coupled to a memory device, the method comprising:

receiving payment card transaction messages relating to a payment card account, the payment card transaction messages relating to interactions with at least one of an agent on behalf of a cardholder of the payment card account and an agent on behalf of an issuer of the payment card account, the payment card transaction messages including at least one of an authorization request, an authorization response, and an application event, the application event comprising an interaction with the payment card account in other than a purchase interaction, the application event transaction message further comprising a device identifier comprising at least one of a device identifier and a hardware identifier associated with the device ;

receiving payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account;

comparing at least one data element in each payment card transaction messages to at least one data element in at least one of: the payment card reputation message and prior transaction history; and

determining at least one of a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

[0009B] Disclosed herein is a computer system for processing data associated with a payment card cardholder account, the computer system comprising:

a memory device;

a processor in communication with the memory device;

a transaction component configured to receive payment card transaction messages relating to a payment card account, the payment card transaction messages relating to interactions with at least one of an agent on behalf of a cardholder of the payment card account and an agent on behalf of an issuer of the payment card account, the payment card transaction messages including at least one of an authorization request, an authorization response, and an application event, the application event comprising an interaction with the payment card account in other than a purchase interaction, the

application event transaction message further comprising a device identifier comprising at least one of a device identifier and a hardware identifier associated with the device;

a reputation component configured to receive payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account;

a comparator component configured to compare at least one data element in each payment card transaction messages to at least one data element in at least one of: the payment card reputation message and prior transaction history;

a decisioning component configured to determine at least one of a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

[0009C] Disclosed herein is a 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 payment card transaction messages relating to a payment card account, the payment card transaction messages relating to interactions with at least one of an agent on behalf of a cardholder of the payment card account and an agent on behalf of an issuer of the payment card account, the payment card transaction messages including at least one of an authorization request, an authorization response, and an application event, the application event comprising an interaction with the payment card account in other than a purchase interaction, the application event transaction message further comprising a device identifier comprising at least one of a device identifier and a hardware identifier associated with the device ;

receive payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account;

compare at least one data element in each payment card transaction messages to at least one data element in at least one of: the payment card reputation message and prior transaction history; and

determine at least one of a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

[0010] In one embodiment, a computer-based method for evaluating a risk of fraud in a payment card transaction on a payment card interchange network, is implemented using a computer device coupled to a memory device, and includes receiving payment card transaction messages relating to a payment card account wherein the payment card transaction messages relate to interactions with a cardholder, an issuer of the payment card account, or both. The payment card transaction messages include an authorization request, an authorization response, and an Application Event and the Application Event includes an interaction with the payment card account in other than a purchase interaction wherein the Application Event transaction message further comprising a device identifier comprising at least one of a device identifier and a hardware identifier associated with the device. The method further includes receiving payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account, comparing at least one data element in each payment card transaction messages to at least one data element in at least one of: the payment card reputation message and prior transaction history, and determining at least one of a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

[0011] In another embodiment, a computer system for processing data associated with a payment card cardholder account includes a memory device, a processor in communication with the memory device, and a transaction component configured to receive payment card transaction messages relating to a payment card account, the payment card transaction messages relating to interactions with at least one of an agent on behalf of a cardholder of the payment card account and an agent on behalf of an issuer of the payment card account, the payment card transaction messages including at least one of an authorization request, an authorization response, and an Application Event, the Application Event comprising an interaction with the payment card account in other than a purchase interaction, the Application Event transaction message further comprising a device identifier comprising at least one of a device identifier and a hardware identifier associated with the device. The computer system further includes a reputation component configured to receive payment card account reputation messages that include historical data relating to

