

## **Protecting Yourself against Credit Card Fraud Operation Educate May 2009**

We frequently get calls from merchants who are suspicious of a particular order, but aren't sure how to distinguish between a legitimate order and fraud. Here are some common earmarks of fraud.

- The order comes via relay for the deaf or other non-traceable email. Customer refuses any other form of communication. Language skills in the email indicate that English is not their native language.
- The order is unusually large. There is no concern for specifics such as color, sizes etc.
- Customer offers to provide their own method of shipping.
- The order has other unusual details; someone in New Jersey orders a standard sewing machine from a store in Utah and is willing to pay shipping for a machine that is actually manufactured in New Jersey.
- The order is coming from or shipping to, a trade-sanctioned country, or is somehow affiliated with a sanctioned country; Examples: 1000 gallons of paint are ordered for an orphanage in Africa, but it is requested that the order be sent to New Jersey.

Most of the examples above refer to card not present transactions. Here are a few scenarios that may occur in a retail environment.

- The purchase is unusually large and the store clerks are intimidated by the "wealthy" customer. Remember she may not have paid for the Louis Vuitton bag she is carrying!
- A customer's card is declined, she insists she paid it off this week and offers to call her bank. After she initiates the call she gives her cell to the clerk and the person on the line gives the clerk an authorization code. The clerk is not prompted for any information such as merchant account number etc.
- Customer purchasing in the store requests the purchase be delivered for various reasons, such as, it is a gift or they are traveling and don't want to carry the item. Later it is claimed that the item was never received.
- The customer is purchasing for someone else such as his girlfriend, but the two never come into the store together. He calls in the number and then later she comes into the store to purchase or try on the item. Another scenario; he buys a gift card for her, she comes in very soon after the gift card is purchased and spends the entire card.

How can you protect yourself? Remember, the standard operating procedures are there to protect you!

- Swipe the card whenever possible!
- When processing card not present sales request the security or CVV2 code.
- Require a signature on the receipt or use signature a confirmation delivery service.
- Keep receipts for at least a year.

- If the card is declined or just a suspicious internet order, request another form of payment such as cash or a cashier's check.
- Initiate voice authorizations and address verifications using the numbers shown below. When requesting an authorization you will be prompted to enter numbers affiliated with your account.

**American Express 1-800-443-2639**

**Discover/MasterCard/Visa 1-800-944-1111**

- Please contact the PCCP (POSIM Credit Card Processing) department 1-800-553-9314 if you have any questions.

### **Useful Links**

[http://usa.visa.com/merchants/risk\\_management/card\\_present.html](http://usa.visa.com/merchants/risk_management/card_present.html)

[http://usa.visa.com/merchants/risk\\_management/card\\_not\\_present.html](http://usa.visa.com/merchants/risk_management/card_not_present.html)

[http://usa.visa.com/download/merchants/card\\_acceptance\\_guide.pdf](http://usa.visa.com/download/merchants/card_acceptance_guide.pdf)