8 fishy transaction traits your merchants can monitor

Help retailers recognize these signs of possible fraud

For any business, turning down a sale is unnatural. After all, the idea is to make money. However, keeping an eye out for fraudulent purchases, particularly those originating from e-commerce, is a smart tactic.

By doing things right, your merchants can avoid chargebacks and keep themselves out of the fraud victim's seat. To help you advise merchants on what to look for, we've outlined some common signs of fraud below.

Warning signs

Merchants that monitor the transaction characteristics and buying behaviors of their customers can help control fraud. Merchants can learn to recognize the signs of fraud and watch for transactions possessing several of the following characteristics:

1. **First-time shopper** — Criminals usually hit a merchant once and don't return.
2. **Larger-than-normal orders** — Because they may be using stolen cards or bogus account numbers that have a limited lifespan, criminals need to maximize the size of their fraudulent purchases.
3. **Orders consisting of several of the same item** — Because these items are intended for resale, having more of them increases the criminal's profits.
4. **Orders made up of big-ticket items** — These items have maximum resale value and, therefore, maximum profit potential.
5. **Orders with rush or overnight shipping** — Criminals want these items in their hands fast for the quickest possible resale and often aren't concerned about extra delivery charges.
6. **Orders shipped to an international address** — A significant number of fraudulent transactions are shipped to bogus cardholders outside the U.S., and the Address Verification Service (AVS) can't validate non-U.S. addresses.
7. **Orders shipped to a single address but paid for with multiple cards** — This is characteristic of a scheme based on auto-generated account numbers or a batch of stolen cards.
8. **Multiple transactions on one card over a very short time period** — Sometimes this is an attempt to run a card until the account is closed.

Watch those email addresses

If your financial institution sponsors merchants that accept orders electronically, encourage them to watch for orders from email addresses offered by free services.

For these services, there's no billing relationship and often no audit trail or verification that a legitimate cardholder has opened the account. Some common free email address services include Yahoo!®Mail, Juno®, Gmail™and Net@address®.

Bottom line

While none of these characteristics alone indicates a merchant has been scammed, several in combination may indicate fraud. Encourage your merchants never to ship a valuable order until they receive a valid authorization.

For more information

If you have questions about merchant fraud, please call Jim McCool, merchant risk analyst, at 800-537- 5427, ext. 4220.