

# Sage Payment Solutions

## ONLINE RESOURCES

Training Material and Education for Merchants



### **RULES FOR VISA MERCHANTS**

Card Acceptance and Chargeback Management Guidelines

[http://merchants.visa.com/ds/pdfs/Card\\_Acceptance\\_and\\_Chargeback\\_Guidelines.pdf](http://merchants.visa.com/ds/pdfs/Card_Acceptance_and_Chargeback_Guidelines.pdf)

### **FRAUD PREVENTION TIPS FOUND ON VISA'S WEBSITE**

[http://usa.visa.com/merchants/risk\\_management/fraud\\_control\\_basics.html](http://usa.visa.com/merchants/risk_management/fraud_control_basics.html)

<http://www.visa.ca/en/merchant/fraud-prevention/visas-layers-of-security/address-verification-service/index.jsp>



### **RULES FOR MASTERCARD MERCHANTS**

Rules for Merchants

[http://www.mastercard.com/us/wce/PDF/12999\\_MERC-Entire\\_Manual.pdf](http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf)

### **FRAUD PREVENTION TIPS FOUND ON MASTERCARD'S WEBSITE**

<http://www.mastercard.com/us/securityandbasics/fraudprevention/index.html>

### **FRAUD PREVENTION GUIDELINES FOR CNP (Card Not Present) TRANSACTIONS**

Visa Card Acceptance and Chargeback Management Guidelines (Section 3, Pages 45 – 50)

[http://merchants.visa.com/ds/pdfs/Card\\_Acceptance\\_and\\_Chargeback\\_Guidelines.pdf](http://merchants.visa.com/ds/pdfs/Card_Acceptance_and_Chargeback_Guidelines.pdf)

## **SAGE PAYMENT SOLUTIONS FRAUD REDUCTION PROGRAM**

### **I. Credit Card Acceptance Policy**

- a. Use Address Verification System (AVS) on all incoming transactions; shipment of product should only be sent to an address that has been verified and associated with the credit card that generated the transactions
- b. Require signature on all product deliveries
- c. Use Card Identification Number (CID and CVV2) on all incoming transactions
  - i. On the majority of Visa credit cards, this is a 3-digit security code that acts as an additional verification measure and provides some assurance that the cardholder is in possession of the credit card
- d. Credit Card Descriptor – Clearly convey your merchant name, location and customer service telephone number in order to clearly identify your transaction on your customer's statement
- e. Use Soft Descriptors – For online merchants, soft descriptors can be used as an extension of the credit card descriptor to identify individual transactions
- f. Credit Card Authorization – To avoid technical chargebacks, be sure to settle all transactions in a timely manner and do not settle transactions with invalid authorization numbers

### **II. Refund Policy**

- a. Provide a clear explanation of all policies with regard to refund, return or customer service related issues on all invoices, promotional materials and websites
- b. Post customer policies in a conspicuous and accessible place
- c. Increase the timeframe in which a customer can request a refund
- d. Create an open line of communication for your customer to contact in case there are customer service issues via telephone or email
- e. Restocking Policy – Implementation of a Restocking Fee may cause partial or full chargebacks

### **III. Recurring Transaction Maintenance**

- a. Daily maintenance of your recurring transaction
- b. Remove all customers from your recurring transaction database in a timely manner

### **IV. Fraud Monitoring**

- a. Create a Negative Database of all customers that issued a chargeback for the purpose of denying future transactions and website access in the future
- b. Create a dedicated team of employees to review daily transactions for the purpose of identifying blatantly fraudulent activity and support customers service issues that may cause future cardholder disputes
- c. Create a rule-based report that identifies high-risk transactions characteristics (i.e. foreign transactions, multiple transactions, on cardholder's card, etc.)
- d. Employ & Implement a Risk Management Software package that could help you identify high-risk transactions (i.e. CyberSource, Retail Decisions, ClearCommerce, etc.)
- e. Website Warnings – Clearly state your policy with regard to credit card fraud on your billing page and report all fraudulent incidents to the proper authorities
- f. Bank Identification Number (BIN) Blocking – Block the acceptance of credit numbers related to high-risk areas (i.e. West Africa, Eastern Block Nations, Pacific Rim Nations, etc.)
- g. Internet Protocol (IP) Blocking – Block transactions generated from IP's originating from high-risk areas (i.e. West Africa, Eastern Block Nations, Pacific Rim Nations, etc.)