Fraud Signs

PayDollar Reference

CAUTIOUS STEPS

Take these steps to accept online payments:

1. Obtain an authorization.

2. Verify the card's legitimacy:

   - Ask the customer for the card expiration date, and include it in your authorization request. An invalid or missing expiration date might indicate that the customer does not have the actual card in hand.

   - Use fraud prevention tools such as Card Verification Value 2 (CVV2), and Verified by Visa.

3. Look for general warning signs of fraud (listed below).

4. If you receive an authorization, but still suspect fraud:

   - Ask for additional information during the transaction (e.g., request the financial institution name on the front of the card).

   - Contact the cardholder with any questions.

   - Confirm the order separately by sending a note via the customer's billing address rather than the "ship to" address.

To report suspicious activity, contact PayDollar or your merchant financial institution.

POTENTIAL FRAUD SIGNS

Keep your eyes open for the following fraud indicators. When more than one is true during a card-not-present transaction, fraud might be involved. Follow up, just in case.

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 another address:** A significant number of fraudulent transactions are shipped to countries outside the country of transaction origination.
7. **Transactions with similar account numbers:** Particularly useful if the account numbers used have been generated using software available on the Internet
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 of time:** 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 e-mail services:** These e-mail services involve no billing relationships, and often neither an audit trail nor verification that a legitimate cardholder has opened the account.

Reference:

http://www.usa.visa.com/business/accepting_visa/ops_risk_management/card_not_present.html?it=l2|/business/accepting_visa/ops_risk_management/fraud_control_basics%2Ehtml|Card-Not-Present