

Operation E-Con

Executive Summary

Operation E-Con is a coordinated initiative focusing on significant Cyber Crime activity both in the United States and a number of other countries across the Globe. The events highlighted in Operation E-Con, represent the culmination of significant investigative activity on the part of Federal, State and Local law enforcement agencies over the last five months. The packaging of this investigative initiative is also intended to illustrate that, despite the appropriate heightened attention given to the war on terrorism and the war to liberate Iraq, serious criminal activity facilitated through the Internet remains a high priority for law enforcement and our companion regulatory agencies.

This initiative has been coordinated at the Federal Level between the Dept of Justice, the FBI, the U.S Postal Inspection Service the U.S Secret Service and the Federal Trade Commission. A myriad of State and Local law enforcement agencies have played a substantial role in advancing many of the investigations highlighted in this Operation, towards successful resolution. The National White Collar Crime Center (NW3C) also facilitated participation of State and Local law enforcement in this noteworthy initiative.

A substantial portion of the activity reflected in Operation E-Con is attributable to numerous Cyber Crime Task Forces that have been established across the United States over the past year. The growing number of these task forces further underscores, not only the priority afforded to cyber crime, but the increasing acknowledgement that a team approach is most effective in charting a course of impact pertaining to Cyber Crime.

The events included in this initiative also illustrates how significant investigative progress can be achieved by extending our task forces to include key representatives of industry, both in identifying evolving schemes early, and in crafting an aggressive proactive counter-attack. A number of the investigations highlighted today were initiated and/or substantially advanced through these partnerships. Industry associations providing noteworthy input include: the Recording Industry Association of America (RIAA), the Business Software Alliance (BSA), the Software and Information Industry Association (SIIA), the Motion Picture Association of America (MPAA) and the Merchants Risk Council (MRC).

Although the investigations highlighted today are substantial in number, with more than 90 investigations, involving 89,000 victims and estimated losses or more than \$176 million dollars, these activities represent only a snapshot of the scope of the ongoing Cyber Crime investigations. Significant activities included in Operation E-Con include the execution of 73 Search and Seizure warrants, and the formal charging or conviction of more than 130 individual subjects.

Common Internet Crime Schemes

Online Auction/Retail

Misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Non-delivery of Goods/Services

The non-delivery of goods or services which were purchased or contracted remotely through the Internet, independent of an Internet auction.

Identity Theft

Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an email solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting.

Credit/Debit Card Fraud

The unauthorized use of a credit/debit card, or card number, to fraudulently obtain money or property. Credit/debit card numbers can be stolen from unsecured web sites, or can be obtained in an identity theft scheme.

Freight Forwarding/Reshipping

Involves the receipt and subsequent repackaging and reshipping of merchandise, often to countries outside the United States. Individuals are often solicited to participate in this activity in chat rooms, or through Internet job postings. Unbeknownst to the reshipper, the merchandise has been paid for with fraudulent credit cards, likely obtained via identity theft.

Counterfeit Check Schemes

The use of a counterfeit cashier's check or corporate check to pay for merchandise. Often these checks are made out for a substantially larger amount than the purchase price. The victims are instructed to deposit the check and return the overage amount, usually by wire transfer, to a foreign country. Because banks may release funds from a cashier's check before the check actually clears, the victim believes the check has cleared and wires the money as instructed.

Business/Employment Schemes

This scheme typically involves identity theft, freight forwarding, and counterfeit checks. The subject's post a help-wanted ad on popular Internet job search sites. Respondents are required to fill out an application wherein they divulge sensitive personal information, such as their date of birth and Social Security number. Subsequently, unbeknownst to the respondent, the subject uses that personal information to obtain credit in the respondent's name. After establishing credit, the subject begins using the credit to purchase merchandise via the Internet.

This scheme now transitions to the freight forwarding phase, commonly known as the "re-shipper." In keeping with the subject's fraudulent business scheme, the respondent who was hired to forward packages to his employer, who incidentally is abroad, now awaits for the packages arrival. Once the packages arrive, the reshipper dutifully forwards the packages as instructed by his/her employer.

The counterfeit check aspect occurs when the respondent, now the "employee," is paid for services rendered. The employee will be provided with a fraudulent check which is issued from another company or a fraudulent cashier's check issued from a bank in the United States. The subject explains this oddity by indicating that those businesses owed him or her money. Usually the check is issued for an amount in excess of the amount due the employee. The employee is instructed to negotiate the check and wire the excess funds to a bank in the subject's country.

Spoofing

A technique whereby a subject pretends to be someone else's email or web site. This is typically done by copying the web content of a legitimate company onto a web site of the subject's own creation. Instead of actually typing in the legitimate business's Uniform Resource Locator (URL), the victim is given a hyperlink, usually in an email, that directs the victim to the fraudulent site. However, upon seeing the content, the victim believes they are dealing with a familiar business and is tricked into divulging sensitive personal information. Spoofing is done to further perpetrate other schemes, including identity theft and auction fraud.

