

An Inside Look at E-Commerce Fraud

Prevention and Solutions

By Sharon Curry
<Fraudchick@aol.com>
Copyright 2000.

E-Commerce Fraud

Remember the big buzz in the media about Internet fraud? One of the biggest concerns was the threat of credit cards being stolen through the online purchase procedure. It is not surprising to me that these fears have not been totally realized. While there is always an opportunity for this to occur, it is definitely not the overwhelming disaster that the experts forecasted. The systems that have been put into place to combat this have been remarkably successful. Interestingly enough, the frauds occurring on the Internet are simple variations of standard consumer fraud and simple mail or telephone order (MOTO) fraud. In other words, the same old wine in a new and improved bottle.

Internet fraud is a fair reflection of basic fraud statistics. The highest numbers of incidents are frauds against consumers — such as pyramid schemes, stock schemes, and work-at-home schemes. Online cons seem to favor Internet auctions where it is most definitely *caveat emptor* — buyer beware! Internet auctions and bartering sites are simply Internet flea markets with the extra-added bonus of anonymity for the fraudster. But my big question is, what about *caveat venditor* — seller beware? Where are all of the headlines about consumers defrauding merchants? It's certainly not as sexy as an arrest of over 100 Wall Street con artists defrauding consumers out of hundreds of millions of dollars. Still, the fact remains that e-commerce fraud is a hot issue for both cyber and click and mortar merchants.

Crunching the Numbers

Have you ever done the math on fraud in your business? Fraud can be very costly, but a laid back approach to the issue can be even costlier. If an e-merchant regularly lets go of losses — or fails to prosecute thieves — the word soon spreads through various networks until, finally, that e-merchant becomes a favored target. The costs can be calculated in merchandise or services lost, shipping and handling, time to process the order, processing chargebacks (\$15-\$25 per transaction on average fraudulent or not), processing fraudulent checks, and your time and effort to investigate the fraud. According to research conducted by Meridien Research, e-merchants lost \$1.5 billion in 1999. That's 10% of the total estimate of \$15 billion in sales in 1999. Small e-commerce businesses cannot afford 10% shrink due to theft. It will be interesting to watch these statistics as databases like the UCR (Uniform Crime Report) better digest and organize cyber crimes reported by merchants.

And now, credit card companies have made the move to address the rise in chargebacks. For example, MasterCard sent notice to its merchants that it intends to fine merchants \$25,000 and up for chargebacks that are 2.5 percent or higher of total sales volume for two consecutive months. Be ready for this trend to take us all to new and interesting places.

The Criminal

I just love the media's portrayal of e-commerce criminals. According to the news services, the cyber criminal is 18 to 25, extremely intelligent, and normally a hacker with something to prove. Before I began investigating external cyber crimes, I envisioned my nemesis as a twenty-something, male, possibly a computer programmer with an attitude. In reality, my nemeses have ranged in age from 11 years old to 60 something, more male than female (but not by much).

Most had no past criminal histories. Occupations range from grade school student to housewife, and nearly all had average to below average knowledge of a personal computer. Most surprising is what the reasons given have been. "I was bored." "I didn't think I'd get caught." "I wanted to see if I could do it." It's the same reasons shoplifters give — it's cyber shoplifting.

Types of E-commerce Schemes Against Merchants

1. **Credit Card Fraud/ Identity Theft:** This is the most common type of e-commerce fraud. It comprises 98% of the frauds I've investigated. There are so many variations in this scheme, I could write a book just on this subject. The credit cards or credit card numbers were stolen in a myriad of ways. Some are stolen through the mail, at restaurants, hotels, pocketbook/purse theft, dumpster diving, card number generators, or any other way that someone can steal a credit card or number.

The most common scheme is where thieves use stolen credit cards to purchase goods through the Internet for their own use. In the instances of software, the product is simply downloaded and the fraudster is long gone. In the case of merchandise, the con may have the merchandise sent to his home, to the house of a neighbor on vacation, or to an abandoned house. But what about schemes where the recipient is not the thief?

