SYSTEMS AND METHODS FOR DEVICE AUTHENTICATION

RELATED APPLICATIONS

[0001] This application is a Continuation-In-Part of U.S. Patent Application Ser. No. 15/069,418, filed March 14, 2016, the disclosure of which is hereby incorporate, by reference, in its entirety.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0002] The present invention generally relates to systems and methods for device authentication.

2. Description Of The Related Art

[0003] It is commonplace for customers to conduct transactions online using a mobile device. For example, a customer may select an item and go to a "checkout screen" where the user then enters his or her credit card information, billing address, and shipping address. The merchant then provides this information to a financial institution to authorize the underlying transaction.

SUMMARY OF THE INVENTION

[0004] Systems and methods for device authentication are disclosed. In one embodiment, a payment system may include a financial institution that may include an acquirer portion; a payment network portion; and an issuer portion. The acquirer portion may communicate with the issuer portion via the payment network portion. The system may further include a merchant having a

merchant-acquirer relationship with the financial institution, the merchant in communication with the acquirer portion using a first network; and a mobile electronic device associated with a customer comprising at least one computer processor executing a mobile payment application. The acquirer portion may receive, from the merchant, at least one mobile device credential and a payment credential that were received from the mobile payment application in conjunction with a transaction, the acquirer portion further receiving transaction data for the transaction from the merchant. The issuer portion may receive, via the payment network portion, the mobile device credentials, the payment credentials, and transaction data from the acquirer portion. The issuer portion may identify and authenticate the customer based on the mobile device credentials and the payment credential.

[0005] In one embodiment, the acquirer portion and/or the payment network portion is associated with a partner of the financial institution.

[0006] In one embodiment, the acquirer portion may further host a risk management service, and the risk management service receives the at least one mobile device credential from the mobile payment application.

[0007] In one embodiment, the at least one mobile device credential comprises at least one of mobile device operating system data, mobile device browser data, mobile device locale data, mobile device system data, mobile device settings data, mobile device cookie data, mobile application data, and a mobile device identifier.

[0008] In one embodiment, the mobile application may communicate with the issuer portion using a second network.

[0009] In one embodiment, the acquirer portion, a risk management service executed by the merchant, a risk management service executed by the acquirer, and the issuer portion may deny the transaction. The transaction may be denied for at least one of a shipping address not matching a billing address; a velocity of transactions with the payment credential; an IP address of the mobile device; and a proxy being used with the mobile device.

[0010] In one embodiment, the payment network portion may provide real-time two-way communication between the issuer portion and the merchant.

[0011] A method for authenticating a device may include, at a financial institution comprising an acquirer portion, a payment network portion, and an issuer portion: (1) the acquirer portion receiving, from the merchant, at least one mobile device credential and a payment credential that were received electronically from a mobile payment application executed by a mobile electronic device in conjunction with a transaction, the acquirer portion further receiving transaction data for the transaction from the merchant; (2) the issuer portion receiving, via the payment network portion, the mobile device credentials, the payment credentials, and transaction data from the acquirer portion; and (3) at least one computer processor at the issuer portion identifying and authenticating the customer based on the mobile device credentials and the payment credential.

[0012] In one embodiment, the acquirer portion and/or the payment network portion may be associated with a partner of the financial institution.

[0013] In one embodiment, a risk management service hosted by the acquirer portion may receive the at least one mobile device credential from the mobile payment application.

[0014] In one embodiment, the at least one mobile device credential comprises at least one of mobile device operating system data, mobile device browser data, mobile device locale data, mobile device system data, mobile device settings data, mobile device cookie data, mobile application data, and a mobile device identifier.

[0015] In one embodiment, the mobile application may communicate with the issuer portion using a second network.

[0016] In one embodiment, the method may further include the at least one computer processor at the issuer portion authorizing the transaction.

[0017] In one embodiment, the method may further include the at least one computer processor at the issuer portion associating the authorization with the at least one mobile device credential.

[0018] In one embodiment, the method may further include denying the transaction by at least one of the an acquirer portion, a risk management service executed by the merchant, a risk management service executed by the acquirer, and the issuer portion. The transaction may be denied for at least one of a shipping address not matching a billing address; a velocity of transactions with the payment credential; an IP address of the mobile device; and a proxy being used with the mobile device.

[0019] In one embodiment, the method may further include at least one of the an acquirer portion, a risk management service executed by the merchant, and a risk management service executed by the acquirer normalizing at least one of the payment credential and the transaction data.

[0020] In one embodiment, the method may further include at least one of the an acquirer portion, a risk management service executed by the merchant, and a risk management service executed by the acquirer validating a shipping address using third party data.

