Online Auctions:

The Bizarre Bazaar

By Sharon Curry

The Bizarre Bazaar

Once upon a time, Bob decided he needed a laptop computer to handle his personal finances, so he researched all the brands and options. Bob was a wise consumer. He did his homework. When the time came for Bob to buy the computer, he decided to find a bargain¾ rather than going through a standard retailer. So, Bob paid a visit to the ATM machine and made his way to the streets of the city. While walking down the street, a strange woman walked up to him, her face hidden by a veil. The woman explained that she had to remain anonymous to protect herself from stalkers. She then showed Bob a photo of a laptop computer she had for sale.

Bob was ecstatic because the glossy magazine photo depicted the exact make and model that Bob wanted. The woman offered it to Bob for $2,000 in cash, which was $1,000 below retail. Bob promptly forked over the money. The woman then told Bob to stay put, and that she would be back in a few days with the laptop. That was one year ago. Bob is out the $2,000 and still has no computer. Sounds absurd? Yes, it is absurd¾ yet this type of sale goes on tens of thousands of times a day through online auctions. Welcome to the Bizarre Bazaar.

Fortunately only a fraction of online auctions have unhappy endings that resemble Bob's. The world's largest online auction, eBay, claims that, out of 40,000 listings only one results in a confirmed case of fraud. Nevertheless, online auction fraud is the number one Internet fraud reported to the Federal Trade Commission (FTC). The FTC received 10,700 complaints about online auctions in 1999¾ compared to just 107 complaints in 1997. The FBI's Internet Fraud Complaint Center (IFCC) gets an average of 1,000 consumer complaints a week. Just under half of those complaints, 48.8%, were about online auction fraud. Most noteworthy is that 85% of those complaints reported to the FTC were transactions where the buyer paid the seller with a money order or cashier's check.

The majority of us use common sense when shopping. When we go to a store we examine the merchandise and take possession before we pay our money. We ask for a receipt. So where does this common sense go when we fire up our computer? Online buyers tend to throw caution to the wind in the heat of a good buy. The Internet’s no-holds-barred, carnival-like atmosphere encourages sellers to exaggerate the condition or quality of their merchandise. The anonymity of bogus IDs emboldens others to commit fraud. Maybe people would be more careful if they knew of the bad things that could happen to them in an online auction. The best prevention is education.

Schemes:

Most online auction flimflams are an old wine in a new bottle. Nearly all are traditional mail order schemes and some are federal crimes because they involve mail fraud. Fraudsters should note that law enforcement agencies have made huge advances in addressing crimes committed using the Internet. The opportunity for mischief on the Internet is boundless. Here area few red flags to beware:

Shilling: A *seller* uses bogus Ids, or co-conspirators, to place additional bids on their own auction item in order to drive up the bid price.

Prevention: Review the bid history for last minute bids from multiple IDs¾ or the same ID multiple times. Then compare these IDs to the seller's last auction. If they match, you may have uncovered shilling. Report your concern to the auction site and avoid that seller's auctions in the future.

Bid Shielding: The *buyer* uses bogus Ids, or co-conspirators, to place multiple bids on an item to inflate the selling price to scare off competitors. The schemers will pull out the high bids at the last minute and enjoy a low bid win. Sometimes juveniles or online anarchists do this for personal amusement with no personal gain.

Prevention: Review the IDs of the last minute bid-withdrawals. Research those IDs against other auctions where they may have done the same thing. You are under no obligation to accept a bid. If you uncover a common theme with these IDs, notify the auction site immediately.

Misrepresentation: A *seller* may intentionally misrepresent the item in the written description or by using a glossy marketing photo, likewise, blurry, or strategically blocked photos can hide flaws. The item in the picture may look fantastic, while the real deal may be a disappointment.

Prevention: Ask questions. The write-up and photo should be enough to give the potential bidder a clear picture of the actual item. Don't let the seller be evasive or distract you with descriptions like "one of a kind." Ask them where they got the item, where they got it appraised, how they verified its value, how old the item is, etc. If they avoid answering, move on. If you've received something that isn't what was described, notify the seller immediately. Inform the seller that you didn't get what was described and ask for your money back. Stay cool and don't be accusatory. If the seller refuses, then report them to the auction site and state the facts in that seller's feedback.

Fee Stacking: Most *sellers* charge a flat rate for postage and handling, charging more for heavy items. A seller could tack on hidden fees after the auction in order to get more money. For example, you may win the bid at $30 and then receive your congratulatory e-mail that reads: "That will be $30 for the item plus $10 for postage, $5 handling fee and $5 for the shipping container." Now you pay $50 for what should only be $30.