BRIEF DESCRIPTION OF THE INVENTION

[0009A] Disclosed herein is a computer-based method of a Risk Based Decisioning Service (RBDS) for evaluating a risk of fraud associated with a payment card transaction processed over a payment card interchange network, the method implemented using a computer device coupled to a memory device, the method comprising: receiving, electronically, by the RBDS, from a point-of-sale (POS) terminal, payment card transaction messages, in an electronic form, relating to a purchase transaction using a payment card account, the payment card transaction messages including at least one of an authorization request and an authorization response; storing data elements of the payment card transaction messages in an RBDS data store; receiving an application event transaction message relating to a non-purchase electronic interaction with the payment card account, the non-purchase interaction initiated with a second computer system, the non-purchase interaction occurring prior to the purchase transaction; storing data elements of the application event transaction message in the RBDS data store; receiving, electronically, by the RBDS, payment card account reputation messages, in an electronic form, from the second computer system, the payment card account reputation messages including historical data relating to the trustworthiness of the payment card account, said second computer system being different than the POS terminal; storing data elements of the payment card account reputation message in the RBDS data store; comparing, by the RDBS, at least one electronic data element in each stored payment card transaction messages to at least one electronic data element in the stored payment card account reputation message and at least one stored prior transaction history electronic data element from the payment card transaction messages; and at least one of when requested and when determined by the RBDS, determining a score of a risk of fraud of the transaction and a trustworthiness score of the payment card account based on the comparison.

[0009B] Disclosed herein is a Risk Based Decisioning Service (RBDS) computer system for processing data associated with a payment card cardholder account, the RBDS computer system comprising: one or more memory devices comprising one or more application data event stores; a plurality of special purpose processors communicatively coupled to said one or more memory devices; a transaction component communicatively coupled to point-of-sale (POS) terminal configured to receive payment card transaction messages relating to a purchase transaction using a payment card account

from the POS terminal, the payment card transaction messages including at least one of an authorization request and an authorization response, the payment card transaction messages including an application event transaction message comprising information regarding a non-purchase interaction with the payment card account, the non-purchase interaction initiated with a second computer system, the non-purchase interaction occurring non-contemporaneously with the purchase transaction, the application event transaction message further comprising a device identifier comprising at least one of a software-based device identifier and a hardware identifier associated with the computer system that initiated the non-purchase interaction; a reputation component configured to receive payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account from said second computer system, said second computer system being different than the point-of-sale (POS) terminal; a comparator component configured to compare at least one electronic data element in each payment card transaction messages to at least one electronic data element in at least one of the payment card reputation account message and prior transaction history; and a decisioning component configured to determine a score that indicates a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

[0009C] Disclosed herein is one or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon when executed by at least one processor communicatively coupled to said computer-readable storage media, the computer executable instructions cause the processor to: receive, from a point-of-sale (POS) terminal, payment card transaction messages relating to a purchase transaction using a payment card account, the payment card transaction messages relating to a purchase interaction with at least one of an agent acting on behalf of a cardholder of the payment card account and an agent acting on behalf of an issuer of the payment card account, the payment card transaction messages including at least one of an authorization request and an authorization response, the payment card transaction messages including an application event transaction message, the application event transaction message comprising information regarding a non-purchase interaction with the payment card account, the non-purchase interaction initiated with a second computer system, the non-purchase interaction occurring non-contemporaneously with the purchase transaction, the application event transaction message further comprising a device identifier of the computer system that initiated the non-purchase interaction, the device identifier

comprising at least one of a software-based device identifier and a hardware identifier; receive payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account from said second computer system, said second computer system being different than the POS terminal; compare at least one electronic data element in each payment card transaction messages to at least one electronic data element in at least one of the payment card account reputation message and prior transaction history; and determine at least one of a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

[0010] In one embodiment, a computer-based method for evaluating a risk of fraud in a payment card transaction on a payment card interchange network, is implemented using a computer device coupled to a memory device, and includes receiving payment card transaction messages relating to a payment card account wherein the payment card transaction messages relate to interactions with a cardholder, an issuer of the payment card account, or both. The payment card transaction messages include an authorization request, an authorization response, and an Application Event and the Application Event includes an interaction with the payment card account in other than a purchase interaction wherein the Application Event transaction message further comprising a device identifier comprising at least one of a device identifier and a hardware identifier associated with the device. The method further includes receiving payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account, comparing at least one data element in each payment card transaction messages to at least one data element in at least one of: the payment card reputation message and prior transaction history, and determining at least one of a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

