What is claimed is:

~~1. A method for removing pop-up windows during an authentication process involving a cardholder using a payment card in an electronic transaction, comprising the steps of:~~

~~sending authentication criteria directly from an access control sever to a merchant plug-in;~~

~~translating said authentication criteria to a language compatible with said merchant plug-in;~~

~~forwarding said authentication criteria through said merchant plug-in to a device operated by said cardholder for entry of said authentication credentials associated with said payment card in the absence of a pop-up window.~~

~~2. The method according to claim 1, wherein said authentication criteria are transmitted in HTML markup, and further comprising the step of translating said HTML markup into application programming interface protocol.~~

~~3~~1. ~~The method according to claim 2, further~~ 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 ~~step~~ 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 ~~through said merchant plug-in~~ entered by said cardholder to said access control server for validation ~~of said credentials~~.

42. The method according to claim ~~3~~1, ~~further comprising the step of~~ the returning step comprising translating, by said merchant plug-in, ~~the~~ said authentication credentials ~~received by said merchant plug-in from said application programming interface protocol~~ to said HTML markup before returning said authentication credentials to said access control server device for validation.

~~5~~3. The method according to claim 42, further comprising the step of ~~sending~~ receiving a validation response from said access control server device ~~to~~ by said merchant plug-in for subsequent transmission to a merchant participating in said electronic transaction in response to said access control server device receiving said authentication credentials for validation.

~~6~~4. 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.

~~7~~5. The method according to claim ~~6~~4, wherein said extracting step includes the further steps of interpreting said HTML markup.

~~8~~6 The method according to claim ~~6~~4, comprising the further step of translating said extracted data into application programming interface protocol.

~~9~~7. The method according to claim ~~6~~4, wherein said authentication credentials are sent from said wallet application to said merchant plug-in via application programming interface protocol.

~~10~~8. The method according to claim ~~6~~4, further comprising the step of displaying a request for said cardholder to enter authentication credentials into said cardholder's phone.

~~11~~9. The method according to claim ~~6~~4, further comprising the step of translating said credentials received from said wallet application into an appropriate format for receipt by said access control server.

~~12~~10. The method according to claim ~~11~~9, further comprising the step of translating said credentials from said application programming interface protocol to said HTML markup

~~13. A method of reducing fraudulent transactions associated with electronic commerce, comprising the steps of:~~

~~providing a wallet application for storage on a mobile phone;~~

~~entering of data associated with a payment card into said wallet application;~~

~~authenticating the identity of the cardholder associated with said payment card via an authentication process;~~

~~placing said wallet application into an authenticated state whereby the data associated with said payment card is stored in a secure manner within said wallet application; and~~

~~communicating said authenticated state of said wallet to a merchant during said electronic translation.~~

~~14. The method according to claim 13, comprising the further steps of:~~

~~analyzing said financial transaction to assign a risk factor to such transaction;~~

~~determining whether further authentication is required based upon said assigned risk factor.~~

~~15~~11. 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 ~~for verification of the~~ 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:~~; and~~

~~wherein said merchant plug-in is capable of~~ 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, ~~and is further capable of~~ translating said authentication criteria to a format compatible with said wallet application, ~~a language which allows transmission of said criteria through said merchant plug-in to an electronic device~~ 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.

~~16~~12. The system according to claim ~~15~~11, wherein said merchant plug-in ~~includes a translator for~~ operations further comprise extracting said authentication criteria ~~data~~ from said HTML markup ~~authentication criteria~~ received from said access control server device and translating said authentication criteria to said format in accordance with an application programming interface protocol.

~~17~~13. The system according to claim ~~15~~11, further comprising a mobile phone and a wallet application, said wallet application being stored on said phone and ~~adapted~~ configured to receive said authentication criteria from said merchant plug-in for ~~subsequent~~ entry ~~of~~ by said cardholder of said ~~validation~~ authentication credentials.

14. The method of claim 1, wherein said electronic transaction involving said payment card utilized 3D Secure protocols without a separate pop up window for entry of said authentication credentials.