Prevention: Ask the seller what all the costs are before the auction begins. Save or print a copy of the response. If you fail to do this and the seller tacks on additional fees, research what the costs should actually be, then ask that the seller stick to actual costs.

Failure to Ship Merchandise: The *seller* posts an auction under a bogus ID (in the case of a dumb criminal a legitimate ID) with the intention of receiving money from sellers and giving nothing in return. The seller sends notice to (usually) several bidders that they've won, and directs them to send money right away. The bidders receive nothing.

Prevention: Don't buy from sellers who only take cash. Favor auctions that take credit cards, checks, or third party payments¾ like i-escrow, Tradesafe or Paypal. An escrow service holds a bidder's payment until they receive the merchandise. Then the payment is released to the seller. These services charge a small fee.

Failure to Pay: The *buyer* fails to pay the seller for goods received. This can be accomplished through a bad check, a bogus money order, a counterfeit certified check, stolen credit card or, simply not paying.

Prevention: Be wary of buyers who demand you send the merchandise immediately. They may want to get their merchandise before the bank discovers that they used a stolen credit card. Sellers should try to accept smart payments¾ like credit card or an escrow service, which covers the seller in the case of fraud. Don't mail items to PO boxes, suites, or drawers. Make it a policy to send merchandise to a *physical* address. Don't let the bidder change addresses on you at the last minute. A thief won't want the actual cardholder to get the merchandise. Send the merchandise to the address that is on the credit card.

Black-market Goods: This can be simplified as the "too good to be true" scheme. The *seller* sells bootlegged music CD's, videos, and computer programs for pennies on the dollar. These items are advertised as the "real deal" but when you get your copy of Microsoft Office 2000, you find it comes without the box, instructions or warranty. Thanks to the advent of CD recorders, this scheme is becoming too common.

Prevention: Beware of anything that's too good to be true. Read the auction description carefully and ask questions. Avoid vague descriptions. Ask if the item comes with the original box. Ask how the seller obtained the software. Do they still have a receipt? Watch out for sneaky phrases like "backup" and "archive." Be especially cautious when buying through Dutch Auctions. Not all are frauds, though, because multiple quantities of an item may have come from liquidation. Use your common sense.

Selling Reproductions and Counterfeits: The *seller* represents a reproduction as the real thing. The seller, himself, may not know the item isn't original.

Prevention: Before you purchase a piece of art, do some research. Find out how much a piece should cost and what the likelihood is of an original being available at the seller's asking price. Since authentication is difficult, it will be up to you to know your items. Ask the seller where he or she got the item, the background of the item, and how long the seller had it. Keep a copy of all responses. Avoid auctions where all sales are final.

Triangulation: This scheme leaves the buyer and a third party holding the bag. In this scheme, the *seller* auctions an item¾ say a laptop computer normally valued at $3,500¾ for $1,500. He offers to ship the computer on approval. If the bidder likes it, he can send the money Western Union. If not, he can send it back without paying¾ no questions asked. How fair and how safe can you get? The bidder happily agrees. The seller then orders the laptop from a company with a stolen credit card and has it shipped to the winning bidder's address. The bidder is thrilled with the new $3,500 laptop and sends the cash immediately. A few days later the police come knocking at the bidder's door, looking for a stolen laptop. The seller is long gone with the cash. Sellers could have multiple winners in a single auction to increase their ill-gotten gains.

Prevention: Don't buy from a seller who only takes cash. If it's too good to be true, it probably is. The seller will be in a rush to get the cash and may ask that you send it Western Union, with no ID required. People fall victim to cons because of their own greed. If you think you are getting one over on someone, you've probably got it backwards. Why the seller is selling at such a low price? Does it make sense? Check the photo¾ don't accept an ad picture. If you've discovered that you've fallen for this scam, call the police and notify the auction site, immediately.

Internet Fencing: The *seller* uses the online auction as an avenue to sell stolen goods. When the police catch on to the thief's activities, they look for the stolen goods and trace them to the buyers. Receiving stolen goods is a crime. Don't get involved.

Prevention: Watch for remarks such as these: "I have easy access to any model of this item." "I work at ***** and can get as many as you want." "I stole (or any similar word) this and can let it go cheap." You get the idea. There is a reason an item sells sharply below cost. For example, I investigated an online auction that promoted $1,000 gift certificates for $750. Why didn't the seller cash in the gift certificates for the full cash amount? Because he purchased the gift certificates with a stolen credit card. Ask the seller where he or she got the item. If the answer is unethical or unclear, stay away.