Phony Escrow Services

In an effort to persuade a wary Internet auction participant, the fraudster will propose the use of a third-party escrow service to facilitate the exchange of money and merchandise. The victim is unaware the fraudster has spoofed a legitimate escrow service. The victim sends payment or merchandise to the phony escrow and receives nothing in return.

Advance-Fee Fraud Schemes

A victim is required to pay significant fees in advance of receiving a substantial amount of money. The fees are usually passed off as taxes, or processing fees, or charges for

notarized documents. The victim pays these fees and receives nothing in return. Perhaps the most common example of this type of fraud occurs when a victim is expecting a large payoff for helping to move millions of dollars out of a foreign country. The victim may also believe he has won a large award in a nonexistent foreign lottery.

Investment Fraud

An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities.

Ponzi/Pyramid Schemes

An investment scheme in which investors are promised abnormally high profits on their investments. No investment is actually made. Early investors are paid returns with the investment money received from the later investors. The system usually collapses; the later investors do not receive dividends and lose their initial investment.

[See .ppt array, slide 2]

[See .ppt array, slide 3]

[See .ppt array, slide 4]

Sampling of Investigations from Operation E-Con:

The following cases are a sampling of the investigations that are a part of this initiative. Some of the information has been generalized due to the on-going nature of some of the investigations.

Identity Theft

On February 11, 2002, FBI-Baltimore received a complaint regarding spam which purported to be from Bank of America (BoA) asking people to provide their financial information through a web site. Neither the spam nor the web site were authorized by BoA. Approximately two weeks later, a similar complaint was received from Wells Fargo Bank. In addition, Wells Fargo subsequently provided the names of specific customers who responded to the spam and had subsequent unauthorized attempts to access their bank account.

FBI-Baltimore initiated an investigation based on the above complaints and identified a subject in New York by tracing the source of the spam, by tracing the origination of the Web site that captured the financial information, and through the email accounts which subsequently received this information. In addition, valid credit card numbers and personal identification information from hundreds of victims was found on the subject's computer.

Investigation, further established that a resident of Portugal had purchased the financial information from the subject. This accomplice then withdrew money from the Wells Fargo customers' accounts at ATM's in Portugal and Germany.

The subject was indicted under a sealed indictment on 5/8/2003 on charges of wire fraud. A sealed warrant was also issued for his arrest. On 10/11/2002, the Portuguese Judicial Police formally filed a criminal complaint against the accomplice with the Judicial Court in Silves, Portugal, for financial institution fraud. Actual losses from this scheme are approximately \$200,000, with 357 victims.

SPAM - Denial of Service

The Internet service provider, EarthLink, of Atlanta, GA, while conducting an internal investigation, determined that the subject was sending over one million SPAM email messages per day. The subject is believed to have sent over 825 million SPAM e-mails over the Internet. He created 324 false EarthLink accounts using alias identities and stolen credit card bank account information. EarthLink contacted members of the Buffalo Cyber Task Force (BCTF). EarthLink estimates their losses at over \$15,000,000.

The participating BCTF agencies are the FBI, the New York State Attorney General's Office (NYSAGO), and the New York State Police (NYSP).

Investment Fraud

From June 2002 to January 2003, a website called EZ-BUCKS offered a high yield loan program promising returns at 2% per day, 200% after 30 days, or 300% after 30 days with a minimum investment of \$5,000. The website collected approximately \$4,700,000 from 5,700 individuals throughout the world through this scheme. Investments were made using an electronic currency called E-Gold. Investigation to date has revealed that Charles Mark Maxey, formerly residing in San Diego, California, operated the EZ-BUCKS website. Three seizure warrants have been executed yielding a 2003 Jaguar XK8 (\$94,000), cash (\$9,864) and a 2003 Jeep Cherokee (\$37,000), as part of this initiative.

Cyberhook Nexgen

CYBERHOOK NEXGEN, is an on-line undercover operation targeting subjects who profit from the illegal sale of copyright protected software, games and movies. Over 250 commercial software, games, and movie titles were available for purchase at www.powerbackup.net. Prices for those items were far below their true retail value. Subsequent to the items purchase, the customer was instructed by e-mail to complete the purchase via one of numerous on-line payment services. Investigation was able to substantiate that the illegally sold software, games and movies had a retail value in excess of \$10 million. (FBI, USCS-BICE)

Reshippers

On March 8, 2003 one subject entered a plea of guilty to one count of criminal conspiracy in U.S. District Court, Northern District of Texas, Ft. Worth Division, in connection with his involvement in an international reshipper scheme.

