

Protecting the Merchant from Credit Card Fraud

Many merchants today do not realize the importance of “**knowing your customer.**” With in the past few years many merchants have been taken advantage of by companies (**thieves**) who want shipments shipped via a freight forwarding company to foreign countries. Sometimes the merchant must incur prepayments to specific forwarding companies before they realize it's a scam. Many of these merchants are use to dealing with corporations who ship overseas and are use to given quotes via fax and email. It is becoming more prevalent that these merchants are becoming easy targets. Here are a few examples:

A few years ago a lawyer friend of mine approached me, knowing that I was in the merchant processing industry, and asked for advice on how to help his client be taken off “the match” list by Visa & MasterCard. This client had processed cards for over 20 years and had never received a chargeback where someone disputed the charge. His merchant had received several orders of products from quotes he had given someone overseas. The prospective buyer gave him 2 different MasterCard's on the 1st order and asked him to run equal amounts on both. The cards were approved and the merchant shipped over \$6,000 worth of product via a freight forwarding company to Singapore. The following week he received a bigger order for almost \$12,000 and again was given 2 new MasterCard's and again told to split the order. Again the cards were approved and therefore the products were shipped same address in Singapore. Within 3 weeks of shipping the last order the merchant had \$18,000 pulled from his checking account. This particular merchant ratio of receiving MasterCard was about 1 MasterCard to 5 Visa and usually would only get MasterCard once in a while. All of a sudden this merchant has 4 charge backs on MasterCard within 1 month. He has officially gone over the ratio of what is acceptable according to the bylaws of MasterCard and his accounts for processing are now turned off.

Several months later another client of mine called and said that a “Pastor” from NY had emailed him and asked him about raw glass material. Asked for several quotes and with in a few days placed the order and used the same scenario as above, but wanted to send someone local to pick up the material. This client became suspicious and called me immediately. We called the risk department of the processing company and got the issuing bank on the phone to find out that the cards were recently issued numbers. They contacted the actual consumer to find out the client never received his cards in the mail. They were stolen before the client could even know they were issued to him. In this case both the merchant and the consumer were protected because the merchant just had that gut feeling that something wasn't right.

Lesson Learned. Just because a credit card gets an approval does not mean that it's a good sale.

Knowing who you are doing business with **is** the merchant's responsibility. The processing companies and issuing banks try very hard to protect consumers from fraud; however, it still happens. Bottom line is no matter how many systems are in place to protect the consumer and the merchants, thieves still find ways to beat the system, however; by taking some simple steps and using common sense can help deter thieves from trying to scam you. Here are some steps for you to follow to help prevent fraud from happening.

A Hesitant Caller. A shaky voice or delayed responses to questions may indicate that the caller is not comfortable with the information he is providing.

Rush Orders. These are a favorite weapon of the "here today/gone tomorrow" schemes.

P.O. Boxes and Mail Receiving Services. This may indicate lack of a permanent address.

Above-Average Transaction Amounts. Merchants often know the amount of an average sale. Be wary of those transactions that greatly exceed the norm.

PURCHASES THAT CAN BE CONVERTED to CASH. Examples include electronics, jewelry and leather goods.

1-800 Return Phone Numbers. Be suspicious of toll-free telephone numbers when given as the day or evening phone number. Attempt to get a direct line instead.

Multiple Orders in a Short Period of Time. Many merchant systems show all orders placed to a certain account or unique customer number. Be especially aware of multiple orders.

Fourth Quarter. Fraud is always a consideration, but fraudulent activity is particularly widespread around the holidays.

Larger than Normal Orders. This is dependent on each merchant's definition of a "normal" sized order. Because criminals are usually using stolen or fictitious credit card numbers that have a limited life span, they need to maximize the size of their purchases

Orders Made Up of "Big Ticket" Items. These items have maximum resale value and therefore maximum profit potential.

Orders Containing Several of the Same Items. Criminals usually select the items with the most resale value. As these items are intended for resale, having more of them increases the criminal's profits.

Orders Shipped "Rush" or "Overnight" or Freight Forwarded. Criminals want these items in their hands as soon as possible for the quickest possible resale, and are not concerned about the extra delivery charges. On first time orders, don't be afraid to ask for too much information. If you don't know them, get billing information, shipping information, security codes and if possible get an imprint of card. I've actually had a merchant who use to ship an imprinter to the prospective client and ask for an imprint of the card and for them to sign the receipt. It sounds like a lot of work, but considering the size of his orders (\$10,000 and up) he was simply taking every effort to protect himself from a chargeback. If you have further questions contact your financial advisor for more information.