[0021] In one embodiment, a payment system may include a financial institution comprising an acquirer portion, a payment network portion, and an issuer portion. The acquirer portion may communicates with the issuer portion via the payment network portion, the merchant may have a merchant-acquirer relationship with the financial institution and may be in communication with the acquirer portion using a first network, and a mobile electronic device associated with a customer comprising at least one computer processor executing a mobile payment application. The acquirer portion may receive, from the merchant, at least one device credential and a payment credential that were received from the mobile payment application in conjunction with a transaction, the acquirer portion further receiving transaction data for the transaction from the merchant, and may perform a first validation assessment on the transaction based on the transaction data. The payment network portion may receive, from the acquirer portion, the device credential, the payment credential, the transaction data, and the first validation assessment; and may perform a second validation assessment on the transaction based on the transaction data. The issuer portion may receive, from the payment network portion, the device credential, the payment

credentials, and transaction data from the acquirer portion, and may identify and authenticate the customer based on the device credential, the payment credential, and at least one of the first validation assessment and the second validation assessment.

[0022] In one embodiment, the device may be a mobile electronic device.

[0023] In one embodiment, the acquirer portion and/or the payment network portion may be associated with a partner of the financial institution.

[0024] In one embodiment, the acquirer portion may perform the first validation assessment on the transaction based on the transaction data and data retrieved from a third party data source. The third party data source may be an address database, an identity verification service, a fraud database, an IP address database, a device information database, etc.

[0025] In one embodiment, the first validation assessment and/or the second validation assessment may be a risk score.

[0026] In one embodiment, the acquirer portion may provide the first validation assessment to the payment network portion.

[0027] In one embodiment, the payment network portion may perform the second validation assessment on the transaction based on the transaction data and data retrieved from a third party data source. The third party data source may be an address database, an identity verification service, a fraud database, an IP address database, a device information database, etc.

[0028] In one embodiment, the payment network portion may provide the first validation assessment and the second validation assessment to the issuer portion.

[0029] In one embodiment, the payment network portion may update the first validation assessment with the second validation assessment, and provide the second validation assessment to the issuer portion.

[0030] In one embodiment, the issuer portion may further perform a first validation assessment on the transaction based on the transaction data and data retrieved from a third party data source. The third party data source may be an address database, an identity verification service, a fraud database, an IP address database, a device information database, etc.

[0031] According to another embodiment a method for authenticating a transaction may include, at a financial institution comprising an acquirer portion, a payment network portion, and an issuer portion: (1) the acquirer portion receiving, from the merchant, at least one device credential and a payment credential that were received from the mobile payment application in conjunction with a transaction, the acquirer portion further receiving transaction data for the transaction from the merchant; (2) the acquirer portion performing a first validation assessment on the transaction based on the transaction data and first data retrieved from a first data source; (3) the payment network receiving, from the acquirer portion, the device credential, the payment credential, the transaction data, and the first validation assessment; (4) the payment network portion performing a second validation assessment on the transaction based on the transaction data and second data retrieved from a second data source; (5) the

issuer portion receiving, from the payment network portion, the device credential, the payment credentials, transaction data from the acquirer portion and the first validation assessment, and the second validation assessment; and (6) the issuer portion identifying and authenticating the customer based on the device credential, the payment credential, and at least one of the first validation assessment and the second validation assessment.

[0032] In one embodiment, the device may be a mobile electronic device.

[0033] In one embodiment, the first data source and the second data source may include an address database, an identity verification service, a fraud database, an IP address database, a device information database, etc.

[0034] In one embodiment, the method may further include the acquirer portion denying the transaction based on the first validation assessment.

[0035] In one embodiment, the method may further include the payment network portion denying the transaction based on at least one of the first validation assessment and the second validation assessment.

BRIEF DESCRIPTION OF THE DRAWINGS

[0036] For a more complete understanding of the present invention, the objects and advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0037] Figure 1 depicts a system for device authentication according to one embodiment;

[0038] Figure 2 depicts a method for device authentication according to one embodiment;

[0039] Figure 3 depicts a system for conducting a transaction according to one embodiment; and

[0040] Figure 4 depicts a method for conducting a transaction according to one embodiment.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0041] Several embodiments of the present invention and their advantages may be understood by referring to Figures 1-4.

[0042] Embodiments disclosed herein facilitate on-line transactions involving a mobile device.

[0043] Embodiments disclosed herein may leverage a device identification method to provide low friction payment interactions in conducing online payments, mobile wallet payments, etc., and may influence merchants in adopting a consistent and/or standard device identification methodology.

[0044] In one embodiment, a single store of device fingerprints captured by merchants that link the method of creation to the device fingerprint along with the date it was created and the method by which it was created is disclosed. The device fingerprint may further identify a link between the device fingerprint and payment transactions sourced by a payment processor. For example, the link may identify that a particular payment came from a particular device.

[0045] Embodiments disclose methodologies that may assess the device trustworthiness based on prior user actions on the device. In one embodiment, an issuer may provide one or more of an assessment of the device and a the customer and return a trustworthiness assessment of the device, a recognition value for the consumer and an assessment of a transaction risk.

[0046] In one embodiment, certain devices may be certified. For example, specific configurations of web and/or mobile systems that test the merchants ability to recognize them may be certified.

[0047] In one embodiment, when a merchant has registered a customer device and wants to submit a device fingerprint with the payment transaction, the merchant may provide a shorter unique identifier provided by an issuer along with other enhanced data (e.g., device fingerprint information).