The investigation was predicated upon receipt of information regarding a nation-wide Internet fraud scheme, in which Internet orders were placed with major retailers across the United States using fraudulently obtained credit card numbers. The exposure nation wide is currently estimated at over \$20 million dollars.

The orders were placed via the Internet from locations in Ghana, Nigeria, and Gambia. The merchandise in each case was shipped to addresses within the United States, repackaged, and reshipped to Ghana.

As the investigation progressed, it was discovered that at least 460 orders, valued at \$79,599.01 were placed with over 35 retailers for shipment to the subject at his Arlington, Texas apartment. It was also determined the subject, a Ghanaian National, had overstayed his visa which expired April 2000, and was in the U.S. illegally.

Federal Bureau of Investigation, and the Bureau of Customs Enforcement participated in the investigation.

Investment Fraud

Subject doing business as J&K Global Marketing, defrauded 23,000 investors in an Internet offshore rent/mortgage fee program. Utilizing the Internet, the subject solicited "membership" fees of \$375 and eventually, he collected more than \$8 million in investments. The subject claimed that the investor's fees were being invested in a "high yield program." The subject also claimed that J&K had been in the trading business for over twelve years, when in actuality that was not the case. On March 25, 2003, a fifteen count indictment was returned against the Subject of this investigation.

The USFIS, and FBI participated in this investigation.

Romanian Auction Fraud

This investigation involves 5 Romanian citizens who conducted fraudulent Ebay auctions selling high-end electronic goods. The scheme used "Bogus Bidders" in order to inflate the auction price. At the conclusion of the auctions the winning bidders (Victims) were instructed to send payment via Western Union, or Moneygram. Western Union and Moneygram records indicate over \$150,000.00 from 64 American citizens was absconded as

a result of this scheme. The perpetrators of this fraud also purchased expensive electronic goods via the Internet using counterfeit checks, and stolen credit cards.

On February 26, 2003 four subjects were convicted by the local Penal Court from Timisoara, Romania and sentenced to 3 years incarceration, and ordered to pay restitution to American victims in the amount of \$43,200.00.

One subject, an intelligence officer in the SRI, (Romanian Domestic Intelligence Bureau) was also charged as a result of this investigation, and will be afforded a trial by a military court at a later date.

The following law enforcement agencies participated in the investigation: General Directorate of Counter Organized Crime, Bucharest, Romania, United States Secret Service, Bucharest Office, FBI, Internet Fraud Complaint Center.

Investment Fraud

Two subjects were successfully extradited from Costa Rica after being indicted for their involvement with the Tri-West Investment Club, an Internet-based investment fraud scheme that allegedly netted more than \$60 million from 15,000 investors worldwide. The fraudulent on-line web site solicited investments in "prime bank notes", with promises of an annualized rate of return of 120 percent. The investors were also to receive substantial referral fees of 15 percent per referred investment. The fraudulent web site listed alleged testimonials describing instant wealth and that all investments were 'guaranteed.'

When the subjects were arrested in Costa Rica, Costa Rican authorities seized and froze nearly \$15 million dollars in assets, including 7 million held in bank accounts and millions more in real properties and assets such as a yacht, helicopter, nineteen (19) new vehicles, expensive jewelry and houses.

The FBI, IRS and Costa Rican Law enforcement participated in the investigation.

Investment Fraud

Subject in this investigation established a sophisticated investment fraud scheme, utilizing Medwireless, a company that purports to manufacture medical diagnostic devices capable of transmitting images over the Internet. The scheme was aided in part by telemarketers and mass mailing service companies, that were enlisted by the subject to market Medwireless stock to potential investors, by providing false representations about Medwireless product success and current usage by certain prestigious Medical Institutions. The scheme was further aided through the use of a professional looking website, which potential investors were directed to visit. The subject established control over Medwireless through certain holding companies, to conceal his direct involvement in the scheme. Losses in the matter exceed \$5 million, obtained from approx 150 separate investors. (FBI Los Angeles)



- ▶ HOME
- ▶ ABOUT US
- ▶ PRODUCTS & SERVICES
- ▶ COMPANY NEWS
- ▶ FAQs
- ▶ CONTACT INFORMATION

Physician Login

U

P

LOGIN

Medical Solutions For The Wireless Age

med wireless



MED *wireless* - new technology

[See .ppt array, slide 5]

Internet Pharmacy

The subjects utilized the internet website, www.success123.com, in order to facilitate the distribution of \$2.2 million dollars worth of pharmaceutical drugs without a prescription or any doctor/patient interaction. A wide variety of drugs to include Oxycontin, Valium, and Xanax were dispensed via the website. Two subjects to include the owner of the website pled guilty to federal charges in January 2003. Another subject is scheduled to plead guilty in May 2003. The FBI, FDA, and DEA participated in the investigation.