In one scheme, a con artist arranges to sell an expensive item, (a \$5,000 computer for example) in an ad on the Internet, in a newspaper or in an online auction. The con offers the brand new, never-been-used computer for \$1,000. The con claims that he or she is going through troublesome times and needs fast cash. An enthusiastic buyer leaps at this great deal. The con tells the buyer that he will ship the computer at the buyer's expense for them to look over. If they are satisfied, they can send the money. What a deal! The con then orders a pricey \$5,000 model through the Internet with a stolen credit card and has it shipped directly to the buyer/victim. Naturally, the buyer is thrilled at the high-end computer and sends the con his money through Western Union, no ID required. Eventually, the credit card owner disputes the charge and the buyer is stuck dealing with the police, but the con has his money and is long gone. The beauty of this scam for the fraudster is that he usually strings several buyers at one time.

2. **Chargebacks/Denial of Receiving Service or Product:** This is my least favorite of all schemes because it encompasses legitimate customer complaints. It's these bad apples that ruin it for the rest of the bunch. In this scheme the fraudster denies receiving the merchandise. It's very difficult to profile this trickster because so many people try it. The modus operandi is to deny, deny, and deny. The customer denies receiving, signing for, and sometimes even ordering a product. The mentality is the same as a shoplifter who places \$200 worth of DVDs under a bag of dog food in a shopping cart where the cashier can't see it. They reason that the store deserves losing the DVDs for not looking under the bag of dog food. The same holds true in the e-commerce scheme, if the e-merchant runs a slipshod business, then it "deserves" to lose. They NEVER consider themselves thieves, ever. They only shine the light of truth on the system.

It's very difficult to uncover a scheme like this, but not impossible. In one case, two customer service representatives were discussing issues with customers who never

received orders. They realized that five of the customers who had called in to complain were the same man. The customer used five variations of his name, reregistered every time he came to the web site to order, and gave five variations of his same address. The address, something like 100 SW 1st Street Apt 5 became 100 Southwest First, Apt Five; One hundred SW 1st #5; 100 SW First, unit 5. I think you get the idea. The police discovered this con was selling the high-ticket merchandise to friends at a deep discount.

3. **Bogus returns.** It's in the mail. The customer claims he sent the merchandise back and it never arrives. They may also send back a single item, but claim the box contained several items more and demand full refund.

Many incidents come to mind when I think of this scheme. The end result of this scheme will depend on what level your business applies customer service. Is the customer always right or will you require some due diligence on the part of the customer? It's up to you.

Tracks of a Cyber Thief

E-merchants are beginning to recognize the warning signs that indicate possible fraud. Here are some tracks of a cyber thief.

1. **Late night orders.** A large percentage of my fraud orders occurred late in the evening or early morning. E-commerce fraud increases at night. In one of my investigations, I found that 9 out of 10 orders were made between midnight and three in the morning.
2. **Orders placed outside the country.** I've read many statistics on this issue and there have been some discrepancies on which countries produce the highest fraud numbers. Russia, West African, and South American countries seem to produce consistent high numbers. The problem with out of country deliveries is that once it's gone, it's gone. We currently do not ship merchandise out of the country. Beware, too, of intermediary drop boxes. We had an incident where a large volume of merchandise was shipped to a "warehouse" in Florida where it was then sent overseas.
3. **Drop box addresses.** Set a policy of not shipping to P.O. boxes, suites, or drawers. Intermediary addresses never look like drop boxes because they use physical addresses to give the illusion of security. Intermediaries will set off warning bells when you follow the rule of reviewing large quantities of merchandise sent to a single address. This is how we found ours before we lost too much money.
4. **Free/Anonymous e-mail services.** While I don't agree that every order made with a free/anonymous e-mail service is fraudulent, I can say that approximately 95% of all fraudulent orders I investigated were made with these types of services. I've found that all of these fraudsters using these e-mail services had legitimate ISP's, but they used the free e-mail service for added anonymity. These services will not give information to e-merchants or the police without a subpoena.
5. **Express shipping.** Online schemers need time to get away. Many are in a rush to get the goods and then close shop. They don't care that the cost of shipping almost equals or exceeds the cost of goods because they aren't paying for either. In one instance, a

fraudster purchased three swimming pools. The cost of the express shipping exceeded the cost of the pools!

