Amended Claims

We claim:

1. A method *of improving the level of security by inserting* a dynamic CVC / CSC / CVV2 (herein referred to as dynamic validation security token) for e-commerce payments through payment gateway for credit and debit cards as a source of funds, said method comprising the steps of:

i. signing in to a merchant system of a merchant portal through a webpage or a mobile browser or an application merchant and initiating the online payment for the items purchased by entering card information of the user in the merchant system of the merchant portal webpage;

ii. signing in to an application interface of the issuing bank / card issuer by a secured network through a webpage or a mobile or desktop browser or an application, IVR, or a bot and providing authentication information to retrieve the card information of said user and the CVC / CSC / CVV2 value retrieved is a dynamic value, which is updated automatically post a configurable expiry period;

iii. entering the card information with a dynamic CVC / CSC / CVV2 using a standard checkout form for credit card / debit card payments requiring no customization in the existing checkout flows

iv. sending a request to a processing system of the online payment portal by the application system of online portal through a secured network channel;

v. generating a security token by the processing system of the online payment portal after authorization and verification processed by the online payment portal and communicating the same through a secured network channel to the application system of the issuing bank / card issuer;

vi. using CVC / CSC / CVV2 as a key to display a dynamic value for the user each time the user retrieves details of the card;

vii. entering the dynamic value of CVC / CSC / CVV2 (hereby referred to as a dynamic validation security token) in a Submit Form of the merchant system webpage as part of the existing credit card / debit card checkout form.;

viii. communicating an authorization request from the merchant system through a network payment infrastructure of Card Networks to the Issuing Bank of the card used to perform the transaction, which in turn will validate the dynamic validation security token sent as part of the standard ISO 8583 authorization request against the value of the token that was generated at the moment user requested for retrieving card details on the application portal;

ix. releasing online payment to the merchant system;

characterized in that the dynamic validation security token is generated following a request by the user by clicking on "get dynamic validation security token" displayed on the webpage of Issuing Bank.

2. The method as claimed in Claim 1, wherein the merchant system of the merchant portal comprises of a Merchant Shopping Cart's webpage where the items are selected by the user to be purchased; Checkout form's webpage allows to provide personal information of the user including virtual card information along with the CVV / CSC / CVV2 which in case of our invention is a Dynamic Validation Security Token; Submit Form's webpage allows the user to initiate a card not present transaction to make the online payment to the merchant portal for items purchased online.

3. The method as claimed in Claim 1, wherein the application system of the online portal comprises of webpage to enter authentication of the user; card information of the user as displayed on online payment portal webpage; and relevant configurations and API's to communicate and receive information with processing system of the online payment portal. The application system may be an application , a web page , an IVR service or even a bot.

4. The method as claimed in Claims 1 and 3, wherein the application system of the online payment portal loads the relevant configurations, initiates an API request to the processing system of the online payment portal through secured network channel with a request of the dynamic validation security token generation.

5. The method as claimed in Claims 1, 3 and 4, wherein the application system of the online payment portal receives dynamic validation security token generated by the processing system of Issuing bank / card issuer through secured network channel and displayed on the dashboard system of the Issuing Bank.

6. The method as claimed in Claim 1, wherein the processing system of the online payment portal comprises of Generate Token which receives API request from Application interface of Issuing Bank and generates dynamic validation security token; and time based counter initialized to validate security token to be sent to the application system of the Issuing Bank through secured network channel and to validate payment transaction authorized by the merchant system of merchant portal to the Issuing Bank / card issuer.

7. The method as claimed in Claims 1 and 6, wherein an open loop channel of the processing system of the online payment portal performs the following:

i. receives authorization request from the merchant system of the merchant portal through card network's payment infrastructure;

ii. sends the authorization request to the processor of Issuing Bank / card issuer;

iii. verifies the card information of the user;

iv. validates the dynamic validation security token generated sent to the application interface of the Issuing Bank / card issuer through secured network channel;

v. releases online payment to the merchant portal through secured network channel; thereby communicating the same through secure network channel to the merchant system of the merchant portal and displays in merchant portal webpage as the transaction successful.

8. The method as claimed in Claims 1 and 6, wherein processing system of Issuing Bank / card issuer performs the following: when Dynamic validation security token has expired / doesn't match the token (if any) associated with the card at that point in time; validation conditions are not met; authorization request is rejected; thereby communicating the same through secured network channel to the merchant system of the merchant portal and displays in the merchant portal webpage as transaction failure.