Address Verification System (AVS) Checking

The Address Verification System (AVS) is a service provided by credit card Issuers intended to authenticate the Purchaser (Customer) as the authorized cardholder. AVS checking is performed by matching the numerical address information provided at the time of a purchase (such as in a shipping address field) with that numerical address information held on record for the authorized cardholder. This information is included with the order and transmitted to the Skipjack Transaction Network and the Issuers networks for scrutiny.

It is important to understand that AVS checking only compares the *numeric* portion of the cardholder's street address and the 5 or 9-digit zip code/postal code to that held on record for the cardholder. AVS return codes are returned based on how well this data matches and the level of matching required can be configured for each Merchant Account. By default, AVS filtering is disabled within Skipjack Transaction Network.

AVS **does not** examine the text portion of the address, such as street names or city names. As a result, AVS is a basic method of fraud prevention only and helps to prevent the use of counterfeit (computer generated) credit card numbers not associated with a legitimate cardholder.

AVS use is not required in all transactions by the card Issuers and Processors. However, submitting AVS data with every transaction can help ensure that Merchants receive improved transaction rates from Processors and Issuers. *For these reasons the use of AVS checking is highly recommended by Skipjack.*

AVS Filtering within the Skipjack Transaction Network

The AVS verification is performed by the credit card Issuer and an AVS response code and message are returned to the Processor and to the Skipjack Transaction Network. The values of this AVS match are carried in the **szAVSResponseCode** and **szAVSResponseMessage** return variables. These return variables indicate the level of matching obtained in the AVS check.

The Skipjack Transaction Network permits AVS filtering options to be set on the Merchant Account. The levels of AVS matching configured are independent of and in addition to the AVS checking done by the Issuer. The Skipjack Transaction Network AVS filters are applied *after* the Issuer performs its AVS checking.

If the Skipjack AVS filtering option is enabled and configured to require a high level of matching for transactions, AVS filtering is performed on each transaction on a particular Merchant Account. **The default setting for this feature is that <u>no</u> AVS filtering will be applied.**

The AVS filters can also be configured to handle Domestic and International transactions differently.

See Also

- For more information about how to configure using the Merchant Interface, see the AVS section in the *Skipjack Merchant Services Guide*.

For more information about the development considerations when configuring International and Domestic AVS handling see "

- **AVS Code Handling for International and Domestic Transactions**" section.

Development Notes for AVS and AVS Filtering

Consider the following when applying AVS and AVS filtering in your application development.

- AVS is not supported for Declined transactions. No further processing is done on transactions Declined by the Issuing Bank.

- When Skipjack AVS is configured to require a high AVS matching threshold, the transaction *can* be Declined by the Skipjack Transaction Network despite the transaction being Approved by the credit card Issuer. The Issuer never declines based on AVS values, they simply pass this information through their networks to Skipjack Financial Services.

- If AVS filtering leads to a transaction Decline, the available credit (headroom) on the card is decreased by the transaction amount submitted. For subsequent transactions the headroom on the card is decreased by this transaction amount for a period of 7 days (normally).

  This creates a problem when the headroom is nearing its limit on the card and the transaction is resubmitted for a second Authorization attempt. This can lead to another Decline with further decreases in headroom being made on the card.

  In these instances, the Merchant must call the card Issuer to reverse the reserved amount(s) from the transaction(s) that were previously Declined. The Merchant can then resubmit the transaction. The Merchant can then receive a transaction Approval, assuming the AVS threshold was sufficiently lowered from the original settings or the correct address information is sent. The presence of an **AUTHCODE** value when the **szIsApproved=0** is the true indicator of the status of the transaction in these cases.

AVS Codes By Card Type

Return Code	Summary	AVS Response Code Description	Visa	MC	AMEX	DISCOVER
X	Match	Street address and 9-digit ZIP code both match		X		
Y	Match	Street address and 5-digit ZIP code both match.	X	X	X	X
A	Partial Match	Street address matches, but both 5-digit and 9-digit ZIP Code do not match.	X	X	X	X
W	Partial Match	Street address does not match, but 9-digit ZIP code matches.		X		X
Z	Partial Match	Street address does not match, but 5-digit ZIP code matches.	X	X	X	X
N	No Match	Street address, 5-digit ZIP code, and 9-digit ZIP code all do not match.	X	X	X	X
U	System Unavailable	Address information unavailable. Returned if non-US. AVS is not available or if the AVS in a U.S. bank is not functioning properly.	X	X	X	X
R	System Unavailable	Retry - Issuer's System Unavailable or Timed Out.	X	X	X	
E	Invalid	AVS data is invalid.	X			
S	Not Supported	U.S. issuing bank does not support AVS.	X	X	X	
Note: By default, the Skipjack AVS filtering configuration is set to NOT DECLINE any transactions based on AVS settings. Increasing the filter configuration matching requirements can lead to more transactions being declined.						

AVS Response Codes for International and Domestic Credit Cards

When sending a transaction with AVS checking required the Issuing Bank will return one of the following AVS response codes. The table below breaks down the responses returned by credit card type.

