MASTERCARD® SECURECODE™
ISSUER BEST PRACTICES

Minimize Abandonment in Authorization and Maximize Fraud Reduction with an Optimal Implementation of SecureCode
The explosive growth of e-commerce has given rise to security concerns among banks and cardholders alike. To support the increasing need for payment guarantee and cardholder authentication, MasterCard’s global e-commerce solution SecureCode enables cardholders to authenticate themselves to their issuers through the use of a unique personal code.

This document details the best practices of implementing MasterCard SecureCode and how to enhance transaction security, enabling fully guaranteed transactions, and building confidence in virtual transactions. For detailed information on technical deployment of MasterCard SecureCode, refer to the SecureCode Member Enrollment and Implementation Guide and the MasterCard SecureCode Cardholder Interface on MasterCard Online.

Based on research and validation across the payments industry, there are four key areas of best practice when implementing an authentication system:

- **Registration**
- **Authentication**
- **Activation**
- **Authorization**

**Registration**

Increasing usage of any new security program is a balancing act between gaining maximum adoption whilst preventing fraudulent registration. Registration is important to any authentication solution and requires the cardholder to opt into the service.

To reduce cardholder abandonment at the point of registration, MasterCard recommends that issuers take the following steps:

- Communicate repeatedly to cardholders at least three months prior to launch and through multiple channels to ensure that the launch of the program is not a surprise and maximizes enrollment.
- An issuer’s website must provide easily accessible information about the SecureCode service and authentication options supported by the issuer.
- An issuer should encourage voluntary registration through its Internet banking and other websites.
- 3-D Secure screens should be designed to minimize cardholder errors and provide:
  - Drop-down fields for numerical inputs from the cardholder or show format examples (e.g. drop-down fields for month and year in birth dates or card expiration dates)
  - Sufficient spacing for an authentication element, if applicable, for input boxes (e.g. instead of providing a single-input box for telephone number entry, split into three input boxes)
  - Clear images and help text to explain Card Validation Code 2 (CVC2) values if used as an authentication element
  - Brief help text via Dynamic HTML technology instead of via pop-up, since most pop-up blockers restrict the cardholder from obtaining information via pop-ups
  - Separate input boxes for name inputs from the cardholder such as prefix, first name, middle name, last name and suffix
• Limit cardholder questions to no more than four to fit Activation During Shopping screen.

• Questions can include AVS and/or CVC2 but must not be limited to these:
  - Two registration questions must be related to non-card data
  - Questions easily answered by the legitimate cardholder but not by a fraudster
  - Questions based on previous data (e.g. select postcode/zipcode of previous address from the following six in a drop-down list)

• Consider using “Knowledge-based Questions” (may require interface between issuer Access Control Server (ACS) and external country specific solutions).
  - Allow questions based on non-traditional financial questions.
  - Avoid questions such as cardholder name, mother’s maiden name, which are strongly associated with spelling/special character failures.
  - Partial answers to sensitive questions are better (e.g. last four digits of National ID Number/Social Security Number, rather than entire number).

• Carefully match questions for single Primary Account Numbers (PANs) that have multiple cardholders, with answers that apply solely to primary cardholder.

• Issuer should allow three opt-outs from registration before enrolling and that enrollment should then be mandatory.
  - Issuer may use risk-based decisions regarding when to mandate registration, and this mandate can be on the first high-risk transaction (if required).

• Consider registering all cardholders with a static password through a “PIN” mailing with details of how the cardholder should use the password and where they can go to change the password.
  - Note that a disadvantage to this solution is that existing e-commerce shoppers would not be able to transact until they received the mailing. It’s a useful tool when used for cardholders not currently shopping as it could prevent fraudulent use of the account.

Authentication solutions which rely on hardware or replacement cards being supplied to a cardholder for all future transactions, such as Display Cards Chip Authentication, do not require registration.
Activation During Shopping (ADS)

ADS is a useful tool for issuers as it allows the enrollment of the cardholder at the point of purchase of a SecureCode merchant. Instead of an authentication window appearing in the frame on the merchant site, the issuer can send a special message requesting that the cardholder confirm his or her identity to complete the purchase and enroll in the issuer’s SecureCode program.

Given the high profile in the media surrounding phishing and other private data attacks, it is important to avoid unnecessary cardholder concern and abandonment of transactions. The best practice surrounding registration is also relevant to ADS but issuers should pay particular attention to the following:

- Communicate your ADS program in mailings, website, etc., to your customers and explain what will happen during a transaction at a SecureCode merchant before launching ADS as an enrollment program.
- Consider partnering with key merchants where your cardholders shop to get the message across by using banner ads, links and discount offers. This can build cardholder confidence, drive transactions, and increase enrollment, through these merchant websites.
  - Some merchants mail their customers the benefits in advance of going live which can be a joint messaging opportunity.
- MasterCard requires merchants for SecureCode to provide a “learn more” button on their web pages that link to registration so that a cardholder can register before shopping.
- MasterCard requests merchants to also assist in messaging through screen designs at point of authentication.
- Issuers should consider using a risk-based system that would require a cardholder to enroll if the transaction meets set criteria with no opt out. Issuers should discuss this system with the provider that supplies their ACS.
- Provide clear links for help, privacy policy information and legal terms on one of two screens for ADS.
- Ensure that cardholders have time to read the telephone number to call on the Transaction Failed screen.

