

to be performed from a remote location, e.g., ordering a product over the internet while standing in line. However, as the number of remote transactions increase, so does the risk of financial fraud.

[0005] There is therefore a need in the art for a method and system for authenticating electronic transactions across multiple channels of commerce. There is a further need in the art for a method and system which operates in conjunction with a phone (e.g., a smart phone) for authenticating financial transactions whether initiated in person, over the internet via a stand alone terminal, via the placement of a call to the call center of a company, and/or via a transaction initiated with the very same phone. Finally, there is a need in the art for a method and system which allows a bank or other financial institution to reduce fees to merchants conducting remote electronic transactions when utilizing enhanced authentication techniques, and to limit/reverse the shifting of fraud liability to the merchant for such remote transactions.

SUMMARY

[0005a] According to an aspect, the present disclosure refers to a method for eliminating the need for an authentication pop-up window during an authentication process of an electronic transaction between a cardholder and a merchant over a payment network, the cardholder using a mobile device having an electronic wallet application that enables entry by the cardholder of authentication credentials within the electronic wallet application, and that is in communication with a merchant plug-in via an electronic wallet API, the method being carried-out by the merchant plug-in and comprising the steps of: receiving, by the merchant plug-in, a cardholder authentication request from the electronic wallet application via the electronic wallet API; sending, by the merchant plug-in, a payer authentication request to an access control server device; receiving, by the merchant plug-in, cardholder authenticating criteria in HTML markup from the access control server device and in response to the payer authentication request; extracting, by the merchant plug-in, the cardholder authenticating criteria from the HTML markup; translating, by the merchant plug-in, the cardholder authenticating criteria from the HTML markup into a protocol compatible with the electronic wallet API; sending, by the merchant plug-in, the

translated authenticating criteria to the electronic wallet application via the electronic wallet API; receiving, by the merchant plug-in, from the electronic wallet API, cardholder authentication credentials entered by the cardholder via an interface of the electronic wallet application; translating, by the merchant plug-in, the cardholder authentication credentials into a format for communication by the merchant plug-in to the access control server device using a HTTP POST command; and sending, by the merchant plug-in, the translated cardholder authentication credentials to the access control server device for validation.

[0005b] According to another aspect, the present disclosure refers to a system for authenticating an identity of a cardholder during authentication of an electronic transaction between a cardholder and a merchant over a payment network, the cardholder using a mobile device having an electronic wallet application that enables entry by the cardholder of authentication credentials via an interface of the electronic wallet application, the electronic wallet application being in communication with a merchant plug-in via an electronic wallet API, the system comprising: a directory server device including at least one processor configured for verification of enrollment of a payment card of the cardholder in an authentication program; an access control server device in communication with the directory server device, the access control server device including at least one processor containing cardholder authenticating criteria associated with the payment card; and a merchant plug-in in communication with the directory server device, the access control server device and the cardholder mobile device, wherein the merchant plug-in including at least one processor; wherein the merchant plug-in, in response to receipt of a cardholder authentication request from the electronic wallet application: sends a payer authentication request to the access control server device; receives cardholder authenticating criteria in HTML markup from the access control server device and in response to the payer authentication request; extracts the cardholder authenticating criteria from the HTML markup; translates the cardholder authenticating criteria from the HTML markup into a protocol compatible with the electronic wallet API; sends the translated authenticating criteria to the electronic wallet application via the electronic wallet API; receives, from the electronic wallet API, cardholder authentication credentials entered by the cardholder via an interface of the electronic

wallet application; translates the cardholder authentication credentials into a format for communication by the merchant plug-in to the access control server device using a HTTP POST command; and sends the translated cardholder authentication credentials to the access control server device for validation.

[0006] In an example, the present disclosure provides a mobile-phone centric electronic wallet providing the security of a virtual card terminal for online and off-line purchases. A wallet server (e.g., an application running in a cloud) and synchronized companion mobile and computer interface enables consumers to make purchases (which can include: retail, e-commerce, mobile, call center, etc) and use the mobile phone to authenticate against one of the authentication techniques tied to the chosen card (which can include: an offline PIN utilizing a secure memory chip, a MasterCard SecureCode PIN, and/or an online PIN such as an ATM PIN) where the necessary transaction and card specific authentication and processing method is directed by a central directory. The authentication process of the present disclosure allows participating banks to deem such transactions as more fully authenticated, which will allow them to lower the costs charged to merchants. The authentication process of the present disclosure will also limit/reverse the shifting of liability to the merchant since these more fully authenticated transactions will have less fraud associated therewith.

