3D Secure Reference Guide

This reference guide is for SHAZAM financial institutions that issue MasterCard® or Visa® payment cards. It describes how to manage the MasterCard SecureCode® or Verified by Visa® program.

What is 3D Secure?

3D Secure is a technology that helps protect card accounts against unauthorized Internet transactions by using identity information established between individual cardholders and your financial institution. Once a cardholder activates the service, the card cannot be used at a participating Internet merchant without authentication by an authorized user of the account.

MasterCard and Visa each have their own 3D Secure program, MasterCard SecureCode and Verified by Visa[®] (VbV). SHAZAM hosts both services on the same platform. The overall objective of SecureCode and VbV is to improve the security of payment transactions in the electronic commerce environment. They are designed to improve both cardholder and merchant confidence in Internet purchases, as well as reduce disputes and fraudulent activity related to the use of MasterCard and Visa payment cards. To realize the full benefits of 3D Secure technology, card issuers, cardholders, and merchants must all participate in the authentication process.

When a cardholder uses his or her card for an Internet purchase, a pop-up window displays his or her basic cardholder information and a request to enter a password in much the same way the cardholder enters a PIN during a face-to-face transaction. The cardholder enters the authentication password and clicks **Submit**. An access-control server authenticates the information and submits the transaction to the issuer's processor for authorization.

Liability

Both MasterCard and Visa have a liability shift from the acquirer to the issuer if the merchant is enrolled in SecureCode or VbV. These apply to both consumer and business debit cards. The details are explained below.

| Enrolled?			
Merchant	**Card Issuer**	**Cardholder**	**Liability**
No	NA	NA	Liability remains with the merchant, whether or not the card issuer/cardholder is enrolled.
Yes	No	No	If an enrolled merchant attempts to authenticate the cardholder, liability shifts from the merchant to the MasterCard or Visa card issuer. The issuer and the cardholder must enroll in VbV/SecureCode to participate.
Yes	Yes	No	An enrolled merchant will not allow the transaction to proceed until the cardholder has activated SecureCode or VbV. **Note:** If a Visa card issuer allows its cardholders to bypass enrollment a certain number of times before forcing them to enroll in VbV, the liability for those transactions lies with the issuer. This situation does not apply to MasterCard issuers because their cardholders must enroll the first time they encounter a participating merchant.
Yes	Yes	Yes	An enrolled merchant processes the transaction for authorization and settlement. If the cardholder activation is denied or not sent, the card issuer may have chargeback or pre-compliance rights. Refer to the Exception Item Processing Manual for further information.

Cardholder Activation

There are two options available for cardholder activation, described below. In each case, a cardholder is asked to create a user name and password to log in each time they visit an enrolled merchant.

Activation During Shopping (ADS)

ADS offers your cardholder the opportunity to activate either SecureCode or VbV while shopping. ADS enrollment begins when the cardholder initiates an Internet purchase:

1. The cardholder clicks **Checkout** or performs an equivalent action.
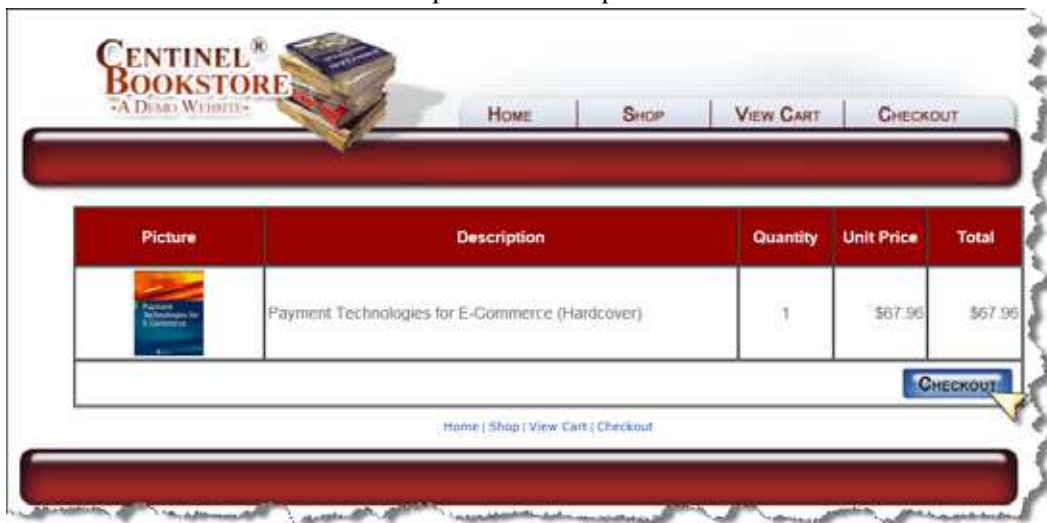
2.   The cardholder is asked to enter his or her card number and the payment card is identified as an eligible card.