[0011] In another embodiment, a computer system for processing data associated with a payment card cardholder account includes a memory device, a processor in communication with the memory device, and a transaction component configured to receive payment card transaction messages relating to a payment card account, the payment card transaction messages relating to interactions with at least one of an agent on behalf of a cardholder of the payment card account and an agent on behalf of an issuer of the payment card account, the payment card transaction messages including at least one of an

authorization request, an authorization response, and an Application Event, the Application Event comprising an interaction with the payment card account in other than a purchase interaction, the Application Event transaction message further comprising a device identifier comprising at least one of a device identifier and a hardware identifier associated with the device. The computer system further includes a reputation component configured to receive payment card account reputation messages that include historical data relating to

CLAIMS

1. A computer-based method for evaluating a risk of fraud in a payment card transaction on a payment card interchange network, the method implemented using a computer device coupled to a memory device, the method comprising:

receiving payment card transaction messages relating to a payment card account, the payment card transaction messages relating to interactions with at least one of an agent on behalf of a cardholder of the payment card account and an agent on behalf of an issuer of the payment card account, the payment card transaction messages including at least one of an authorization request, an authorization response and an application event, the application event comprising an interaction with the payment card account in other than a purchase interaction, the application event transaction message further comprising a device identifier comprising at least one of a device identifier and a hardware identifier associated with the device ;

receiving payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account;

comparing at least one data element in each payment card transaction messages to at least one data element in at least one of: the payment card reputation message and prior transaction history, and

determining at least one of a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

2. The computer-based method of Claim 1, wherein the payment card transaction messages include at least one of a Primary Account Number (PAN), a virtual PAN, a transaction amount, a merchant identifier, an acquirer identifier, a transaction date-time, and an address verification.

3. The computer-based method of Claim 1, wherein the payment card reputation messages include at least one of attributes of the authorization, a payment history of the payment card account, historical authorization details, historical clearing transaction details, historical chargeback details, and reports of a compromised PAN.

4. The computer-based method of Claim 3, wherein the reports of a comprised PAN are received from at least one of an issuer, a merchant, an acquirer, a payment card cardholder, a law enforcement agency, and security agency.

5. The computer-based method of Claim 1, wherein the application event messages include at least one of a billing address, a shipping address, an email address, a phone number, an application account identification (ID), a wallet ID, an Internet protocol (IP) address, a device identifier, and a hardware identifier.

6. The computer-based method of Claim 1, wherein personally identifiable information is encrypted to protect the cardholders' privacy.

7. The computer-based method of Claim 1, further comprising receiving the payment card transaction messages, the payment card reputation messages, and the application event messages at a central store that is updated periodically.

8. A computer system for processing data associated with a payment card cardholder account, the computer system comprising:

a memory device;

a processor in communication with the memory device;

a transaction component configured to receive payment card transaction messages relating to a payment card account, the payment card transaction messages relating to interactions with at least one of an agent on behalf of a cardholder of the payment card account and an agent on behalf of an issuer of the payment card account, the payment card transaction messages including at least one of an authorization request, an authorization response, and an application event, the application event comprising an interaction with the payment card account in other than a purchase interaction, the application event transaction message further comprising a device identifier comprising at least one of a device identifier and a hardware identifier associated with the device ;

a reputation component configured to receive payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account;

a comparator component configured to compare at least one data element in each payment card transaction messages to at least one data element in at least one of: the payment card reputation message and prior transaction history;

a decisioning component configured to determine at least one of a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

9. The computer system of Claim 8, wherein the payment card transaction messages include at least one of a Primary Account Number (PAN), a virtual PAN, a transaction amount, a merchant identifier, an acquirer identifier, a transaction date-time, and an address verification.

10. The computer system of Claim 8, wherein the payment card reputation messages include at least one of attributes of the authorization, a payment history of the payment card account, historical authorization details, historical clearing transaction details, historical chargeback details, and reports of a compromised PAN.

11. The computer system of Claim 10, wherein the reports of a comprised PAN are received from at least one of an issuer, a merchant, an acquirer, a payment card cardholder, a law enforcement agency, and security agency.

12. The computer system of Claim 8, wherein the application event messages include at least one of a billing address, a shipping address, an email address, a phone number, an application account identification (ID), a wallet ID, an Internet protocol (IP) address, a device identifier, and a hardware identifier.

13. The computer system of Claim 8, wherein personally identifiable information is encrypted to protect the cardholders' privacy.

14. The computer system of Claim 8, wherein the payment card transaction messages, the payment card reputation messages, and the application event messages are updated periodically at a central store..

