Consumer Reports WebWatch's 'Look Before You Click' Campaign
Detecting and Avoiding Online Auction Fraud

As shown throughout this report, there are myriad ways perpetrators can commit fraud via online auctions. The 2007 Consumer Reports National Research Center survey on eBay measured consumers' experiences with the auction site and explored the issues of scams and deception. Here are some of the key findings:

- Almost half of the respondents who made eBay purchases in the past year said they had experienced at least one type of apparent deceptive practice or scam, ranging from the seller failing to disclose relevant information about the product (15%) and the actual merchandise being significantly different from the seller's description (13%) to more egregious cases, such as finding later an item bid on or purchased was counterfeit (5%).

- Another indication of possible fraud: 6% of those who purchased within the previous year said they participated in an auction that ended because eBay shut it down. That usually happens when fraud occurs.

- After experiencing deceptive practices on eBay, 48% said they would conduct more research on sellers before bidding.

- In response to dishonesty on eBay, the most frequently taken actions to resolve such issues were not necessarily the most effective. Along with percentages that took each action, the table below shows proportions that said it helped to resolve the issue to their satisfaction. Most tried to deal with the seller directly, which eBay does recommend as the first resort. However, not many of those who took this route said that it helped. Reporting the incident to eBay authorities was more effective, although still not always successful. Relatively fewer used eBay's "dispute console," and this helped just over half of the time. Most who filed a formal complaint with PayPal found it helpful. Only 2% actually contacted a law enforcement agency, yielding too small a sample to report effectiveness. (While one in four left negative feedback for the seller, respondents were not asked to evaluate the helpfulness of this action.)

When you experienced this most recent scam or deceptive practice, what actions, if any, did you take to resolve the issue?	**% Who took this action**	**Did the following help to resolve the issue to your satisfaction?***	
	(base = 1119)	**% Yes**	**base**
Tried to resolve the matter with the seller directly	52.9	37.8	574
Reported incident to eBay authorities	42.3	59.9	441
Used eBay's "Dispute Console" to try to resolve the problem	31.0	51.5	330
Filed a formal complaint with PayPal	23.0	66.4	238

* Among those who completed the process

Corrupted Accounts & Bogus Queries

As noted in the case studies, Donna from Brooklyn encountered fraud when she bid for a Bugaboo stroller on eBay and was notified by the seller that apparently a third party had corrupted the seller's account to post a phony sale. Her experiences with fraudulent activity on eBay were not confined to that incident.

Recently she posted an item for sale on the site, then received a message from eBay that her password had been "compromised" and needed to set a new one. Although that message was legitimate, Donna previously had received bogus but authentic-looking messages from parties pretending to be eBay and requesting information from her.

"Oh yeah, I have had negative things happen," Donna recalls. "Can I also point out I've had to change my PayPal password several times in the last few months because it was 'compromised' in some way? I don't know how but eBay informed me of this. I don't even trust them anymore. I got a message recently from someone wanting to buy my baseball cap and I'm like, 'I'm not selling a baseball cap.' This stuff scares me now. Maybe someone is using *my* ID."

Donna's Bugaboo encounter was not an isolated case. An eBay user posted a lengthy alert in the site's Reviews & Guides section entitled, "A SCAM! Bugaboo Strollers & Scam Artists on eBay."

Bugaboo stroller scams often have several traits in common:

- The auction suggests the bidder contact the seller via e-mail first
- The auction lasts for a short period of time, even as little as 24 hours
- The auction is listed as private

The user's posting notes con artists undoubtedly realize Bugaboos are a good target. The posting states: "The bottom line on scams...If a seller seems to be begging you to e-mail privately, it is probably a stolen account." The posting includes detailed advice for avoiding buying Bugaboos and other products through phony sellers; here is a summary of that advice:

- Beware of short auctions for expensive items. Most scammers use one-day or two-day auctions because they are using someone else's account through stolen passwords. They have to make quick sales before the account owner discovers them.

- Beware of "Buy It Now" offers with no "But It Now" button provided by eBay. This is a lure to a request for payment through Western Union. It's hard for scammers to accept PayPal payments -- they have to steal those passwords as well.

- Never agree to "Buy It Now" deals through e-mail conversations.

- Beware of hidden bidder IDs by posting a "Private Auction." Sellers may be preventing others from warning bidders. Any reputable dealer will not hide behind a private auction, and if you as a buyer wish to remain anonymous so you and your purchases are kept private, you can simply request a reputable seller to not give you feedback on the item.

- If you see the same stock or personal picture show up multiple times, this is a red flag. Scammers study successful ads and steal photos.

