MasterCard SecureCode

What is MasterCard SecureCode? MasterCard SecureCode is a security feature, available for merchants operating in a card-not-present environment that enables cardholders to authenticate themselves to their MasterCard card issuer through the use of a preselected personal code. MasterCard SecureCode protects e-commerce merchants from “cardholder unauthorized” or “cardholder not recognized” chargebacks.

How does MasterCard SecureCode work? When a cardholder is ready to check out at a participating merchant, the MasterCard SecureCode service takes the consumer through the following steps to ensure that he or she is authorized to use the card:

1. Once a consumer is taken to a participating merchant’s check-out page, he or she is prompted to enter their MasterCard credit or debit account number.
2. At this time a new window opens up and the card issuer requests the cardholder’s preselected SecureCode. After the SecureCode is submitted, the issuer will authenticate the transaction and confirm that the cardholder is authorized to make the purchase.
3. Once the cardholder’s identity is authenticated, the online transaction can be completed.

Card activation. Before a MasterCard SecureCode can be used to authenticate a cardholder, the card needs to be activated. There are several ways to do that:

1. MasterCard provides a step-by-step activation procedure on its website – **MasterCard SecureCode activation.**
2. MasterCard card issuers provide online activation on their websites and cardholders can contact their customer service representatives for details.
3. Merchants may also provide activation on their websites.

Benefits of using MasterCard SecureCode. Merchants benefit from MasterCard SecureCode in multiple ways:

- Participated merchants are protected from “cardholder unauthorized” chargebacks for fully compliant transactions. By limiting their chargeback exposure, merchants reduce processing costs.
- Participation in MasterCard SecureCode shows that you are serious about transaction security and promotes consumer confidence, which makes it more likely that customers will make a purchase on your website.
- Participating merchants can expand their geographic reach by selling to customers in countries where online debit cards are used more widely than credit cards. In addition to added protection against chargebacks for these customers, you will be able to process their Maestro debit transactions.
- MasterCard offers participating merchants free advertising on its consumer website.

Visa’s equivalent to MasterCard SecureCode is **Verified by Visa.**

2 Reasons to Use MasterCard SecureCode

The two biggest reasons to enroll in MasterCard SecureCode are:

1. The program protects you from “cardholder unauthorized” chargebacks for all fully compliant MasterCard and Maestro transactions. This is a great benefit, considering that more than 70 percent of all chargebacks resulting from e-commerce transactions are designated with either reason code 4837 (No Cardholder Authorization) or reason code 4863 (Cardholder Not Recognized), according to MasterCard.

2. Participation in SecureCode builds consumer trust. The SecureCode logo shows the visitors to your website that you are serious about fraud prevention.

As an added benefit, MasterCard allows merchants enrolled in its SecureCode program to place a free ad on its consumer website.

How to Enroll in SecureCode

MasterCard SecureCode is only available to your organization through your payment processor. To start using it, you need to:

1. Confirm with your processor that they support SecureCode. If they do not, MasterCard tells you to send an e-mail to securecodemerchant@mastercard.com, but the only real option you have is to look for a new processor.
2. Install the SecureCode plug-in on your website. This is a 3-D Secure-compliant application, which will facilitate the processing of SecureCode authentication requests. A list of approved vendors that provide SecureCode integration is available on MasterCard's website.
3. Test your newly-installed SecureCode application with MasterCard to make sure it is working properly.
4. Display the SecureCode logo on your website. This is mandatory, but you would be well-advised to let visitors to your website know that you support the authentication system anyway. After all, it is a trust symbol.
5. Communicate all transaction authentication results to the card issuer through the authorization process.

Once SecureCode is deployed on your website and it's been successfully tested, it is ready for use.

How SecureCode Works

The way merchants use MasterCard SecureCode has evolved over the years. When the program was first launched, the idea was to authenticate every single transaction involving a participating card. Lately, however, both merchants and issuers have begun adopting a more selective approach, using screening procedures to identify only the high-risk transactions, which are then authenticated, while the others are not.

Whatever your approach, the SecureCode authentication process goes through the following stages:

1. The customer enters her card information in the checkout form to complete a purchase.
2. A new window opens up, hosted on the card issuer's website, asking the cardholder to enter their pre-selected SecureCode.
3. The issuer verifies the code and confirms that the customer is authorized to use the card.
4. The customer is taken back to the merchant's website and the transaction is completed.