[0048] In another embodiment, when a merchant submits a payment transaction, the issuer may provide the additional data points necessary to support device fingerprinting (e.g., as determined by risk) to the authorization flow as enhanced data.

[0049] In one embodiment, merchants may be able to submit, along with the device fingerprint, additional information such as customer name and address in order to provide a full consumer persona for assessment by the issuer. The issuer may provide an assessment of the device and consumer persona and return a trust score of the device, a recognition value for the consumer and an assessment of transaction risk.

[0050] In one embodiment, an on-line payment system may include an option for device recognition and enablement of "1-Click" shopping that includes a default payment product and shipping address and the ability to opt for a lightweight verification mechanism. The merchant may accept the payment method and shipping address and process the payment without prompting the user for further information unless the customer has opted for a light weight verification mechanism which will be invoked and the results will affect the notification back to the merchant as the consumer may opt not to proceed with payment.

[0051] In one embodiment, the customer may to determine the level of interaction available for "1-Click" shopping. For example, the customer may configure it to allow selection from a set of payment devices and to determine which shipping address to use based on identified devices.

[0052] Referring to Figure 1, a system for device authentication is disclosed according to one embodiment. System 100 may include customer 110, merchant 120, and financial institution 140. In one embodiment, acquirer 150, payment network 160, and issuer 170 may all be associated with or under the control of financial institution 140 or a payment processing partner of financial institution 140.

[0053] Customer 110 may interact with merchant 120 using device 115. Device 115 may be any suitable electronic device that may execute a wallet application, access a merchant website, execute a payment application, etc.

[0054] In one embodiment, device 115 may be a mobile electronic device, such as a smartphone, tablet computer, etc.

[0055] In one embodiment, merchant 120 may have a relationship with financial institution 140, such as a merchant-acquirer relationship.

[0056] Merchant 120 and acquirer 150 may provide risk management services (RMS) 125 and 155, respectively. RMS 125 may collect device fingerprint data from device 115. The device fingerprint data may be used to uniquely identify device 115 from other devices. Device fingerprint data may include, for example, operating system data (e.g., operating system version number, etc.), browser data (e.g., browser, version, etc.), locale data (e.g., country, language, etc.), hardware/system data (e.g., operating system, screen resolution, screen aspect ratio, manufacturer, serial number, SIM card, jailbreak information, etc.), settings data, cookie data, mobile application data, etc. It may further collect data from a mobile wallet application, such as user id and password. Other device data may be used as is necessary and/or desired.

[0057] Merchant 120 may also collect transaction information, including, for example, customer information (name, shipping address, etc.), payment information (e.g., card number), and price data.

[0058] In one embodiment, RMS 155 may receive the device fingerprint data from RMS 125, and may provide the device fingerprint data to issuer 170 via payment network 170.

[0059] In one embodiment, RMS 125 and/or RMS 155 may receive, for example, information about the customer, transaction information (e.g., amount of transaction, shipping address, billing address, etc.), content of the customer's shopping card, the frequency of usage of the payment instrument (e.g., credit card), information from third parties (e.g., confirmation that the shipping

address is valid from the United States Postal Service), aging information, number of customer transactions with merchant, email address black list, IP/proxy blacklist, etc.

[0060] In one embodiment, because acquirer 150, payment network 160, and issuer 170 may be part of, or under the control of, financial institution 140, decision making among these elements may be distributed. In addition, RMS 125 and RMS 155 may also be included in the distributed decision making. For example, one or more of RMS 125, acquirer 150, RMS 155, and issuer 170 may compare the shipping address to the billing address; may determine if there are suspicious number of deliveries to that email address; may determine if there are a suspicious number of transactions using the payment instrument with multiple merchants; may determine if there are a suspicious number of transactions from different IP addresses using the same payment instrument; may determine if the card is being used on a device with a proxy; etc.

[0061] In one embodiment, payment network 160 may be an enhanced payment network that may communicate additional data, such as device data, to the issuer. An example of such a payment network is ChaseNet. In one embodiment, payment network 160 may provide two-way communication from the merchant to the issuer that may provide portions of real-time authorization, portions of non-real time authorization, and combinations thereof. For example, transaction data may be provided in real-time to authorize the transaction, but if a shipping address does not match a billing address, a flag may be provided in real-time, but details on the discrepancy (e.g., the mismatched address) may be provided in due course.

[0062] In one embodiment, learning may be used to inform acquirer 150, RMS 155, merchant 120, RMS 125, and/or device 115 of transaction issues. For example, issuer 170 may determine that the financial instrument submitted for a transaction is valid, but the device is invalid. Issuer 170 may inform acquirer 150 to deny the transaction and merchant 120 to not ship the order. In one embodiment, the application on device 115 may be deactivated, have the financial instrument removed, an out-of-band message communicated to customer 110, etc.

[0063] In one embodiment, RMS 125 and/or RMS 155 may update respective databases with transaction information.

[0064] In one embodiment, customer 110 may interact with issuer 170 directly using device 115. For example, device 115 may execute an application (not shown) associated with issuer 170, access issuer 170's website, etc. In one embodiment, issuer 170 may authenticate device 115 and/or customer 110 directly.