The eBay Reviews & Guides section also contains a second posting from a user about these strollers entitled "Bugaboo Scam...Don't Buy!" This user recommends buyers do not bid on any auction for a Bugaboo stroller for a "ridiculously low price" if the seller suggests you contact through a ".gmail" account. Last year, MSNBC's Robert Sullivan reported on this trend and noted: "Con artists often try to 'hijack' eBay accounts in order to use them for fraudulent sales. That way, the con artist can take advantage of a legitimate eBay user's good ratings. Hijacking has been going on for years, and it can be as simple as a criminal correctly guessing an obvious password. Criminals also trick users into divulging their passwords, using spam to send out fake 'please update your password' notices that include a link to a look-alike eBay site that's really run by the con artists."

Keep these tips in mind:

- Be very cautious about responding to any e-mail requests from eBay or any other online auction site or financial services company. Such messages may include a request to e-mail or fax information about your address, telephone accounts, or driver's license. In fact, visit the site's "About us" or "Contact us" page and notify the company about the request before you respond.

- Choose your password carefully, and be particularly cautious about using some form of your name, a family member's name, your address, or some other easily identifiable code in your password. Also, do not use the same password for more than one account.

- Always contact the seller before forwarding a payment. If you're using PayPal or an online financial system, verify the seller and the PayPay account are linked to the same account. If you have any doubts, notify the auction site *before* you forward a payment.

- Overstock.com also provides advice about fraud on its site: "Note: Overstock.com Auctions will never ask for personal information in an e-mail. Fraudsters will often imitate the company in legitimate-looking spoof e-mails and request passwords and/or credit card information. If you think you have received a spoof e-mail, do not respond and forward the correspondence to spoof@auctions.overstock.com."

Money Orders That Are Not In Order
For sellers, the biggest risk is shipping a product before funds are in hand. Although money orders are commonly used for many online auctions, they present several challenges.

Dean from Yonkers, N.Y. is an online seller, and he explains that in the case of an Olympus 35mm camera, a bidder sent a message requesting he pay with a money order issued overseas. Luckily, Dean said no, since he had learned of a process whereby buyers "take back" their money order proceeds, rendering such payments worthless.

Even if the money order is valid, it may carry processing fees. An eBay Education Specialist based in Australia offers advice on "The Perils of the Foreign Money Order," noting some banks charge high fees to cash international money orders.

Dean is not alone in avoiding money orders. Joseph from Franklin Square, whose selling experiences were detailed in the case studies section of this report, also avoids this form of payment, having heard about forged money orders from other sellers. In fact, the greatest risk in transacting with money orders—whether issued in the United States or abroad—is forgery.

In 2005, the International Herald Tribune reported "a surge in schemes involving sophisticated counterfeiting of a different form of payment: U.S. postal money orders." Sources at the Federal Bureau of Investigation and postal inspectors cited a new wave of international forgers based in Nigeria, Ghana, and Eastern Europe. For more information about money order security, the U.S. Postal Inspection Service offers money order security tips.

The U.S. Postal Service provides guidance and tips on its Money Order Security Features page, with detailed advice on how to identify official money orders.

The dangers of accepting money orders for online auctions are well documented. In fact, eBay itself has issued a warning for sellers. On its "Today's Scams in Progress" page, eBay provides the following information on what it calls the Fake Money Order Scam:

Scenario:
eBay seller-of-expensive-widget receives message from successful buyer, asking if seller will overnight express the expensive widget, if buyer quickly sends a money order with extra funds for the express shipment. The seller agrees. Money order appears quickly. Seller ships the widget immediately after receipt of the MO. The money order is later found to be fraudulent, and the seller loses both the expensive widget and the money.

Protection:

- *Consider accepting only U.S. Postal Service money orders, since they are more difficult to counterfeit.*
- *If you accept a non-U.S. Postal Service money order, call the issuing bank to make sure the document is legitimate.*
- *Cash your money order, and ship only after you have the dollars in hand.*

From a buyer's perspective, however, the seller's acceptance of checks and/or money orders is usually a good sign. According to the Auction Guild site, keep this in mind:

> *"A check or money order is generally an indication that the seller is legitimate, as the person needs a valid bank account and valid ID to cash such instruments. Since the persons/banks/organizations who cash out these items are at risk of losing their money if they don't validate the authenticity of the seller, the persons/banks/organizations who cash out these items them are likely to take thorough precautions. Combined with the steps in authenticating the seller, it will provide you with a trail to the seller that law enforcement can follow. Because of this, outright scammers will usually not accept payment via check or money order."*

Finally, as one authentication service told Consumer Reports: "If they make it, they fake it." Everything from jewelry to autographed sports memorabilia can be duplicated or knocked off. If the item is important enough, consider using an authentication service.