Appendix II
Best Practices to Prevent Internet Crime

Internet Auction Fraud

Prevention tips:

- Understand as much as possible about how Internet auctions work, what your obligations are as a buyer, and what the seller's obligations are before you bid.
- Find out what actions the website takes if a problem occurs and consider insuring the transaction and shipment.
- Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.
- Examine the feedback on the seller, and use common sense. If the seller has a history of negative feedback then do not deal with that particular seller.
- Determine what method of payment the seller is asking for and where he/she is asking to send payment. Use caution when the mailing address is a post office box number.
- Be aware of the difference in laws governing auctions between the U.S. and other countries. If a problem occurs with the auction transaction that has the seller in one country and a buyer in another, it might result in a dubious outcome leaving you empty handed.
- Be sure to ask the seller about when delivery can be expected and warranty/exchange information for merchandise that you might want to return.
- To avoid unexpected costs, find out if shipping and delivery are included in the auction price or are additional.
- Finally, avoid giving out your social security number or driver's license number to the seller, as the sellers have no need for this information.

Steps to take if victimized:

1. File a complaint with the online auction company. In order to be considered for eBay's Fraud Protection Program, you should submit an online Fraud Complaint at http://crs.ebay.com/aw-cgi/ebayisapi.dll?crsstartpage 90 days after the listing end-date.
2. File a complaint with the Internet Crime Complaint Center (http://www.ic3.gov).
3. Contact law enforcement officials at the local and state level (your local and state police departments).
4. Also contact law enforcement officials in the perpetrator's town & state.
5. File a complaint with the shipper USPS, UPS, Fed-Ex, etc.
6. File a complaint with the National Fraud Information Center (http://www.fraud.org/info/contactnfic.htm).
7. File a complaint with the Better Business Bureau (http://www.bbb.org).

Non-Delivery of Merchandise

Prevention tips:

- Make sure you are purchasing merchandise from a reputable source. As with auction fraud, check the reputation of the seller whenever possible, including the Better Business Bureau.
- Try to obtain a physical address rather than merely a post office box and a phone number. Also call the seller to see if the number is correct and working.
- Send them e-mail to see if they have an active e-mail address. Be cautious of sellers who use free e-mail services where a credit card wasn't required to open the account.
- Investigate other websites regarding this person/company.
- Do not judge a person/company by their fancy website; thoroughly check the person/company out.
- Be cautious when responding to special offers (especially through unsolicited e-mail).
- Be cautious when dealing with individuals/companies from outside your own country. Remember the laws of different countries might pose issues if a problem arises with your transaction.
- Inquire about returns and warranties on all items.
- The safest way to purchase items via the Internet is by credit card because you can often dispute the charges if something is wrong. Also, consider utilizing an escrow or alternate payment service, after conducting thorough research on the escrow service.
- Make sure the website is secure when you electronically send your credit card numbers.

Credit Card Fraud

Prevention tips:

- Don't give out your credit card number(s) online unless the website is both secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but may provide you some assurance.
- Before using a site, check out the security software it uses to make sure that your information will be protected.
- Make sure you are purchasing merchandise from a reputable/legitimate source. Once again investigate the person or company before purchasing any products.
- Try to obtain a physical address rather than merely a post office box and a phone number. Call the seller to see if the number is correct and working.
- Send them e-mail to see if they have an active e-mail address and be wary of sellers who use free e-mail services where a credit card wasn't required to open the account.
- Do not purchase from sellers who won't provide you with this type of information.
- Check with the Better Business Bureau to see if there have been any complaints against the seller before.
- Check out other websites regarding this person/company.
- Be cautious when responding to special offers (especially through unsolicited e-mail).
- Be cautious when dealing with individuals/companies from outside your own country.
- If you are going to purchase an item via the Internet, use a credit card since you can often dispute the charges if something does go wrong.
- Make sure the transaction is secure when you electronically send your credit card numbers.
- You should also keep a list of all your credit cards and account information along with the card issuer's contact information. If anything looks suspicious or you lose your credit card(s) contact the card issuer immediately.

