Electronic Commerce Risk Management Guidelines

The continuously rapid growth of internet transactions has provided businesses with an important tool for attracting Customers around the world. When accepting transactions in this non-face-to-face environment, merchants must take additional steps to ensure the validity of the Customer and the card being presented. MasterCard® and Visa® regulations provide little recourse for merchants that receive chargebacks for internet transactions, due to the fact that neither the card nor the cardholder were present during the transaction. Listed below are guidelines to reduce exposure to fraudulent activity in these transactions, as well as other disputes from genuine Customers.

Card Type

Ask for both a card type (Visa, MasterCard, American Express®, etc.) and the card number. Ensure that the card type matches the beginning digit(s) of the card number as listed below. Invoke an error message for all mismatches and do not proceed with the transaction.

Card type	Beginning digit(s)
American Express	37
Visa	4
MasterCard	5
Discover/Novus	6
Diners Club	3000-3059 3600-3699 3800-3899

Address Verification Service (AVS)

Include an address verification service (AVS) request with all authorization requests. AVS will identify if the billing address given by the Customer matches the billing address on file with the issuing bank. This service is currently available on cards issued in the U.S with U.S. addresses only.

Although a transaction may be completed without a positive AVS response, a negative match may indicate that the Customer is not the authorized cardholder. Use caution when sending merchandise to a shipping address that differs from the billing address, regardless of whether the billing address received a positive AVS response. AVS response codes are as follows:

- Y Exact match of street address and five or nine digit zip code
- A Street address matches; zip code does not match
- Z Zip code matches; street address does not match
- N No match
- U Address information unavailable or issuer does not support AVS
- R Issuer authorization system unavailable, retry at a later time

Fraud Prevention Screening

Utilize a payment gateway that offers fraud prevention screening. Fraud screening will check the Customer's information against a database of those known to have past fraudulent activity. Reject any transaction that does not pass this process.

Validation Code (CVV/CVC)	Secure payment information in a manner that will prevent fraud by staff and external individuals. 1. Display only the last four digits of the card number to internal staff and require a password to obtain the full card number for operational purposes. 2. Track internal access to payment information. 3. Encrypt all stored card numbers on secure server and retain payment information behind firewalls to prevent unauthorized access.
Preventing Fraud	Require the Customer to provide the three-digit validation code appearing as the last three digits on the signature panel of the card. This will require the Customer to have the card in his/her possession to provide a valid code.
Email Confirmation	Send an email order confirmation to the Customer with detailed information regarding the transaction, such as: 1. Business name as it will appear on the Customer's billing statement 2. Total sales amount including sales tax and shipping and handling charges 3. Summary of items ordered and stock status with expected shipping and delivery date 4. Any applicable return/cancellation policy including any restocking fee if merchandise is returned 5. Customer service contact information (toll-free telephone number and email address) to prompt Customer to contact Customer service rather than submitting an inquiry to the issuing bank.

Guidelines – CVV2/CVC2

The CVV2/CVC2 indicator is a tool to help protect mail/phone order merchants against fraud.

When a cardholder calls to place an order, ask them for the three-digit code located on the signature panel following the card number on the back of the card. If you receive a match on the transaction, you can have some comfort in knowing the cardholder has the card in hand. If you receive a response of P or N, verify the correct code was entered. If the correct code was entered and you still receive a P or N, we don't recommend you process the order. This tells you the cardholder does not have the card present and the chances of receiving a chargeback for a fraudulent mail/phone transaction is greater.

When key-entering the transaction, the terminal will prompt you for a CVV code. If the cardholder claims there is no code on the back of the card, be highly suspicious. As of April 2001, Visa/Mastercard required all U.S. banks to have the CVV2/CVC2 code present.

Once the transaction has been entered into the terminal/software, one of the following code values will be issued in the authorization response.

M	The CVV2/CVC2 value matched the value on the account record.
N	The CVV2/CVC2 value did not match the value on the account record.
P	The CVV2/CVC2 value was not processed.
S	The CVV2 value was on the plastic, but not submitted with the authorization request. (Visa only)
U	The issuing bank either is not certified or did not provide the CVV2 keys to Visa. (Visa only)
Blank	No CVV2/CVC2 data was in the authorization response.

If you receive a response of U, you are protected against chargebacks for fraudulent mail/phone transactions. If you receive a response other than a U, and decide to process the transaction, you are liable for any fraudulent chargebacks received.

Please note: Non-U.S. bank transactions are not supported by CVV2 or CVC2 at this time.