Authentication

MasterCard SecureCode offers a number of authentication options that allows issuers considerable choice in both static and one-time password solutions to further enhance online shopping security.

There has been an increasing desire to move away from static solutions. MasterCard already supports a range of options, including the generation of dynamic codes based on chip solutions either embedded in a card (known as display cards), the use of card readers, mobile applications and SMS of one-time codes.

MasterCard has also partnered with providers to examine risk-based authentication solutions that allow issuers to decide both when they will authenticate a transaction and how the authentication occurs. This solution is already offered by MasterCard as part of the hosted solution for issuers.
In choosing the right solution(s), issuers need to look at the risk, reward and consumer experience to gain a good balance. Each solution has differing costs for deploying the solution and the technology itself.

Below are some best practices related to the authentication event itself:

- 3-D Secure screens and redirected Transaction URL must convey authenticity.
  - For 3-D Secure authentication screens:
    - Authentication screens should have clear messaging regarding 3-D Secure on both ADS and enrolled cardholder authentication.
    - Issuer contact number must be clearly visible to cardholder on the authentication screen or via DHTML.
    - Issuer logo must be regularly updated as per changes in graphics at the issuer’s parent site.
    - 3-D Secure authentication screen must be 390 pixels x 400 pixels in size (including dual-language ACS screens).
  - For the issuer’s ACS visible security for cardholders:
    - ACS can have Extended Validation Certificates (special type of X.509 certificate) which require more extensive investigation of the requesting entity by the certificate authority before being issued. These certificates show up as a green-colored URL in the latest browsers but does not impact older browsers.
    - ACS URL should be using its own domain name rather than the vendor’s (e.g. cardsecurity.abcbank.com).
• Consider using risk-based systems that build a profile of the PC being used by many banks for their existing Internet banking solutions.

• It is critical to provide the cardholder with a way to reset a forgotten password when shopping, which occurs at least 30% of the time. However, an issuer should monitor for frequency of change etc, as this could be an indication that the account may have been compromised.

• Rather than allowing a cardholder to lock his or her account through ‘Incorrect password used’, consider offering to reset the password on the cardholder’s last attempt before lockout. Again, this feature needs careful administration.

Authorization

MasterCard SecureCode is a fraud management tool that should be used within an authorization strategy and not a replacement for a sound authorization strategy. The type of authentication used may influence the decision on when to authorize a transaction. While an authorization strategy will be driven by an issuer’s view of risk, cardholder impact, authentication strategies, etc., this section suggests some points to consider as an issuer develops the plan.

When an authorization is presented to an issuer it is flagged in accordance with the requirements of the program as detailed in the MasterCard Authorization System Manual and the SecureCode Member Enrollment and Implementation Guide. One key field that indicates the security, and where liability rests, is known as the Security Level Indicator (SLI) which can have the following values:

<table>
<thead>
<tr>
<th>SLI 0</th>
<th>The merchant is not participating in the SecureCode program or does not claim SecureCode protection on this transaction. The merchant has liability so an issuer could authorize subject to funds being available knowing that the issuer retains the right of chargeback.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLI 1</td>
<td>Merchant only—The merchant has participated in the SecureCode program but either the issuer or cardholder has not participated. With some exceptions this will mean that liability will rest with the issuer. Full details are contained within the SecureCode Member Enrollment and Implementation Guide.</td>
</tr>
<tr>
<td>SLI 2</td>
<td>The cardholder authenticated the transaction and liability remains with the issuer.</td>
</tr>
<tr>
<td>SLI 3</td>
<td>The merchant participated in the Maestro Advance Registration Program (MARP)—liability rests with the merchant.</td>
</tr>
</tbody>
</table>

The changing liability demonstrated by these values should be included in any authorization decision. The decisions also need to be reviewed as a program matures and cardholder adoption is high, as selectively declining merchant-only transactions should be considered where issuer expectation is that all transactions should be fully authenticated.

Please note that an issuer strategy of declining merchant-only traffic when no program is available to cardholders is not permitted under the selective authorization rule.
Further Information

Further details surrounding the MasterCard SecureCode program can be obtained from various guides available in the Member Publications tool on MasterCard OnLine including:

- SecureCode Member Enrollment and Implementation Guide
- MasterCard OnLine Authentication Service Guide
- SecureCode Cardholder Interface Requirements Guide
- SecureCode Merchant Implementation Guide

As announced in Global Security Bulletin No. 2, February 16, 2010, the MasterCard SecureCode Education Program was developed in an effort to increase awareness and promote adoption of MasterCard SecureCode by participants in the payment value chain.

The MasterCard SecureCode Education Program offers a complimentary series of Webinars to customers and merchants. Issuers, acquirers, and merchants can access these Webinars at: [www.webcasts.com/securecode](http://www.webcasts.com/securecode)