12 Potenial Signs of Card Not Present Fraud

Keep your eyes open for fraud indicators.

When more than one is true during a card-not-present transaction, fraud might be involved.

1. First-time shopper- Criminals are always looking for new victims.

2. Larger than normal orders- Because stolen cards or account numbers have a limited life span, crooks need to maximize the size of their purchase.

3. Orders that include several of the same item- Having multiples of the same item increases a criminal's profits.

4. Orders made up of "big-ticket" items- These items have maximum resale value and therefore maximum profit potential.

5. "Rush" or "overnight" shipping- Crooks want these fraudulently obtained items as soon as possible for the quickest possible resale and aren't concerned about extra delivery charges.

6. Shipping to an international address- A significant number of fraudulent transactions are shipped to fraudulent cardholders outside the US. Visa® AVS can't validate non-US, except in Canada and the United Kingdom.

7. Transactions with similar account numbers- Particularly useful if the account numbers used have been generated using software available on the internet (e.g. CreditMaster).

8. Shipping to a single address, but transactions placed on multiple cards- Could involve an account number generated using special software, or even a batch of stolen cards.

9. Multiple transactions on one card over a very short period- Could be an attempt to "run a card" until the account is closed.

10. Multiple transactions on one card or a similar card with a single billing address but multiple shipping addresses- Could represent organized activity, rather than one individual at work.

11. In online transactions; multiple cards used from a single IP (Internet Protocol) address -More than one or two cards could indicate a fraud scheme.

12. Orders from internet addresses that make use of free email services- These email services involve no billing relationships and often neither an audit trail nor verification that a legitimate cardholder opened the account.

Other Possible Scams

Deaf Relay System

This service allows the fraudster to not have to speak a word to the business and has been targeted for fraud sales. Please use careful precautions when accepting sales.

Wires or Western Union

Scammers pay using a fraudulent credit card but ask for money to be wired or sent via Western Union back to them for one reason or another.

"Too Good to Be True"

If the sale is a very large amount, the customer is asking for large quantities or the sale is otherwise out of the norm for your business it might be a fraudulent sale.

Fraud and Chargeback Tips

I. Credit Card Acceptance Policy

- 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
- Require signature on all product deliveries
- Use Card Identification Number (CID and CVV2) on all incoming transactions
  i.e. on most 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
- 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
- Use Soft Descriptors – For online merchants, soft descriptors can be used as an extension of the credit card descriptor to identify individual transactions
- 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

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

III. Recurring Transaction Maintenance

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

IV. Fraud Monitoring

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

Please reference Visa© and Mastercard for more detailed tips:

https://usa.visa.com/support/small-business/fraud-protection.html

http://www.mastercard.com/us/merchant/security/fraud_prevention.html