Fraud Awareness Month

Moneris SOLUTIONS

Fraud can represent a considerable cost for your business. Being aware of what to look for can prevent merchants from becoming victims of fraud and from suffering from significant financial losses. Moneris is committed to ensuring that our merchants have access to best practices and tips to keep their businesses safe. For more information, we encourage merchants to visit our website and review all tips and best practices at **http://www.moneris.com/fraud**

Fraud can take place at any time, both with the card-present and during a card-not-present transaction. A card-not-present transaction can lend itself to more risk as this type of transaction occurs with a credit card and is made over the telephone, through the mail or on the Internet where the physical card has not been swiped into a reader.

12 Potential Signs of Card Not Present (CNP) Fraud

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, buying the most that they can at one time.
3. **Orders that include several of the very 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 of the country. Visa Address Verification Service can't validate customers outside of Canada, United States 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.
8. **Shipping to a single address, but transactions are placed on multiple cards:** This 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:** This could represent 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:** This 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 definitely 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.

For more information on Moneris' fraud prevention tips and best practices, please visit **http://www.moneris.com/fraud**