Buy and Switch: Here the winning *bidder* will swap the item you sent for an identical item that's been damaged or in poorer condition, and then send it back with a complaint.

Prevention: Take excellent photos of your item before you ship. Take note of any nicks or scrapes. Mark the item if you can. For stuffed animals or clothing, you could sew a small colored knot in the seam and photograph that. For other items, you could take a pen with ink that shows up under black light and put a small dot on the bottom. I don't recommend doing this for photos or collectors items, like trading cards. This method doesn't prove that you've been duped, but in small claims court it is a preponderance of evidence that counts. Don't damage the item when you mark it and don't ruin the guaranteed condition.

Loss or Damage Claims: This is not always a scam. Items do get lost or damaged in transit. However, be wary of *bidders* who claim it was so damaged they discarded the item and demand their money back.

Prevention: If an item is sent insured or certified, it can be traced. The recipient must sign the certified letter and an insured item will be covered if it lost or damaged. A bidder who doesn't want to fork over a couple of extra dollars for insurance should be informed in writing that they will be liable. Keep this correspondence for your own protection.

Shell Auctions: The *seller* sets up an auction for the sole purpose of obtaining names and credit cards. There is no merchandise; the seller only wants to take your identity.

Prevention: If your credit card number is stolen you can easily replace it. Credit card companies will charge only $50 and, in some cases, the credit card companies have waived this charge. Nothing is more important than your identity. Never give out your personal identification, such as social security number or driver's license number.

What Can You Do to Protect Yourself?

You can protect yourself from fraud without ruining the fun of online auctions. Remember to stay calm and use common sense. Don't do online what you wouldn't do offline. Some of these tips are buyer or seller specific.

1. Be suspicious of deals that seem too good to be true. They most likely are.
2. Research the auction site. Is there a protection service? Do they offer insurance, guarantees, escrow, or verified identity through a third party? Know the rules and expectations before selling or bidding.
3. Research the desired item. Know the value of the item up for bid. Review the terms of the sale.
4. Avoid buying unseen merchandise when "all sales are final." Ask about return policies and warranties. Get this information in writing, in case you need small claims court to recover your money.
5. Be skeptical of claims about collectibles. Use caution when you come across auctions that are vague in description of the item, but lavish in flash with statements like, "one of a kind," "won't last long!" Glitz is a suspicious substitute for important information¾such as the item's manufacturer, size, color, age, condition, and history. Ask for a detailed description of the item in writing, and walk away from the auction, if the seller's response is vague.
6. Get a clear picture. Don't accept fuzzy photos or even fancy marketing photos or ads from the manufacturer as an indication of the item's condition. Ask! Ask about condition, age, and where the item was purchased. Avoid the auction if the seller is non-responsive.
7. Make sure you understand the waiting period and method of delivery up front and insist that the shipment is insured. Let the seller know if the cost is unreasonable.
8. Check the seller's feedback and ask for referrals to other happy customers. Avoid a seller with negative feedback.
9. If the seller is a business, and not a private individual, you may want to check them out at a consumer protection agency or the Better Business Bureau. Understand that most consumer protection laws, and the government agencies that enforce them, do not address private sales. It could be difficult to resolve problems.
10. Know the other party. Make sure you get a *phone number* and a *physical address*, **not** a PO box. Try the phone number to make sure it is valid before completing the transaction. Never rely on e-mail as your sole source of communication. A valid physical address and phone number will be vital in tracking down the seller if you are scammed. Avoid any seller who is unwilling to provide these.
11. Make sure that you communicate expectations in detail. Let the seller understand that you expect concise communication is return. Most fraud complaints turn out to be miscommunication between the buyer and seller.
12. Be wary of sellers or buyers who use free, anonymous e-mail services such as Hotmail.com, Yahoo.com, etc. It's too easy for fraudsters to use these addresses as fake IDs. It is just good business to know who you are dealing with.
13. Never provide personal information about yourself, such as social security number or driver's license number. There is always the possibility that an auction could be set up for the purpose of stealing identities and credit card numbers.
14. Look out for buyers who seem in a hurry. Fraudsters are anxious to use stolen credit cards before they have been reported stolen. They may even offer a higher price if you will sell the item to them before the auction ends.
15. Do not pay in cash, ever. Cash leaves no trail for the authorities to follow. A request for cash is a clear sign of fraud. Choose a safe payment method like a credit card. If the seller has no merchant ID and cannot take credit cards, or insists on a money order or cashier's check, then use an online escrow service. The service's small fee is a pittance compared to the peace of mind you receive in return. You could arrange COD (cash on delivery), preferably by check made out to the seller, not the post office. That way you can stop payment if necessary.
16. Document all communication with the buyer or seller. Retain all pertinent documents, such as cancelled checks, phone bills, faxes, credit card receipts and statements, receipts and certifications of

authenticity. Print out or save to disk all e-mails. This information will be important in pursuing prosecution or a civil remedy in the case of fraud.