15. 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 payment card transaction messages relating to a payment card account, the payment card transaction messages relating to interactions with at least one of an agent on behalf of a cardholder of the payment card account and an agent on behalf of an issuer of the payment card account, the payment card transaction messages including at least one of an authorization request, an authorization response, and an application event, the application event comprising an interaction with the payment card account in other than a purchase interaction, the application event transaction message further comprising a device identifier comprising at least one of a device identifier and a hardware identifier associated with the device ;

receive payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account;

compare at least one data element in each payment card transaction messages to at least one data element in at least one of: the payment card reputation message and prior transaction history; and

determine at least one of a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

16. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to receive payment card transaction messages that include at least one of a Primary Account Number (PAN), a virtual PAN, a transaction amount, a merchant identifier, an acquirer identifier, a transaction date-time, and an address verification.

17. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to receive payment card reputation messages that include at least one of attributes of the authorization, a payment history of the payment card account, historical authorization details, historical clearing transaction details, historical chargeback details, and reports of a compromised PAN.

18. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to receive reports of a comprised PAN from at least one of an issuer, a merchant, an acquirer, a payment card cardholder, a law enforcement agency, and security agency.

19. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to receive application event messages that include at least one of a billing address, a shipping address, an email address, a phone number, an application account identification (ID), a wallet ID, an Internet protocol (IP) address, a device identifier, and a hardware identifier.

20. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to periodically update the payment card transaction messages, the payment card reputation messages, and the application event messages at a central store.

CLAIMS

1. A computer-based method of a Risk Based Decisioning Service (RBDS) for evaluating a risk of fraud associated with a payment card transaction processed over a payment card interchange network, the method implemented using a computer device coupled to a memory device, the method comprising:

receiving, electronically, by the RBDS, from a point-of-sale (POS) terminal, payment card transaction messages, in an electronic form, relating to a purchase transaction using a payment card account, the payment card transaction messages including at least one of an authorization request and an authorization response;

storing data elements of the payment card transaction messages in an RBDS data store;

receiving an application event transaction message relating to a non-purchase electronic interaction with the payment card account, the non-purchase interaction initiated with a second computer system, the non-purchase interaction occurring prior to the purchase transaction;

storing data elements of the application event transaction message in the RBDS data store;

receiving, electronically, by the RBDS, payment card account reputation messages, in an electronic form, from the second computer system, the payment card account reputation messages including historical data relating to the trustworthiness of the payment card account, said second computer system being different than the POS terminal;

storing data elements of the payment card account reputation message in the RBDS data store;

comparing, by the RDBS, at least one electronic data element in each stored payment card transaction messages to at least one electronic data element in the stored payment card account reputation message and at least one stored prior transaction history electronic data element from the payment card transaction messages; and

at least one of when requested and when determined by the RBDS, determining a score of a risk of fraud of the transaction and a trustworthiness score of the payment card account based on the comparison.

2. The computer-based method of Claim 1, wherein the payment card transaction messages include at least one of a Primary Account Number (PAN), a virtual PAN, a transaction amount, a merchant identifier, an acquirer identifier, a transaction date-time, and an address verification.

3. The computer-based method of Claim 1, wherein the payment card account reputation messages include at least one of attributes of the authorization, a payment history of the payment card account, historical authorization details, historical clearing transaction details, historical chargeback details, and reports of a compromised PAN.

4. The computer-based method of Claim 3, wherein the reports of a compromised PAN are received from at least one of an issuer, a merchant, an acquirer, a payment card cardholder, a law enforcement agency, and security agency.

5. The computer-based method of Claim 1, wherein the application event transaction messages include at least one of a billing address, a shipping address, an email address, a phone number, an application account identification (ID), a wallet ID, an Internet protocol (IP) address, a device identifier, and a hardware identifier.

6. The computer-based method of Claim 1, wherein personally identifiable information is encrypted to protect the cardholders' privacy.

7. The computer-based method of Claim 1, further comprising receiving the payment card transaction messages, the payment card account reputation messages, and the application event transaction messages at a central store that is updated periodically.