3.   The cardholder is presented with an activation page in a separate, secure session.

4.   The cardholder enters the information requested and a quick identity verification process takes place.

5.   The cardholder's identity is verified.

6. The cardholder is asked to establish a user ID, password, and a personal message.

   Password Requirements
   - 8–10 characters
   - At least one upper case letter
   - At least one numeric character
   - At least one special character

7. Once the system accepts the cardholder's user ID, password, and personal message, the cardholder is returned to the merchant site and the transaction is completed.

During all subsequent Internet transactions, the cardholder is presented with the a password entry page. The cardholder enters his or her password correctly to complete transactions with the registered card.

Enrolling Cards with Multiple Cardholders. ADS supports cards with multiple cardholders, but only the first cardholder who attempts to enroll using the card number will have the option of enrolling using ADS. Each additional cardholder will need to enroll through the self-enrollment website, accessible through his or her financial institution's website.

Activation at Your Financial Institution's Registration Website

Your cardholders can visit your financial institution's enrollment website to activate SecureCode or VbV. The registration process verifies the cardholder's identity and creates a password and personal message. When the cardholder shops at a participating Internet merchant, he or she is presented with the password entry page and must enter his or her password correctly to complete the transaction with that card.

Your cardholder will follow the steps below to activate his or her 3D Secure account using your financial institution's registration website:

1. The cardholder clicks on your financial institution's enrollment website URL and then clicks **Register Card**.
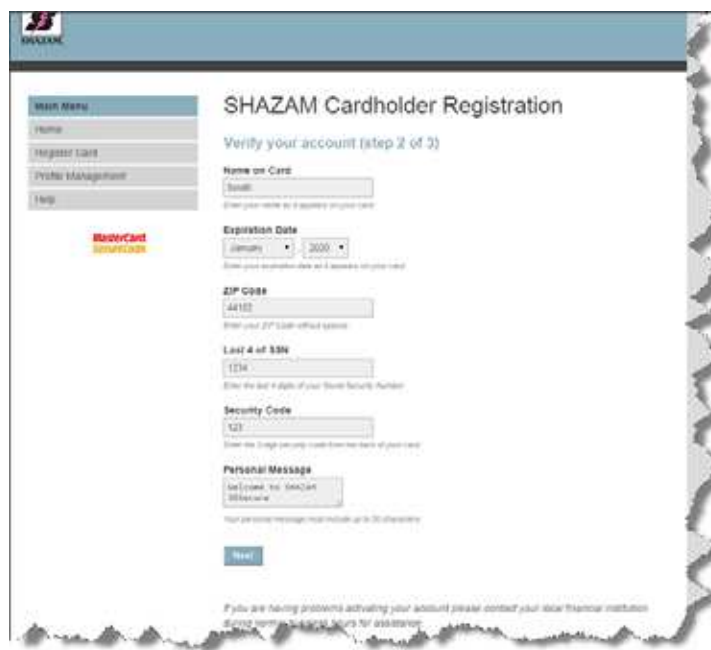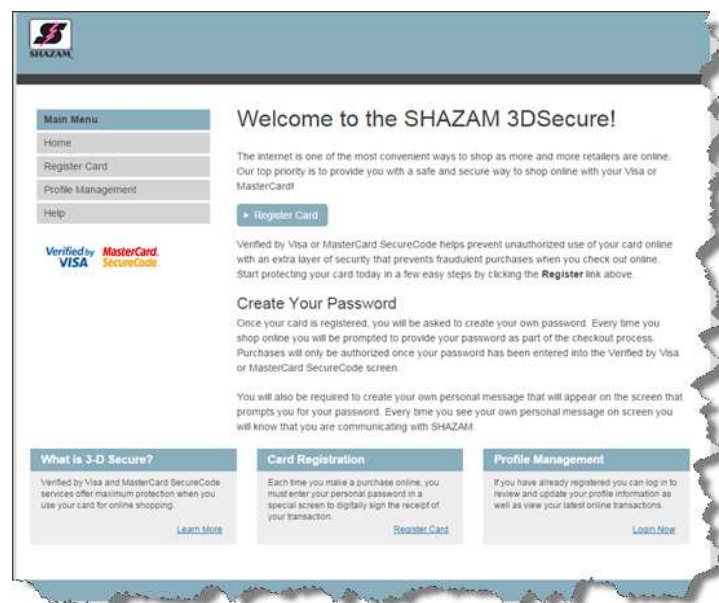
2. The cardholder enters his or her 16-digit card number and then clicks **Activate**.

3. The cardholder completes the activation form and then clicks **Next**.

4. The cardholder enters a user name and password, accepts the terms and conditions, and clicks **Next**.

Password Requirements

The password must meet the following requirements:

- 8–10 characters
- At least one upper case letter
- At least one numeric character
- At least one special character

5. Cardholder activation is complete!

Troubleshooting

Activation/Authentication

During the activation process (ADS or Manual), the authentication platform is integrated with the processing system and the following information is verified.

- First and last name
- ZIP code
- Expiration date
- CVV2/CVC2 Code
- Last 4 of SSN

If any of the above information is incorrect, it will show in *SHAZAM Access > Transactions* and on the SHAZAM Risk Management (FD020-R) Report.

