interest of companies in this area. As a result, more and more transactions are likely 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 OF THE INVENTION

[0006] The present invention provides a mobile-phone centric electronic wallet providing the security of a virtual card terminal for online and off-line purchases.

[0006a] According to one aspect, there is provided a method for authenticating an electronic transaction with a merchant involving a cardholder using a payment card in said electronic transaction, responsive to the initiation, by a wallet application, of an authentication request for said electronic transaction, wherein said wallet application provides a wallet interface for said cardholder to conduct said electronic transaction, the method comprising the steps of: receiving authentication criteria by a merchant plug-in from an access control server device, wherein said authentication criteria are in HTML markup; extracting, by said merchant plug-in, said authentication criteria from said HTML markup; translating, by said merchant plug-in, said authentication criteria extracted from said HTML markup to a format compatible with said wallet application in accordance with an application programming interface protocol; forwarding, by said merchant plug-in, said translated authentication criteria to said wallet application for entry within said wallet interface by said cardholder of authentication credentials associated with said payment card; and returning, by said merchant plug-in, said authentication credentials entered by said cardholder to said access control server for validation.

[0006b] According to another aspect, there is provided a method of authenticating the identity of a cardholder during an electronic transaction involving a payment card utilizing 3D Secure protocols, comprising the steps of:

a) sending a verify enrollment request to a directory server;

b) identifying an access control server associated with said card;

c) sending a verify enrollment response from said access control server to said directory server, said verify enrollment response including a URL address of said access control server;

d) sending said verify enrollment response to a merchant plug-in associated with a merchant involved in said electronic transaction;

e) sending a payor authentication request from said merchant plug-in to said access control server;

f) sending a browser HTML markup from said access control server to said merchant plug-in;

g) extracting data from said HTML markup associated with said authentication of said card;

h) transmitting said extracted data to a wallet application associated with said cardholder for entry of authentication credentials;

i) sending said credentials from said wallet application through said merchant plug-in to said access control server;

j) sending said translated credentials from said merchant plug-in to said access control server for validation;

k) transmitting, upon validation of said credentials, a payer authentication response and a payment authorization from said access control server to said merchant plug-in;

l) transmitting said authorization from said merchant plug-in to said wallet application for subsequent transmission to said merchant.

[0006c] 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 invention 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 invention will also limit/reverse the shifting of liability to the merchant since these more fully authenticated transactions will have less fraud associated therewith.

[0006d] According to a further aspect, there is provided a system for authenticating the identity of a cardholder during an electronic transaction involving a payment card enrolled in an authentication program and a wallet application, the system comprising: a directory server configured to verify enrollment of said payment card in said authentication program; an access control server device in communication with said directory server device, said access control server device containing authentication credentials associated with said payment card; a merchant server device comprising a merchant plug-in stored thereon, wherein the merchant plug-in is in communication with said directory server and said access control server device, said merchant plug-in configured to perform operations comprising: receiving verification of enrollment of said payment card from said directory server device, receiving authentication criteria in HTML markup directly from said access control server device, translating said authentication criteria to a format compatible with said wallet application, forwarding said translated authentication criteria to said wallet application associated with said cardholder, and receiving authentication credentials entered by said cardholder through a wallet interface provided by said wallet application.

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