[0065] Referring to Figure 2, a method of device authentication is disclosed according to one embodiment.

[0066] In step 205, a customer that is conducting a transaction may present a payment device to a merchant. In one embodiment, customer may present the payment device using, for example, a mobile wallet application executed by a mobile electronic device.

[0067] In step 210, the merchant may collect payment device information and device information from the device. In one embodiment, this may be

performed by, on in conjunction with, a risk management service (RMS). In one embodiment, the information that may be collected may include customer information, payment information, transaction information, shipping information, and device information.

[0068] In one embodiment, the combination of the payment device information (e.g., a credit card number) and device information may be sufficient to identify and authenticate the customer without requiring additional logging in to the financial institution and/or merchant.

[0069] In step 215, the merchant and/or RMS may provide the collected information to its acquirer.

[0070] In one embodiment, the acquirer may perform partial decisioning on the transaction. For example, the acquirer may compare the shipping address for the transaction to the billing address for inconsistencies.

[0071] In step 220, the acquirer may provide the collected information to the issuer using, for example, a payment network. In one embodiment, the acquirer, the payment network, and the issuer may all be part of, associated with, and/or controlled by the financial institution.

[0072] In one embodiment, the payment network may handle a larger amount of data than a conventional payment network, such as VisaNet. An example of a suitable payment network is ChaseNet. Such a payment network may communicate additional data, such as the device information, in addition to the payment device information and transaction information.

[0073] In one embodiment, the acquirer, either RMS, and/or the issuer may normalize the data from the merchant. For example, each merchant may collect customer data, device data, etc. in a different format. Thus, any or the acquirer, RMSs, or the issuer may normalize the data (e.g., look up the missing digits from the nine digit ZIP code if only five digits are provided) so that it has a common format.

[0074] For example, a merchant may have its own template for receiving customer date (e.g., customer name fields, customer address fields, customer

[0075] In step 225, the issuer may authenticate the customer based on the payment device information and the device information. In one embodiment, the combination of the payment device and the device is sufficient to authenticate the customer.

[0076] In one embodiment, intelligence may be used to take appropriate action(s) following the authentication, or lack thereof. For example, if a customer cannot be authenticated because the device could not be validated, but the credit card number was valid, only transactions from the device may be blacklisted, while transactions with the card may be approved. Additional actions, including sending out-of-band messages to the customer, disabling an electronic wallet, disabling an on-line account, etc. may be taken as is necessary and/or desired.

[0077] In one embodiment, issuer may communicate the lack of authentication to the acquirer and/or the merchant. Thus, if the same device attempts the transaction with the same payment device, the acquirer may deny the transaction without involvement from the issuer.

[0078] In one embodiment, once the customer is authenticated, the customer may be authenticated with other merchants that have a similar relationship with the financial institution.

[0079] In step 230, the issuer may decision the transaction (e.g., approve or deny the transaction) based on the transaction information, account information, etc.

[0080] In step 235, the issuer may provide the decision to the merchant and the acquirer via the payment network.

[0081] In one embodiment, the issuer may provide the decision to the acquirer, merchant, and the device.

[0082] Referring to Figure 3, a system for conducting a transaction is disclosed according to one embodiment. System 300 may include customer 110, merchant 320, and financial institution 340. In one embodiment, acquirer 350, payment network 360, and issuer 370 may all be associated with or under the control of financial institution 340 or a payment processing partner of financial institution 340.

[0083] In one embodiment, merchant 320, acquirer 350, payment network 360, issuer 370, and financial institution 340 may be similar to merchant 120, acquirer 150, payment network 160, issuer 170, and financial institution 140, respectively.

[0084] In one embodiment, merchant 320, acquirer 350, payment network 360, issuer 370 may each be provided with risk management system (RMS)

325, 355, 365, and 375, respectively. RMS 325, RMS 355, RMS 365, and RMS 375 may function similar to RMS 125 and RMS 155, described above.

[0085] In one embodiment, merchant 320, acquirer 350, payment network 360, issuer 370 may be provided with validation tools 327, validation tools 357, validation tools 367, and 377, respectively. In one embodiment, validation tools may access internal and/or external source(s) 380 for data validation. For example, merchant 320 may use validation tool 327 to validate the existence and validity of a shipping address, while acquirer 350 may use validation tools 357 to check against a database of fraudulent addresses, verified good addresses, etc.

[0086] Validation tools 327, 357, 367, and 377 may work with associated RMS 325, RMS 355, RMS 365, and RMS 375 to perform distributed decision making regarding each transaction.

[0087] In one embodiment, merchant 320, acquirer 350, payment network 360, issuer 370 may communicate with one or more external source 380 to retrieve information that may assist in the distributed decision making. Example external sources may include address information (e.g., U.S. Postal Service databases), fraud databases, IP address databases, device information databases, other customer purchase information from other merchants, financial institutions, identity validation services, device operators for carrier verification, social engineering and analytics (e.g., Axciom or Experian), compromised email databases, etc.