SHAZAM Access

All information provided by the cardholder, with the exception of the CVV2/CVC2, will appear in SHAZAM Access. You can compare what the cardholder entered with the card information on file with SHAZAM.

Follow these steps to search for VbV or SecureCode activation attempts. The detail provided will show you valid attempts as well as failed attempts, including the reason the activation attempt failed.

1. Under the Transactions tab, select the **VbV/SecureCode** button.

2. Complete the fields as instructed on the screen.

3. Click **Search**.

4. Click a record to view more detail for that activation attempt.

Note: Successful activations are valid. Possible reasons for activation failure include:

- CVV2
- Cardholder Name
- ZIP Code
- Expiration Date
- Last 4 SSN

SHAZAM Risk Management Report (FD020-R)

This report provides a summary of a prior day's (midnight to midnight) activation attempts. The following values are checked during validation:

- CVV2
- Cardholder Name
- ZIP Code
- Expiration Date
- Last 4 SSN

The validation success or a failure reason will be provided in this report under the *Blocked Reason* column.

Transactions

The following SHAZAM Action, Response, Reversal, and Completion Codes indicate a denied SecureCode transaction:

- Action Code = 119 (Transaction not allowed for cardholder)
- Response and Completion Code =

  - 57 MV — Indicates cardholder not authenticated in MasterCard SecureCode.
  - 57 MC — Indicates BIN and/or cardholder not enrolled in MasterCard Secure Code.
  - 57 CV — Cardholder authentication verification value (CAVV) failed (this appears for failed VbV activations)

The Action, Response, Reversal and Completion Codes display in:

- SHAZAM Access Transaction Detail
- Cardholder Exception Journal (SSR100) report
- Cardholder Institution Activity (SSR110) report

MasterCard SecureCode

Refer to the Universal Cardholder Authentication Field (UCAF) Indicator on *SHAZAM Access > Transaction Detail > MasterCard* to determine the status of SecureCode for a particular transaction. This is useful when determining chargeback rights (see the [Liability](#) section). Valid values include:

UCAF Value	Definition	Description
0	Merchant does not participate in SecureCode.	Transaction continues processing.
1	Cardholder is not enrolled in SecureCode.	• MasterCard business cards transactions will be rejected. • MasterCard HSA card transactions will continue processing. • Address Verification Only transactions will continue processing. • Account Status Inquiry transactions will continue processing.
2	The merchant and the cardholder participate in Securecode.	If UCAF data does not start with a "j", the transaction is rejected.
3	Merchant does not participate in SecureCode	Transaction continues processing.

Verified by Visa

Refer to the Mail/Phone Auth Indicator on *SHAZAM Access > Transaction Detail > Visa* to determine if an activated cardholder performed a transaction at a participating VbV merchant. This is useful when determining chargeback rights (see the [Liability](#) section). Valid values include:

Value	Definition	Chargeback Rights for Issuer
05	Secure e-commerce transaction at a Verified by Visa merchant.	No
06	Unauthenticated security transaction at a Verified by Visa merchant.	Yes

How to Market VbV/SecureCode to Your Cardholders

SHAZAM offers the following options for each card brand to educate your cardholders about the protection these services offer against unauthorized transactions.

MasterCard SecureCode

SHAZAM offers two free statement inserts through the SHAZAM Power Marketing Program.

Verified by Visa

Visa has provided the following sample verbiage for you to use to educate your cardholders.

Sample 1— Cardholder Memo

From: [Your Financial Institution Name]
To: Sample A. Sample
Subject: Shop Online with Greater Security

Expect something new the next time you shop online.

The next time you use your Visa® card when you shop online, you'll be asked to activate Verified by Visa. That's because your card is now equipped with Verified by Visa—it password protects your card for free.

It's safe and easy to activate while you shop.

When you shop at a participating online store, enter the information requested to activate your card in order to complete your transaction. It only takes a moment, and then your card will have password protection whenever you shop online.

It's now even safer to shop online.

Once you activate your card, Verified by Visa protects you at every participating store- so only you can use your card.

Shop online with greater security at participating stores listed at www.visa.com/shopverified.

Sample 2— Newsletter or Newspaper Copy

Verified by Visa—Activation During Shopping

Headline:
What to expect the next time you shop online.

Sub-Headline:
Shop online and activate Verified by Visa.

Body Copy:
Your Visa card is now protected by Verified by Visa - it password protects your card for free. The next time you shop at participating online stores, enter the information requested to activate your card in order to complete the transaction. It only takes a moment, and then your card will have password protection whenever you shop online.

Shop online with greater security at participating stores listed at www.visa.com/shopverified.

Sample 3— Statement Message

Activation During Shopping—VbV

Your Visa card is now protected by Verified by Visa - it password protects your card for free. The next time you shop at participating online stores, enter the information requested to activate your card in order to complete the transaction. Your card will then have password protection whenever you shop online at participating stores listed at www.visa.com/shopverified.

Change Log

Below is a summary of changes that have been made to this document.

Revision History

Date	Action	Section and Description of Change
April 13, 2015	New	New document. This replaces both the MasterCard SecureCode Reference Guide and the Verified by Visa Reference Guide.