

APPLIED MERCHANT | systems

Electronic Commerce Risk Management Guidelines

The continuous rapid growth of Internet generated transactions has provided businesses with an invaluable tool for attracting customers around the world. With 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 as well as the follow through with the total transaction. MasterCard and Visa regulations provide little recourse to merchants that receive charge-backs for Internet based transactions based on the fact that both the card and the cardholder were not present during the transaction.

Listed below are guidelines for accepting Internet transactions to reduce exposure to fraudulent activity as well as other disputes from genuine customers. A complete Visa manual entitled "Electronic Commerce Risk Management – Merchant Best Practices" is available for a minimal cost of \$10. This manual will provide comprehensive information relating to conducting an electronic commerce business from website content to Internet resources.

- 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	6
Diners Club.....	3000-3059 3600-3699 3800-3899

- Require the customer to manually enter the valid / expiration date(s) of the card. Do not provide a default date(s). This will ensure the customer enters the information and does not allow the default date(s) to stand, which will most likely differ from the actual valid / expiration date(s).
- 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 is currently available within the United States only.
- Although a transaction may be completed without a positive AVS response, a negative match may indicate that the customer is not the authorized owner of the card number being used. Also, use caution when sending merchandise to a shipping address that differs from the billing address, regardless of whether or not 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

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

- 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. In the near future, this three-digit code will be required for the authorization process to cross-check the validity of the information embossed on the card.
- Secure payment information in a manner that will prevent fraud by staff and external individuals:
 - ü Display only the last four digits of the card number to internal staff and require a password for staff that is required to obtain the full card number for operational purposes.
 - ü Track internal access to payment information.
 - ü Encrypt all stored card numbers on a secure server and retain payment information behind firewalls to prevent unauthorized access.
- Send an email order confirmation to the customer including detailed Information regarding the transaction such as:
 - ü Business name as it will appear on the customer's billing statement.
 - ü Total sales amount including sales tax and shipping and handling charges.
 - ü Recap of item(s) ordered and stock status with expected delivery date.
 - ü Any applicable return/cancellation policy including any restocking fee upon possible return of merchandise.
 - ü Customer service contact information, preferably both a toll-free telephone number and e-mail address to prompt the customer to contact customer service with any inquiries or cancellation requests prior to contacting the Issuing bank to request a chargeback.
- Set parameters to review high-risk transactions prior to the authorization request based on type of merchandise, dollar limits, amount of separate transactions, and any past spending patterns from individual customers.
- Avoid duplicate transaction processing by both staff and the customer:
 - ü Provide buttons that require a customer to click to order instead of hitting the [ENTER] key which is more likely to be in error.
 - ü Display a message during any real-time authorization process to alert the customer that the transaction is in process.
 - ü Send an email notification to the customer as detailed above to confirm the initial order has been successfully placed.
 - ü Set a system in place to identify identical orders within a specified short period of time and confirm with the customer that the order is indeed a separate transaction.
- Establish a detailed return/cancellation policy displayed on the website. Require the customer to click to accept the terms prior to completing the transaction.
- Upon receipt of cancellation and/or returned merchandise from a customer, issue credit promptly. Confirm the processing of the credit with the customer to avoid a potential chargeback. Please keep in mind that MasterCard and Visa do not recognize return/cancellation policies generated from an Internet transaction as being valid against cardholder disputes as they are not physically signed by the customer.