6. **High quantity orders.** Cons will attempt to order large quantities of the same item. Examples I've personally run across have ranged from ten 1-carat engagement rings to six VCRs in one order.
7. **High dollar orders.** Money is no object when it's not yours to begin with. This one is fairly self-explanatory.
8. **"Ship to" differs from "Bill to."** This one can be a difficult track to follow, especially around Christmas. Most e-commerce has been built on convenience and the ease of having gifts sent for the customer. Still, this can be a key indicator of a possible fraudulent order. Here's a quick check: the telephone number given should match the "Bill to" not "Ship to" address. If the telephone number matches the "Ship to", do yourself a favor and call the issuing bank.
9. **E-mail address.** The e-mail address itself can give some clues. The e-mail address, in most cases, will match something in the customer's name. But, cons may use extremely crude or cute e-mail names, i.e. Imathief@domainname.com, getbent@domainname.com, etc.
10. **Repeated attempts to order on the same card.** There are computer programs that generate credit card numbers for online thieves, but they still require some finessing. It is not uncommon for a con who has generated a credit card number or stolen one to make numerous attempts on the same credit card keying in different expiration dates. Review all of your repeated and failed order entry attempts.
11. **Frequent calls from customers.** I really enjoy this one because you have a chance to record and trace the call. Fraudsters can be really anxious people. Remember that they may want to close the deal fast so they can close up shop before being caught. They may call in repeatedly to check on the status of orders. In one case, a schemer called in over thirty times in one day! She was absolutely giddy with greed. Some fraudsters call simply to bully and can be extremely obnoxious. I recommend you tape all incoming calls, but I'll discuss this more later in this article.

I would like to make it absolutely clear that none of these signals are an absolute identifier of fraud. They are indicators of possible fraud.

Safeguards

There are countless ways to safeguard your business from fraud. But here are some simple ways to help yourself.

1. **Held orders.** Create a "held orders" department where orders can be reviewed manually. Set certain guidelines for what orders will be held. Examples might be orders over \$250, which might be raised to \$500 or higher at Christmas.

2. **In-house database.** Create an in-house database of all fraudulent orders by address. Take the time to run all orders through this database.
3. **Shared database/Chain calls.** I will probably get some feedback on this one, but I will mention it anyway. Establish a network with other e-merchants in the same business as yours. Share fraudulent order information with them. Chain calls benefit everyone. We should all be working together to stop these bad guys.
4. **Telephone database.** You can purchase these on CD-ROM or use services such as Anywho.com's reverse telephone look-up. Use these databases to check phone numbers.
5. **Issuing Bank.** Contact the Credit Issuing Bank (CIB) and they will contact the customer for you. The CIB will confirm the name and address given by the customer. Many times the phone number given to you on the order form is no good; the CIB can help you in this instance. Have your merchant ID ready when calling the credit card company. Here are phone numbers you can call.

| | |
|---|--------------------------|
| American Express | 1-800-528-5200 |
| Discover Card | 1-800-347-2000 |
| Visa/MasterCard | 1-800-228-1122 |
| CardService International Merchant Services | 1-800-456-5989 |
| E-Commerce Exchange Merchant Account Set-Up | 1-800-242-0363 Ext. 2736 |
6. **Call the customer.** In the instance where you think you have the correct number you can call the customer yourself. Otherwise, the CIB will contact the customer and have them call you.
7. **Document customer phone calls.** This is extremely helpful when you've lost merchandise to a fraudster. I recommend that you get caller id and record incoming phone calls. Have your customer service employees document the calls on a log as well.
8. **Cyber shoplifting notices.** Almost every retailer has shoplifting notices posted, why don't you? Let the shopper know that all fraudulent orders will be pursued to the fullest extent of the law. Since each prosecution will vary according to the fraudster's state of residence, it is best to keep this vague.

What to Do if You've Been Scammed

Yes, there will be instances where you will hit a brick wall on any sort of recovery, but contrary to what some experts are saying, there are some things you can do once you've been scammed. Most law enforcement agencies want to help. The problem is that law enforcement needs tools to do their jobs. Tools in this case means laws. There are not many laws that are specific to this crime, many agencies use identity theft, mail fraud, receiving stolen goods, and other standard laws currently on the books. Here are the steps you should take when someone has stolen from you.