8. A Risk Based Decisioning Service (RBDS) computer system for processing data associated with a payment card cardholder account, the RBDS computer system comprising:

one or more memory devices comprising one or more application data event stores;

a plurality of special purpose processors communicatively coupled to said one or more memory devices;

a transaction component communicatively coupled to point-of-sale (POS) terminal configured to receive payment card transaction messages relating to a purchase transaction using a payment card account from the POS terminal, the payment card transaction messages including at least one of an authorization request and an authorization response, the payment card transaction messages including an application event transaction message comprising information regarding a non-purchase interaction with the payment card account, the non-purchase interaction initiated with a second computer system, the non-purchase interaction occurring non-contemporaneously with the purchase transaction, the application event transaction message further comprising a device identifier comprising at least one of a software-

based device identifier and a hardware identifier associated with the computer system that initiated the non-purchase interaction;

a reputation component configured to receive payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account from said second computer system, said second computer system being different than the point-of-sale (POS) terminal;

a comparator component configured to compare at least one electronic data element in each payment card transaction messages to at least one electronic data element in at least one of the payment card reputation account message and prior transaction history; and

a decisioning component configured to determine a score that indicates a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

9. The computer system of Claim 8, wherein the payment card transaction messages include at least one of a Primary Account Number (PAN), a virtual PAN, a transaction amount, a merchant identifier, an acquirer identifier, a transaction date-time, and an address verification.

10. The computer system of Claim 8, wherein the payment card account reputation messages include at least one of attributes of the authorization, a payment history of the payment card account, historical authorization details, historical clearing transaction details, historical chargeback details, and reports of a compromised PAN.

11. The computer system of Claim 10, wherein the reports of a compromised PAN are received from at least one of an issuer, a merchant, an acquirer, a payment card cardholder, a law enforcement agency, and security agency.

12. The computer system of Claim 8, wherein the application event transaction messages include at least one of a billing address, a shipping address, an email address, a phone number, an application account identification (ID), a wallet ID, an Internet protocol (IP) address, a device identifier, and a hardware identifier.

13. The computer system of Claim 8, wherein personally identifiable information is encrypted to protect the cardholders' privacy.

14. The computer system of Claim 8, wherein the payment card transaction messages, the payment card account reputation messages, and the application event transaction messages are updated periodically at a central store.

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

receive, from a point-of-sale (POS) terminal, payment card transaction messages relating to a purchase transaction using a payment card account, the payment card transaction messages relating to a purchase interaction with at least one of an agent acting on behalf of a cardholder of the payment card account and an agent acting on behalf of an issuer of the payment card account, the payment card transaction messages including at least one of an authorization request and an authorization response, the payment card transaction messages including an application event transaction message, the application event transaction message comprising information regarding a non-purchase interaction with the payment card account, the non-purchase interaction initiated with a second computer system, the non-purchase interaction occurring non-contemporaneously with the purchase transaction, the application event transaction message further comprising a device identifier of the computer system that initiated the non-purchase interaction, the device identifier comprising at least one of a software-based device identifier and a hardware identifier;

receive payment card account reputation messages that include historical data relating to the trustworthiness of the payment card account from said second computer system, said second computer system being different than the POS terminal;

compare at least one electronic data element in each payment card transaction messages to at least one electronic data element in at least one of the payment card account reputation message and prior transaction history; and

determine at least one of a risk of fraud of the transaction and a trustworthiness of the payment card account based on the comparison.

16. The computer-readable storage media of Claim 15, wherein the computer executable instructions further cause the processor to receive payment card transaction messages that include at least one of a Primary Account Number (PAN), a virtual PAN, a transaction amount, a merchant identifier, an acquirer identifier, a transaction date-time, and an address verification.

17. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to receive payment card account reputation messages that include at least one of attributes of the authorization, a payment history of the payment card account, historical authorization details, historical clearing transaction details, historical chargeback details, and reports of a compromised PAN.

18. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to receive reports of a compromised PAN from at least one of an issuer, a merchant, an acquirer, a payment card cardholder, a law enforcement agency, and security agency.

19. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to receive application event transaction messages that include at least one of a billing address, a shipping address, an email address, a phone number, an application account identification (ID), a wallet ID, an Internet protocol (IP) address, a device identifier, and a hardware identifier.

20. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to periodically update the payment card transaction messages, the payment card account reputation messages, and the application event transaction messages at a central store.