[0007] This system with its various authentication mechanisms will preferably utilize a central, hosted directory, which, when queried by the wallet application during a

internet browser session/window to communicate with the bank's authentication server. To facilitate this, the mobile phone will prompt the user for entry of the MSC password or PIN within the wallet-driven interface on the phone and communicate securely with the ACS (the bank's MSC authentication server). Successful authentication will be communicated from the wallet to the merchant's checkout system to be relayed to the Acquirer for approval. This last step preferably replaces the pre-existing MSC Merchant software, thus reducing the implementation requirements for the merchant. Finally, this interface will preferably allow setup and reset of a MSC password or PIN, again without the need to use a separate browser window or session with the bank's authentication server.

[0011] Thus, the system and method of the present disclosure provide an electronic wallet for authenticating transactions across multiple channels of commerce using the consumer's own mobile phone. The present invention provides better economics for merchants through lower fee structures, and limits/reduces the shifting of fraud liability to the merchant for remote transactions. The present invention is scalable in design to provide easy integration for merchants, and to avoid issuer by issuer sales and implementations. It is also easy to deploy directly to customers. Finally, the present invention will promote profitability by driving transaction volumes and revenues.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 is a schematical representation of a mobile phone-based payment/authentication system;

[0013] Figure 2 is a flow chart depicting the wallet application of the present invention being used in an e-commerce transaction originating via a computer, the wallet application cooperating with a secure element on the phone and an offline PIN;

[0014] Figure 3 is a flow chart depicting the wallet application of the present invention being used in an e-commerce transaction originating via computer, the wallet application cooperating with a SecureCode PIN for authentication;

What is claimed is:

1. A method for eliminating the need for an authentication pop-up window during an authentication process of an electronic transaction between a cardholder and a merchant over a payment network, the cardholder using a mobile device having an electronic wallet application that enables entry by the cardholder of authentication credentials within the electronic wallet application, and that is in communication with a merchant plug-in via an electronic wallet API, the method being carried-out by the merchant plug-in and comprising the steps of:

receiving, by the merchant plug-in, a cardholder authentication request from the electronic wallet application via the electronic wallet API;

sending, by the merchant plug-in, a payer authentication request to an access control server device;

receiving, by the merchant plug-in, cardholder authenticating criteria in HTML markup from the access control server device and in response to the payer authentication request;

extracting, by the merchant plug-in, the cardholder authenticating criteria from the HTML markup;

translating, by the merchant plug-in, the cardholder authenticating criteria from the HTML markup into a protocol compatible with the electronic wallet API;

sending, by the merchant plug-in, the translated authenticating criteria to the electronic wallet application via the electronic wallet API;

receiving, by the merchant plug-in, from the electronic wallet API, cardholder authentication credentials entered by the cardholder via an interface of the electronic wallet application;

translating, by the merchant plug-in, the cardholder authentication credentials into a format for communication by the merchant plug-in to the access control server device using a HTTP POST command; and

sending, by the merchant plug-in, the translated cardholder authentication credentials to the access control server device for validation.

2. The method according to claim 1, further comprising the steps of:

receiving, by the merchant plug-in, from the access control server device, an authentication response of validation of the authentication credentials of the cardholder; and

sending, by the merchant plug-in, the authentication response to the electronic wallet application via the electronic wallet API.

3. The method according to claim 1, further comprising the step of

receiving, by the merchant plug-in, an access server device identification from a directory server device.

4. A system for authenticating an identity of a cardholder during

authentication of an electronic transaction between a cardholder and a merchant over a payment network, the cardholder using a mobile device having an electronic wallet application that enables entry by the cardholder of authentication credentials via an

interface of the electronic wallet application, the electronic wallet application being in communication with a merchant plug-in via an electronic wallet API, the system comprising:

- a directory server device including at least one processor configured for verification of enrollment of a payment card of the cardholder in an authentication program;

- an access control server device in communication with the directory server device, the access control server device including at least one processor containing cardholder authenticating criteria associated with the payment card; and

- a merchant plug-in in communication with the directory server device, the access control server device and the cardholder mobile device, wherein the merchant plug-in including at least one processor;

wherein the merchant plug-in, in response to receipt of a cardholder authentication request from the electronic wallet application:

- sends a payer authentication request to the access control server device;

- receives cardholder authenticating criteria in HTML markup from the access control server device and in response to the payer authentication request;

- extracts the cardholder authenticating criteria from the HTML markup;

- translates the cardholder authenticating criteria from the HTML markup into a protocol compatible with the electronic wallet API;

- sends the translated authenticating criteria to the electronic wallet application via the electronic wallet API;

- receives, from the electronic wallet API, cardholder authentication credentials entered by the cardholder via an interface of the electronic wallet application;

translates the cardholder authentication credentials into a format for communication by the merchant plug-in to the access control server device using a HTTP POST command; and

sends the translated cardholder authentication credentials to the access control server device for validation.

5. The system according to claim 4, wherein the merchant plug-in further receives, from the access control server device, an authentication response of validation of the cardholder authentication credentials, and sends the authentication response to the electronic wallet application via the electronic wallet API.