1. **Documentation.** Pull together all documentation, including any phone records you may have accumulated. Include the original order, who the cardholder victim is (if applicable), date it was sent and identifiers for the merchandise (serial numbers, etc).

This is where you will want to take a deep breath and do some basic research on your con. Do the reverse phone number lookup if he's called in. Run the name of the fraudster through Anywho.com or other online phone books. Check TheUltimates.com to research e-mail addresses. If your loss is high, then it would benefit you to pay \$30 to have a private investigator skip trace the "Ship To" address for you. You can try to identify the e-mail address domain name at Network Solutions. It can give you limited information about who owns the domain name.

2. **Follow the product.** Where was the merchandise sent? Hopefully you have established a firm policy against shipping to drop boxes and post office boxes. If you have, then the address will be a firm physical address. Don't give up if you find out that the address is a deserted house. The police may have an investigation established on that location.
3. **Shipping Information.** Pull the shipping information to get documentation of who signed for the merchandise and the date and time it was received.
4. **Local police.** Contact the local police who have jurisdiction over the address where you sent the merchandise. To locate the appropriate law enforcement agency you can use the area code and telephone information or Internet sites like the police directory at <http://www.copscgi.com/>. Explain to them what happened. Police are interested in "sexy" cases. When I call them, I usually tell them that, in the majority of cases, the fraudster has stolen from more companies than mine and it could result in a high dollar case. It would amaze you how often this is true.

This is where it can get tricky. Some police will not go in after the fact, but others will. If the fraudster has another order on deck, offer to help the police conduct a *controlled delivery*. A controlled delivery is a delivery that the seller has complete control over in order to collect enough information from the fraudster to prosecute him. Let's say your company has an order pending for a \$500 television set for a fraudster who has already received other pieces of merchandise. Contact the police and arrange to deliver the television under their supervision. In some cases I've had police dress up as UPS and make the delivery themselves. The moment the con signs for the package, the arrest is made on the spot. I enjoy controlled deliveries. Nine times out of ten the controlled delivery will net the law enforcement agency more than the fraud against your company.

If there are no more orders pending, then there are some tricky things you can do to help the police identify the fraudster. What things you can do depend on what type of business you have. The key to this "after the fact" solution is to flush the fraudster out again. What can you do to get the con to call in and talk to you? What can you do to engage the thief in an e-mail correspondence without arousing his suspicions? Use your imagination. Your objective is to identify the individual(s) who ordered and then received the stolen goods. One trick is to send an e-mail to inform them that a part on a delivered product had a recall and you need to ship the replacement part. Then do a controlled delivery with that shipment.

Maybe that customer ordered over a certain dollar amount and your company wishes to send a freebie as a "thanks." And, oh, what a thanks it will be! When the fraudster signs for the "gift" you can nab him on a controlled delivery.

As you read this some ideas will pop into your minds. You can inform them that they are due a refund and then make arrangements for the check to be hand delivered. I could go on and on. There are all sorts of things you can do to help the police do their jobs. All you have to do is make the offer and be diligent.

If you have any questions about e-commerce fraud feel free to contact me at Fraudchick@aol.com.

Here are some helpful databases:

Telephone Databases: This includes reverse telephone directories.

<http://www.theultimates.com/>

<http://people.yahoo.com/>

<http://www.anywho.com/>

<http://www.infospace.com/people1.htm>

<http://www.tollfree.att.net/tf.html>

E-mail Databases: This includes reverse e-mail searches.

<http://www.theultimates.com/>

<http://people.yahoo.com/>

<http://www.infospace.com/email1.htm>

Internet Domain Databases

<http://www.networksolutions.com/>

<http://www.dotcomdirectory.com/nsi/basic.htm>

<http://www.networksolutions.com/cgi-bin/whois/whois/>

<http://www.websense.com/locator.cfm>

Want to go it alone? Here is a comprehensive archive of databases from the Dow Jones to people finders like DBT (Auto Track), <http://www.lainet.com/factfind/database.htm>