What is Payer Authentication?

Payer Authentication, also known as Verified by Visa (VbV) and MasterCard SecureCode™, are security protocols developed by Visa and MasterCard that allow consumers to shop online more securely. Visa and MasterCard also give back to eCommerce businesses that enable these programs by providing chargeback protection and lower interchange rates.

Simply put, Payer Authentication is validation that the online shopper is the cardholder. Merchants participating in the programs are helping to fight identity theft and consumers are thanking them by repeat shopping at these secure websites. Verified by Visa and MasterCard SecureCode are the #1 sought after fraud tool for the second year in a row according to industry Annual Online Fraud Reports.

How does Verified by Visa and MasterCard SecureCode work?

VbV and SecureCode enable cardholders to create a PIN (or "secure code") and assign it to their credit card. During checkout, the Customer is prompted to enter their PIN and the cardholder's identity can then be confirmed by their Card Issuing bank. The Card Issuer provides additional data elements to confirm the cardholder's identity. The data elements are amended to the authorization and settlement messages, thus providing the proper benefits of VbV/MCSC.

What are the benefits of Verified by Visa and MasterCard SecureCode?

With the programs, Visa and MasterCard aim to increase consumer confidence in online shopping and reduce fraud. To encourage 3-D Secure adoption, Visa and MasterCard offer significant merchant benefits including:

- Fraudulent chargeback protection (per the rules of Visa and MasterCard)
- Interchange discounts averaging 20 basis points
- Dramatic reduction in the fraud screening costs and manual review
- Higher AOV (Average Order Value); secure, confident Customers spend more
- Free and automatic platform upgrades
- Expand internationally, risk-free
- Consumer brand loyalty and security

Get in touch with us to learn more:

+(599 9) 844-0088 | Hello@cxpay.global | www.cxpay.global | FB: CXPay

What is the path of a Payer Authentication transaction?

Transactions from your system are routed to both the card associations, as well as the banking authentication networks via an Internet connection through the Payment Gateway. This authentication information can be accessed in real-time through the gateway's comprehensive reporting system, allowing you to easily identify authenticated transactions and recognize fraudulent ones. Enabling authentication does not interrupt the current authorization process.

1. During checkout, information about the cardholder is directed to the appropriate card association to check their program enrollment status.
2. If the cardholder is enrolled, an authentication form will be displayed by the cardholder's bank. This form will collect the password and the bank will validate it is correct.
3. Results of authentication are returned in less than one second. The results, new data elements, are proof that the merchant authenticated or attempted to authenticate the cardholder.
4. The transaction is then sent for authorization through typical processes and channels. The new data elements (ECI and CAVV) are also submitted during the authorization request, thus providing the appropriate benefits associated with VbV and MCSC.