17. Beware of sellers who try to contact you to conduct a private deal. You will lose any protection the auction site may provide.
18. Ship the merchandise to the address listed on the credit card. Fraudsters who steal credit cards want the merchandise to go to them, so they usually change the address with the seller after the transaction is approved. They usually use the ruse that the item is a gift and they want to change to the address of the recipient of the gift.
19. Do not accept multiple payments. A buyer may want to pay ten payments of $150 rather than a $1,500 lump sum. Users of stolen credit cards do this to avoid alerting the credit card company with a large charge.

During the auction make sure that you are professional in all correspondence. This is the correspondence you may submit to the auction site or the authorities. Don't be accusatory; if you think something is amiss be firm but polite. Tell them what you think would be a fair remedy. Consider a third party mediation service provided by the auction site if you can't come to a meeting of minds.

The important thing is for the two parties to try to work it out. Give the other party the benefit of the doubt. The whole issue may be a result of novice error, or misunderstanding. This is a step that is sometimes skipped before people submit negative feedback, which is unfair.

Stick to the issues when posting a negative feedback. There should be no personal shots or remarks about character. State only the facts. Consider the feedback forum as a "community watch." Many eyes will see your feedback. Extreme feedback may be libelous.

Got scammed?

Let's say you've been scammed. What can you do? There are many things, depending on the scheme. But first, take a deep breath and don't panic. Not receiving payment or merchandise is a federal crime under postal laws. The crime is mail fraud. There are a number of different agencies that you can contact, if you've been ripped off. There are some things you can do to get reimbursed for your loss as well. But there are some things that you have to do first.

1. Gather and organize all of your documentation before you contact anyone.
2. Go through your file with objective eyes to check that it will be easily understood.
3. Write a statement, beforehand, so that when you present the complaint to the authorities, or file a complaint in small claims court, your thoughts will be organized.

If you really want to make an impact, pull together an *e-posse* and hit the fraudster where it hurts. For example, in the case you sent money and got nothing in return, contact others who may have been duped by the same fraudster. One San Diego con duped 300 people for $150,000, while the one individual who made the complaint lost only $95. Your molehill could quickly change into a mountain that quickly grabs the attention of the authorities.

Not all scams are ones that would or should be reported to the authorities. All of them should be reported to the auction site.

1. Stay professional when posting negative feedback about a seller. There is no need to make personal attacks. Stick to the issue at hand and only give the facts.
2. You can contact the United States Postal Inspection Service. Once you file a complaint letter with them you will receive a letter of intent to investigate. You can get the address for the appropriate local office online at http://www.framed.usps.com/ncsc/locators/find-is.html or http://www.searchgov.com/. You can also get a mail fraud form in the mail by calling 1-800-275-8777 or print one out online at http://www.usps.gov/postalinspectors/ps8165.pdf.
3. Notify the Federal Trade Commission. The FTC investigates instances of online fraud. You can contact them by phone at 1-877-382-4357 or make a complaint online at http://www.ftc.gov/. If you'd rather contact them by mail, write to Consumer Response Center, FTC, 600 Pennsylvania Avenue, NW, Washington, DC, 20580.

4. The *fastest* way to get relief is to call your local police department as well as the one in the other party's town. You can find the law enforcement agency with the proper jurisdiction by calling directory assistance, or online at http://www.bad-boys.net/.
5. You can also file a complaint with your District Attorney.
6. Contact the seller's Internet Service Provider to let them know you have filed charges.

Want your money back? File in small claims court and include the filing fees in your complaint. The cost to file is minimal, usually between $15 and $50. This can be done even if you have filed criminal charges. If the loss is significant, consider using a collection agency.

It's always better to take preventative measures rather than have to go through the drudgery of recovering your losses. If you have any questions about this type of fraud, you can contact me at Fraudchick@aol.com.