Code	Summary	Description
D	Match	Street Address and Postal Code match for International Transaction.
M	Match	Street Address and Postal Code match for International Transaction.
B	Partial Match	Street Address Match for International Transaction. Postal Code not verified due to incompatible formats.
P	Partial Match	Postal Codes match for International Transaction but street address not verified due to incompatible formats.
C	No Match	Street Address and Postal Code not verified for International Transaction due to incompatible formats.
I	No Match	Address Information not verified by International issuer.
O	Not Supported	Non-US. Issuer does not participate.

AVS Code Handling for International and Domestic Transactions

The Merchant Interface allows the configuration of different matching criteria for AVS checks performed on Domestic and International transactions. In this context, Domestic is always defined as from the country where the Originating Bank/Issuer is located.

This means that for Originating Banks (Card Issuers) based in the United States of America (USA), Domestic will always means USA-based transactions and International will always be any transaction to cardholders with Issuers located outside the USA.

Please note that for Canadian Merchant Accounts handling Canadian transactions some Merchants might see different handling of the AVS codes than is described here.

Use of Canadian Postal Codes in AVS Checks

For Canadian Merchant Accounts with a Canadian Originating Bank/Issuer with AVS checking enabled for Domestic transactions, the Zip Code is used in place of the Postal Code for AVS checking.

For American Originating Banks/Issuers that have AVS checking enabled for International transactions, the Postal Code is used in the AVS matching process.

For more information about how to configure the Merchant Account through the Merchant Services GUI see the applicable section in the *Skipjack Merchant Services Guide* .

Card Verification Values (CVV) and Interpreting CVV Return Codes

Card Verification Values (CVV) codes are proprietary three or four-digit codes used by credit card Issuers as an anti-fraud mechanism for credit card transactions. CVV checking is used most commonly in card-not-present transaction situations, however, CVVs may also be used in card-present transactions to run the cryptographic authentication check of the CVV code to determine whether the card is legitimate or a counterfeit card.

CVV codes appear only on the card itself and are not included on bank statements, receipts, or encoded in the trackdata information on the back of the card. Therefore, successful submission of CVV confirms that the purchaser is in physical possession of the credit card. CVV code checking in transactions is not mandatory by all Processors and Issuers, however use of CVV in transactions is highly recommended by Skipjack.

How CVV code checking is used in Transactions

The Merchant requests the CVV code from the purchaser at the time of purchase. (Actual code names and locations are proprietary and vary by Card Type and Issuer, see the table below.) The CVV value is input along with other transaction details at the time of purchase.

When the CVV code is sent to the Skipjack Transaction Server it is passed to the Processor and Issuer's systems for scrutiny. A return code is issued by the Processor/Issuer and sent back to the Skipjack Transaction Network. The **szCVVResponseCode** and the **szCVVResponseMessage** return variables and values are used to determine the outcome of the CVV match.

The Skipjack Merchant Interface allows the Merchant Account to be configured to require the use of CVV matching for every transaction. Enabling this feature (Mandatory CVV Matching) ensures that CVV values must be included for every transaction.

To enable Skipjack Transaction Server to require CVV checking for every transaction:

1. Login to the Merchant Account.
2. Click on the **Edit Account** button located in the bottom section of the Account Summary page.
3. Scroll to the bottom of the page and select the check-box beside **Make CVV a required field**. The new feature is toggled on when a check mark is displayed in this box.
4. Scroll to the bottom of the page and select the **Submit** button. The feature is now enabled and a message is displayed to indicate that these account changes were successful.
5. Use the **Back** button on the Web browser to return to the previous screen.

6. Select the **Exit** link at the top of the page to log out of the Merchant Account.

The table below lists the card types by Issuer and related information about each proprietary codes by card type.

CVV Code Locations by Card Type

Card Type	Name	Location on Card and Notes
Visa	Card Verification Value (CVV2)	Three digits to the right of the credit card number in the signature area on back of the card.
MasterCard/Eurocard	Card Verification Code (CVC2)	Three digits to the right of the credit card number in the signature area on back of the card.
Discover	Card Identification Number (CID)	Three digits to the right of the credit card number in the signature area on back of the card. Does not return a CVV return code.
American Express	Card Identification Number (CID)	Four digits printed (not embossed) on the right front of the card above the credit card number. Does not return a CVV return code.

Response Codes for Visa and MasterCard/Eurocard

CVV Response Code	Description
M	CVV Match
N	CVV No Match
P	Not Processed
S	Issuer indicates that CVV2 data should be present on the card, but the Merchant has indicated data is not present on the card.
U	Issuer has not certified for CVV2 or Issuer has not provided Visa with the CVV2 encryption keys.
Empty	Transaction failed because incorrect CVV2 number was entered or no CVV2 number was entered.

Note: If you have questions about how your application must be designed to use the CVV data or CVV requirements for your Processor you should contact your Processor(s) directly.