Prevention tips for Businesses:

- Do not accept orders unless complete information is provided (including full address and phone number). Require address verification for all of your credit card orders. Require anyone who uses a different shipping address than their billing address to send a fax with their signature and credit card number authorizing the transaction.
- Be especially careful with orders that come from free e-mail services -- there is a much higher incidence of fraud from these services. Many businesses won't even accept orders that come through these free e-mail accounts anymore. Send an e-mail requesting additional information before you process the order asking for: a non-free e-mail address, the name and phone number of the bank that issued the credit card, the exact name on credit card, and the exact billing address.
- Be wary of orders that are larger than your typical order amount and orders with next day delivery.
- Pay extra attention to international orders. Validate the order before you ship your product to a different country.
- If you are suspicious, pick up the phone and call the customer to confirm the order.
- Consider using software or services to fight credit card fraud online.
- If defrauded by a credit card thief, you should contact your bank and the authorities.

Investment Fraud

Prevention tips:

- Do not invest in anything based upon appearances. Just because an individual or company has a flashy website doesn't mean it is legitimate. Web sites can be created in just a few days. After a short period of taking money, a site can vanish without a trace.
- Do not invest in anything you are not absolutely sure about. Do your homework on the investment to ensure that it is legitimate.
- Thoroughly investigate the individual or company to ensure that they are legitimate.
- Check out other websites regarding this person/company.
- Be cautious when responding to special investment offers (especially through unsolicited e-mail) by fast talking telemarketers. Know whom you are dealing with!
- Inquire about all the terms and conditions dealing with the investors and the investment.
- Rule of Thumb: If it sounds too good to be true, it probably is.

Nigerian Letter Scam/419 Scam

Prevention tips:

- Be skeptical of individuals representing themselves as Nigerian or other foreign government officials asking for your help in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- Do not give out any personal information regarding your savings, checking, credit, or other financial accounts.
- If you are solicited, do not respond and quickly notify the appropriate authorities.

Business Fraud

Prevention tips:

- Purchase merchandise from reputable dealers or establishments.
- Try to obtain a physical address rather than merely a post office box and a phone number, and call the seller to see if the number is correct and working.
- Send them e-mail to see if they have an active e-mail address and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Do not purchase from sellers who won't provide you with this type of information.
- Purchase merchandise directly from the individual/company that holds the trademark, copyright, or patent. Be aware of counterfeit and look-alike items.
- Beware when responding to e-mail that may not have been sent by a reputable company. Always investigate before purchasing any products.

Identity Theft

Prevention tips:

- Check your credit reports once a year from all three of the credit reporting agencies (Experian, Transunion, and Equifax)
- Guard your Social Security number. When possible, don't carry your Social Security card with you.
- Don't put your Social Security Number or driver's license number on your checks.
- Guard your personal information. You should never give your Social Security number to anyone unless they have a good reason for needing it.
- Carefully destroy papers you discard, especially those with sensitive or identifying information.
- Be suspicious of telephone solicitors. Never provide information unless you have initiated the call.
- Delete any suspicious e-mail requests without replying.

Steps to take if victimized:

1. Contact the fraud departments of each of the three major credit bureaus and report that your identity has been stolen.
2. Get a "fraud alert" placed on your file so that no new credit will be granted without your approval.
3. Contact the security departments of the appropriate creditors and/or financial institutions for any accounts that may have been fraudulently accessed. Close these accounts. Create new passwords on any new accounts that you open
4. File a report with your local police and/or the police where the identity theft took place.
5. Retain a copy of the report because it may be needed by the bank, credit card company, or other businesses to prove your innocence.

Cyberstalking

Prevention tips (from W.H.O.A – Working to Halt Online Abuse at www.haltabuse.org):

- Use a gender-neutral user name/e-mail address.
- Use a free e-mail account such as Hotmail (www.hotmail.com) or YAHOO! (www.yahoo.com) for newsgroups/mailing lists, chat rooms, Instant messages (IMs), e-mails from strangers, message boards, filling out forms and other online activities.
- Don't give your primary e-mail address to anyone you do not know or trust.
- Instruct children to never give out their real name, age, address, or phone number over the Internet without your permission.

- Don’t provide your credit card number or other information as proof of age to access or subscribe to a website you’re not familiar with.
- Lurk on newsgroups, mailing lists and chat rooms before “speaking” or posting messages.
- When you do participate online, be careful – only type what you would say to someone’s face.
- Don’t be so trusting online – don’t reveal personal things about yourself until you really and truly know the other person.
- Your first instinct may be to defend yourself – Don’t – this is how most online harassment situations begin.
- If it looks to good to be true – it is.