[0088] In one embodiment, RMS 325, 355, 365, 375 and/or Validation Tools 327, 357, 367, 377 may receive a transaction and provide an assessment

of the transaction. Depending on its position within the transaction chain (e.g., merchant, acquirer, payment network, or issuer), RMS 325, 355, 365, 375 and/or Validation Tools 327, 357, 367, 377 may receive an assessment from one or more prior elements in the transaction chain. For example, RMS 365 and/or Validation Tools 367 may receive assessments from RMS 325/Validation Tools 327 and RMS 355/Validation Tools 357.

[0089] For example, a merchant tool and/or RMS may assess the accuracy and validity of the customer information based on the information collected including the type of merchandise, the velocity at the merchant level, the IP address, and device fingerprint, device status (e.g., new, old, etc.), etc. Acquirer 350 may use some or all of the information as merchant 320 to validate whether they are any risk intelligence seen for the customer 110 based on all transactions across all the merchants for which this acquirer is processing, Payment network 360 may evaluate a transaction against, for example, a compromised card database, identify theft info, etc. across all the issuers information for the given card holder name or specific information, such as email address, etc. Issuer 370 may perform its own validation based on card information as well as the full relationship with the consumer, including, for example, identifying possible account take over based on recent changes in key consumer information, a velocity across all merchants for the given consumer/card, etc.

[0090] In one embodiment, each RMS 325, 355, 365, 375 and/or Validation Tools 327, 357, 367, 377 may provide an individual assessment, or it may modify the assessment from the prior element(s) in the transaction chain.

[0091] In one embodiment, the assessment may be a go/no-go, a risk score, a flag for further investigation, etc. Any suitable assessment technique may be used as is necessary and/or desired.

[0092] In one embodiment, each element in the transaction chain may have a specific responsibility for transaction assessment. For example, RMS 355 and/or Validation Tools 357 for acquirer 350 may verify the shipping address, and RMS 365 and/or Validation Tools 367 for payment network 360 may verify the IP address for the incoming transaction. In another embodiment, the elements may provide redundant validation. Any suitable responsibility distribution may be used as is necessary and/or desired.

[0093] In one embodiment, any element in the transaction chain may reject a transaction based on its respective RMS and/or validation tools. In another embodiment, only RMS 375 and/or Validation Tools 377 for issuer 370 may rejection a transaction. In one embodiment, RMS 375 and/or Validation Tools 377 may consider assessments from one or more of RMS 325/Validation Tools 327, RMS 355/Validation Tools 357, and RMS 365/Validation Tools 367.

[0094] Referring to Figure 4, a method for conducting a transaction is disclosed according to one embodiment. In step 405, a customer that is conducting a transaction may present a payment device to a merchant. In one embodiment, customer may present the payment device using, for example, a wallet application, and in step 410, the merchant may collect payment device information and device information from the device. These steps may be similar to steps 205 and 210, respectively.

[0095] In one embodiment, in step 415, the merchant's RMS and/or validation tools may perform partial decisioning on the transaction. In one embodiment, merchant may communicate with one or more external source to assess the transaction.

[0096] In step 420, the merchant and/or RMS/Validation tools may provide the collected information to its acquirer. This may be similar to step 215, above, and it may further include the assessment of the transaction.

[0097] In step 425, the acquirer's RMS and/or Validation Tools may assess the transaction and may perform partial decisioning on the transaction. In one embodiment, the acquirer's RMS and/or Validation Tools may access external sources to assess the transaction. The assessment may be provided in any suitable manner (e.g., go, no-go, risk score, etc.).

[0098] In one embodiment, the acquirer's RMS and/or Validation Tools may provide an independent assessment, or may modify the assessment of the merchant.

[0099] In one embodiment, instead of, or in addition to, providing an assessment, the acquirer's RMS and/or Validation Tools may reject the transaction.

[00100] In step 430, the acquirer may provide the collected information and assessment(s) to the issuer using, for example, a payment network. In one embodiment, the acquirer, the payment network, and the issuer may all be part of, associated with, and/or controlled by the financial institution. This may be similar to step 220, above.

[00101] In one embodiment, the payment network may handle a larger amount of data than a conventional payment network, such as VisaNet. An example of a suitable payment network is ChaseNet. Such a payment network may communicate additional data, such as the device information, in addition to the payment device information and transaction information.

[00102] In one embodiment, the acquirer, either RMS, and/or the issuer may normalize the data from the merchant. For example, each merchant may collect customer data, device data, etc. in a different format. Thus, any or the acquirer, RMSs, or the issuer may normalize the data (e.g., look up the missing digits from the nine digit ZIP code if only five digits are provided) so that it has a common format.

[00103] For example, a merchant may have its own template for receiving customer date (e.g., customer name fields, customer address fields, customer

[00104] In step 435, the payment network's RMS and/or Validation Tools may assess the transaction and may perform partial decisioning on the transaction. In one embodiment, the payment network's RMS and/or Validation Tools may access external sources to assess the transaction. The assessment may be provided in any suitable manner (e.g., go, no-go, risk score, etc.).