SecureCode authentication can only be performed if the card is registered with the program. Consumers can do that on their card issuer's website, but registration can be initiated on your website as well.

The Takeaway

The best thing about SecureCode is that it protects you against the type of chargebacks you are most likely to suffer from. There is really no good reason not to take advantage of that, especially considering that you can design your system in a way that allows low-risk transactions (for example transactions placed by repeat customers, for low purchase amounts, etc.), which don't need authentication, to be processed straight through, bypassing SecureCode.

Be advised that a SecureCode authentication is not a substitute for an authorization approval. All card-not-present transactions, regardless of the amount, must be authorized, whether or not they've been SecureCode-authenticated.

Verified by Visa

Verified by Visa (VbV) is a card authentication service for Visa credit and debit cards. Visa developed VbV as an additional security layer to help protect merchants that accept cards over the internet.

Based on the 3-D Secure protocol, VbV benefits participating e-commerce merchants in the following ways:

- Reduces merchant liability for fraud resulting from accepting unauthorized Visa cards.
- Minimizes chargebacks. Merchants who use VbV are protected from fraud-related chargebacks on all personal Visa cards — credit or debit — whether or not the issuer or cardholder is participating in VbV, with limited exceptions.
- Provides a safer place for consumers to shop.
- In many cases using VbV lowers participating merchants' Visa credit card processing costs. Depending on the structure of your pricing agreement, you could qualify for lower discount fee on internet transactions that use VbV. To take advantage, you should require that your pricing is based on the interchange-plus model.

Merchants offering VbV to their customers must install a software module called a Merchant Plug-In (MPI), on their hosting server. The plug-in is easily installed and is compatible with all major e-commerce systems.

To use Verified by Visa, cardholders must first activate their cards. The activation can be done in one of several ways:

- Card issuers usually provide an online activation site and have integrated Verified by Visa activation in the card issuer's online banking site. Cardholders should have an easy access to the activation site or they can ask the card issuer for assistance.
- Visa, card issuers, and participating merchants may display "Activation Anytime" banners or buttons that enable cardholders to activate their Visa card by clicking on the banner or button and following the prompts.
- Cardholders may also register with VbV during shopping, on the merchant's website.

Once VbV is activated, a Visa credit or debit card is automatically recognized when used for purchases at participating e-commerce websites. The verification process goes through the following stages:

1. When ready to finalize a purchase, a Visa cardholder clicks "Complete Order" or an equivalent option at the checkout. Software previously installed on the merchant website's server recognizes a VbV eligible Visa card account and initiates the next steps of the process.
2. At this time a Verified by Visa page appears in a new browser showing the merchant website's URL. If the cardholder has previously activated the card with Verified by Visa, he or she will be asked to enter the password that they created during the activation process. There is an option for retrieving forgotten passwords as well. If the cardholder has not previously activated the card, he or she may be asked to do so now. If the card issuer does not participate in Verified by Visa, no cardholder interaction takes place. However, the merchant still qualifies for certain fraud liability protection. The merchant receives an "Attempted Authentication" response with authentication data to be submitted with the authorization request as proof of qualification for chargeback protection for the transaction.
3. The card issuer verifies its cardholder's identity for cards that have been activated and sends a response to the merchant with the authentication result. If the authentication fails, the merchant should request an alternative payment method.
4. When the Verified by Visa verification process is complete, the merchant includes the authentication data received from the card issuer with the transaction authorization request.

Merchants participating in VbV get additional chargeback protection:

- If the cardholder is successfully authenticated, the merchant is protected from fraud-related chargebacks, and can proceed with authorization using Electronic Commerce Indicator (ECI) of “5.”
- If the card issuer or cardholder is not participating in Verified by Visa, the merchant is protected from fraud-related chargebacks, and can proceed with authorization using ECI of “6.”
- If the card issuer is unable to authenticate, the merchant is not protected from fraud-related chargebacks, but can still proceed with authorization using ECI of “7.” This condition occurs if the card type is not supported within VbV or if the cardholder experiences technical problems.