[00105] In one embodiment, the assessment performed by the payment network RMS and/or payment network may verify different aspects of the transaction from what was verified by the acquirer's RMS and/or payment network. In another embodiment, the verification may be the same, thereby

providing redundancy. Any suitable arrangement of verifications may be provided as necessary and/or desired.

[00106] In one embodiment, the payment network's RMS and/or Validation Tools may provide an independent assessment, or may modify the assessment of the merchant and/or acquirer.

[00107] In one embodiment, instead of, or in addition to, providing an assessment, the payment network's RMS and/or Validation Tools may reject the transaction.

[00108] In step 440, the payment network and/or RMS/Validation tools may provide the collected information to the issuer. This may include all information received by the payment network as well as its assessment.

[00109] In step 445, the issuer may authenticate the customer based on the payment device information and the device information. This may be similar to step 225, above.

[00110] In step 450, the issuer's RMS and/or Validation Tools may assess or decision the transaction and may perform partial decisioning on the transaction. In one embodiment, the issuer's RMS and/or Validation Tools may access external sources to assess the transaction. The assessment may be provided in any suitable manner (e.g., go, no-go, risk score, etc.).

[00111] In one embodiment, the assessment performed by the issuer's RMS and/or payment network may verify different aspects of the transaction from what was verified by the acquirer's or payment network's RMS and/or payment network. In another embodiment, the verification may be the same, thereby

providing redundancy. Any suitable arrangement of verifications may be provided as necessary and/or desired.

[00112] In one embodiment, the issuer's RMS and/or Validation Tools may provide an independent assessment, or may modify the assessment of the merchant acquirer, and/or payment network.

[00113] In step 455, the issuer may provide the decision to the merchant and the acquirer via the payment network. This may be similar to step 235, above.

[00114] Although several embodiments have been disclosed, it should be recognized that the embodiments are not necessarily exclusive.

[00115] The following documents are hereby incorporated, by reference, in their entireties: U.S. Patent Application Serial Number 14/699,511, U.S. Provisional Patent Application Serial No. 62/148,493, filed April 16, 2015; U.S. Provisional Patent Application Serial No. 62/107,800, filed January 26, 2015; and U.S. Provisional Patent Application Serial No. 62/037,891, filed August 15, 2014.

[00116] Hereinafter, general aspects of implementation of the systems and methods of the invention will be described.

[00117] The system of the invention or portions of the system of the invention may be in the form of a "processing machine," such as a general purpose computer, for example. As used herein, the term "processing machine" is to be understood to include at least one processor that uses at least one memory. The at least one memory stores a set of instructions. The instructions

may be either permanently or temporarily stored in the memory or memories of the processing machine. The processor executes the instructions that are stored in the memory or memories in order to process data. The set of instructions may include various instructions that perform a particular task or tasks, such as those tasks described above. Such a set of instructions for performing a particular task may be characterized as a program, software program, or simply software.

[00118] In one embodiment, the processing machine may be a specialized processor.

[00119] As noted above, the processing machine executes the instructions that are stored in the memory or memories to process data. This processing of data may be in response to commands by a user or users of the processing machine, in response to previous processing, in response to a request by another processing machine and/or any other input, for example.

[00120] As noted above, the processing machine used to implement the invention may be a general purpose computer. However, the processing machine described above may also utilize any of a wide variety of other technologies including a special purpose computer, a computer system including, for example, a microcomputer, mini-computer or mainframe, a programmed microprocessor, a micro-controller, a peripheral integrated circuit element, a CSIC (Customer Specific Integrated Circuit) or ASIC (Application Specific Integrated Circuit) or other integrated circuit, a logic circuit, a digital signal processor, a programmable logic device such as a FPGA, PLD, PLA or

PAL, or any other device or arrangement of devices that is capable of implementing the steps of the processes of the invention.

[00121] The processing machine used to implement the invention may utilize a suitable operating system. Thus, embodiments of the invention may include a processing machine running the iOS operating system, the OS X operating system, the Android operating system, the Microsoft Windows™ operating system, the Unix operating system, the Linux operating system, the Xenix operating system, the IBM AIX™ operating system, the Hewlett-Packard UX™ operating system, the Novell Netware™ operating system, the Sun Microsystems Solaris™ operating system, the OS/2™ operating system, the BeOS™ operating system, the Macintosh operating system, the Apache operating system, an OpenStep™ operating system or another operating system or platform.

[00122] It is appreciated that in order to practice the method of the invention as described above, it is not necessary that the processors and/or the memories of the processing machine be physically located in the same geographical place. That is, each of the processors and the memories used by the processing machine may be located in geographically distinct locations and connected so as to communicate in any suitable manner. Additionally, it is appreciated that each of the processor and/or the memory may be composed of different physical pieces of equipment. Accordingly, it is not necessary that the processor be one single piece of equipment in one location and that the memory be another single piece of equipment in another location. That is, it is contemplated that the processor may be two pieces of equipment in two different physical locations. The two distinct pieces of equipment may be

connected in any suitable manner. Additionally, the memory may include two or more portions of memory in two or more physical locations.

[00123] To explain further, processing, as described above, is performed by various components and various memories. However, it is appreciated that the processing performed by two distinct components as described above may, in accordance with a further embodiment of the invention, be performed by a single component. Further, the processing performed by one distinct component as described above may be performed by two distinct components. In a similar manner, the memory storage performed by two distinct memory portions as described above may, in accordance with a further embodiment of the invention, be performed by a single memory portion. Further, the memory storage performed by one distinct memory portion as described above may be performed by two memory portions.

[00124] Further, various technologies may be used to provide communication between the various processors and/or memories, as well as to allow the processors and/or the memories of the invention to communicate with any other entity; i.e., so as to obtain further instructions or to access and use remote memory stores, for example. Such technologies used to provide such communication might include a network, the Internet, Intranet, Extranet, LAN, an Ethernet, wireless communication via cell tower or satellite, or any client server system that provides communication, for example. Such communications technologies may use any suitable protocol such as TCP/IP, UDP, or OSI, for example.

[00125] As described above, a set of instructions may be used in the processing of the invention. The set of instructions may be in the form of a program or software. The software may be in the form of system software or application software, for example. The software might also be in the form of a collection of separate programs, a program module within a larger program, or a portion of a program module, for example. The software used might also include modular programming in the form of object oriented programming. The software tells the processing machine what to do with the data being processed.

[00126] Further, it is appreciated that the instructions or set of instructions used in the implementation and operation of the invention may be in a suitable form such that the processing machine may read the instructions. For example, the instructions that form a program may be in the form of a suitable programming language, which is converted to machine language or object code to allow the processor or processors to read the instructions. That is, written lines of programming code or source code, in a particular programming language, are converted to machine language using a compiler, assembler or interpreter. The machine language is binary coded machine instructions that are specific to a particular type of processing machine, i.e., to a particular type of computer, for example. The computer understands the machine language.

[00127] Any suitable programming language may be used in accordance with the various embodiments of the invention. Illustratively, the programming language used may include assembly language, Ada, APL, Basic, C, C++, COBOL, dBase, Forth, Fortran, Java, Modula-2, Pascal, Prolog, REXX, Visual Basic, and/or JavaScript, for example. Further, it is not necessary that a single

type of instruction or single programming language be utilized in conjunction with the operation of the system and method of the invention. Rather, any number of different programming languages may be utilized as is necessary and/or desirable.

[00128] Also, the instructions and/or data used in the practice of the invention may utilize any compression or encryption technique or algorithm, as may be desired. An encryption module might be used to encrypt data. Further, files or other data may be decrypted using a suitable decryption module, for example.

[00129] As described above, the invention may illustratively be embodied in the form of a processing machine, including a computer or computer system, for example, that includes at least one memory. It is to be appreciated that the set of instructions, i.e., the software for example, that enables the computer operating system to perform the operations described above may be contained on any of a wide variety of media or medium, as desired. Further, the data that is processed by the set of instructions might also be contained on any of a wide variety of media or medium. That is, the particular medium, i.e., the memory in the processing machine, utilized to hold the set of instructions and/or the data used in the invention may take on any of a variety of physical forms or transmissions, for example. Illustratively, the medium may be in the form of paper, paper transparencies, a compact disk, a DVD, an integrated circuit, a hard disk, a floppy disk, an optical disk, a magnetic tape, a RAM, a ROM, a PROM, an EPROM, a wire, a cable, a fiber, a communications channel, a satellite transmission, a memory card, a SIM card, or other remote transmission,

as well as any other medium or source of data that may be read by the processors of the invention.

[00130] Further, the memory or memories used in the processing machine that implements the invention may be in any of a wide variety of forms to allow the memory to hold instructions, data, or other information, as is desired. Thus, the memory might be in the form of a database to hold data. The database might use any desired arrangement of files such as a flat file arrangement or a relational database arrangement, for example.

[00131] In the system and method of the invention, a variety of "user interfaces" may be utilized to allow a user to interface with the processing machine or machines that are used to implement the invention. As used herein, a user interface includes any hardware, software, or combination of hardware and software used by the processing machine that allows a user to interact with the processing machine. A user interface may be in the form of a dialogue screen for example. A user interface may also include any of a mouse, touch screen, keyboard, keypad, voice reader, voice recognizer, dialogue screen, menu box, list, checkbox, toggle switch, a pushbutton or any other device that allows a user to receive information regarding the operation of the processing machine as it processes a set of instructions and/or provides the processing machine with information. Accordingly, the user interface is any device that provides communication between a user and a processing machine. The information provided by the user to the processing machine through the user interface may be in the form of a command, a selection of data, or some other input, for example.

[00132] As discussed above, a user interface is utilized by the processing machine that performs a set of instructions such that the processing machine processes data for a user. The user interface is typically used by the processing machine for interacting with a user either to convey information or receive information from the user. However, it should be appreciated that in accordance with some embodiments of the system and method of the invention, it is not necessary that a human user actually interact with a user interface used by the processing machine of the invention. Rather, it is also contemplated that the user interface of the invention might interact, i.e., convey and receive information, with another processing machine, rather than a human user. Accordingly, the other processing machine might be characterized as a user. Further, it is contemplated that a user interface utilized in the system and method of the invention may interact partially with another processing machine or processing machines, while also interacting partially with a human user.

[00133] It will be readily understood by those persons skilled in the art that the present invention is susceptible to broad utility and application. Many embodiments and adaptations of the present invention other than those herein described, as well as many variations, modifications and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and foregoing description thereof, without departing from the substance or scope of the invention.

[00134] Accordingly, while the present invention has been described here in detail in relation to its exemplary embodiments, it is to be understood that this disclosure is only illustrative and exemplary of the present invention and is made to provide an enabling disclosure of the invention. Accordingly, the

foregoing disclosure is not intended to be construed or to limit the present invention or otherwise to exclude any other such embodiments, adaptations, variations, modifications or equivalent arrangements.

CLAIMS

What is claimed is:

1. A payment system, comprising:

a financial institution comprising:

an acquirer portion;

a payment network portion; and

an issuer portion;

wherein the acquirer portion communicates with the issuer portion via the payment network portion;

a merchant having a merchant-acquirer relationship with the financial institution, the merchant in communication with the acquirer portion using a first network; and

an electronic device associated with a customer comprising at least one computer processor executing a payment application;

wherein:

the acquirer portion receives, from the merchant, at least one device credential and a payment credential that were received from the payment application in conjunction with a transaction, the acquirer portion further receiving transaction data for the transaction from the merchant;

the acquirer portion performs a first validation assessment on the transaction based on the transaction data;

the payment network portion receives, from the acquirer portion, the device credential, the payment credential, the transaction data, and the first validation assessment;

the payment network portion performs a second validation assessment on the transaction based on the transaction data;

the issuer portion receives, from the payment network portion, the device credential, the payment credentials, and transaction data from the acquirer portion; and

the issuer portion identifies and authenticates the customer based on the device credential, the payment credential, and at least one of the first validation assessment and the second validation assessment.

2. The system of claim 1, wherein at least one of the acquirer portion and the payment network portion is associated with a partner of the financial institution.

3. The system of claim 1, wherein the acquirer portion performs the first validation assessment on the transaction based on the transaction data and data retrieved from a third party data source.

4. The system of claim 3, wherein the third party data source comprises at least one of an address database, and an identity verification service.

5. The system of claim 3, wherein the third party data source comprises at least one of a fraud database, an IP address database, and a device information database.

6. The system of claim 1, wherein at least one of the first validation assessment and the second validation assessment comprises a risk score.

7. The system of claim 1, wherein the acquirer portion provides the first validation assessment to the payment network portion.

8. The system of claim 1, wherein the payment network portion performs the second validation assessment on the transaction based on the transaction data and data retrieved from a third party data source.

9. The system of claim 8, wherein the third party data source comprises at least one of an address database, and an identity verification service.

10. The system of claim 8, wherein the third party data source comprises at least one of a fraud database, an IP address database, and a device information database.

11. The system of claim 1, wherein the payment network portion provides the first validation assessment and the second validation assessment to the issuer portion.

12. The system of claim 1, wherein the payment network portion updates the first validation assessment with the second validation assessment, and provides the second validation assessment to the issuer portion.

13. The system of claim 1, wherein the issuer portion further performs a first validation assessment on the transaction based on the transaction data and data retrieved from a third party data source.

14. The system of claim 13, wherein the third party data source comprises at least one of an address database, and an identity verification service.

15. The system of claim 13, wherein the third party data source comprises at least one of a fraud database, an IP address database, and a device information database.

16. A method for authenticating a transaction, comprising:

at a financial institution comprising an acquirer portion, a payment network portion, and an issuer portion:

the acquirer portion receiving, from the merchant, at least one device credential and a payment credential that were received from the payment application in conjunction with a transaction, the acquirer portion further receiving transaction data for the transaction from the merchant;

the acquirer portion performing a first validation assessment on the transaction based on the transaction data and first data retrieved from a first data source;

the payment network receiving, from the acquirer portion, the device credential, the payment credential, the transaction data, and the first validation assessment;

the payment network portion performing a second validation assessment on the transaction based on the transaction data and second data retrieved from a second data source;

the issuer portion receiving, from the payment network portion, the device credential, the payment credentials, transaction data from the acquirer portion and the first validation assessment, and the second validation assessment; and

the issuer portion identifying and authenticating the customer based on the device credential, the payment credential, and at least one of the first validation assessment and the second validation assessment.

17. The method of claim 16, wherein the first data source and the second data source comprises at least one of the following: an address database, and an identity verification service.

18. The method of claim 16, wherein the first data source and the second data source comprises at least one of the following: a fraud database, an IP address database, and a device information database.

19. The method of claim 16, further comprising:

the acquirer portion denying the transaction based on the first validation assessment.

20. The method of claim 16, further comprising:

the payment network portion denying the transaction based on at least one of the first validation assessment and the second validation assessment.