Russian Bride Scheme

Subjects posted ads purportedly from women living in Russia looking for relationships with men from other countries. Men who replied would receive email from the women initiating a relationship which would develop very quickly. The women would call to explain that she wants to come to the country of the man, but she has no money and does not know the procedures or paperwork to complete. A dating agency that is willing to take care of all the necessary paperwork and coordination for a small fee, would then correspond with the man.

If the man sends the money, they are told that the woman is arriving on a certain date, however before the date of arrival, the man receives an urgent email or telephone call

regarding a new problem requiring more funds. Regardless of whether the man sends money or not, he never hears from the woman or agency again.

Estimates indicate that there are over 400 victims, who lost approximately \$3000 each. The estimated damage is over \$600,000. Indictments and arrests in addition to the execution of a search warrant have been coordinated in conjunction with Operation E-Con. San Diego FBI.



*** The above photos have not been specifically tied to criminal conduct that has been charged at this point.*

Identity Theft

Subject while employed in the credit processing department of a large retail department store obtained information from customers applying for a store credit account. Using the stolen customer information, the subject opened numerous fraudulent accounts for himself and established credit with the information he received. He used Post Office boxes in various states to accept mail for the various identities he was using. The subject operated a “business” in which one of his false identities would make purchases from another one of his false identities. He used some of the identities to establish credit in order to make large purchases. In the attempt to avoid detection the subject would use others to pick up his mail at different locations. There were over 130 victims involved in this case with an estimated loss of \$1.3 million. At the time of his March 2003 arrest, the subject possessed several passports in various names and countries.

The following agencies participated in the investigation: FBI, USPIS, Cherokee Georgia Sheriff’s Office, Cobb County Georgia Sheriff’s Office, and Floyd County Georgia Sheriff’s Office.

Identity Theft

The subject, an active duty military person who had access to private information as a result of his classification, and his wife, were recently indicted by a Houston County Georgia Grand Jury on charges of Financial Identity Fraud. The subjects fraudulently obtained numerous charge accounts using the victims' names and Social Security numbers. The subjects were able to obtain cell phones, charge accounts for computers, and credit cards for illicit use.

Approximately fifty people, from several different states were victimized as well as at least ten major corporations where accounts were obtained. To facilitate the fraudulent scheme, the subjects used a wide number of electronic names, email addresses, and obtained Internet service through the theft of victims' identities. The estimated loss is over \$100,000.

The Warner Robbins Police Department, and District Attorneys Office are participating in the investigation/prosecution of this matter.

Work at Home Scheme

An Internet work at home scheme affecting over 40,000 victims was shut down through a cooperative effort between the U.S. Postal Inspector Service and the Federal Trade Commission. Subjects in this case offered work at home employment opportunities through a variety of media, including direct mail, classified advertisements in newspapers, and internet web sites. Subjects requested a registration fee of \$45 to be paid for the potential to earn \$720 to \$2,000 per week working at home. The Federal Trade Commission filed a complaint and in a final judgment, subjects were ordered to pay \$221,620 in equitable monetary relief to be placed into a fund administered by the FTC. The subjects entered a plea of guilty to Mail Fraud on May 12, 2003.

Auction Fraud

This case involves two subjects who acted as the president and/or registered agent for several businesses in Southern California. The subjects acted as primary sellers and distributors of counterfeit merchandise. Between August 2000 and March 2003, the subjects sold large quantities of counterfeit merchandise through eBay using various seller IDs and contact information. Over \$145,000 in sales were conducted on eBay using five different seller IDs, thirty different email addresses and thirteen different physical addresses. Losses in this case are over \$700,000. In a cooperative effort between the U.S. Postal Inspector Service, and the Internal Revenue Service, Search Warrants were executed in March of 2003. Arrest Warrants for the subjects were issued the week of 5/12/2003.

Case Illustrations:

[See .ppt array, slide 6]

[See .ppt array, slide 7]

[See .ppt array, slide 8]

[See .ppt array, slide 9]

[See .ppt array, slide 10]

[See .ppt array, slide 11]

[See .ppt array, slide 12]

FTC Auction Fraud Tips. (from the FTC.gov “Facts for Consumers”)

Tips for Buyers...

Despite complaints of fraud, online auctions remain a fun, efficient and relatively safe way to do business - if you act prudently. Here's how:

Before Bidding

- Become familiar with the auction site. Never assume that the rules of one auction site apply to another. If the site offers a step-by-step tutorial on the bidding process, do it. It may save you frustration and disappointment later.
- Find out what protections the auction site offers buyers. Some sites provide free insurance or guarantees for items that are undelivered, not authentic or not what the seller claimed.
- Know exactly what you're bidding on. Read the seller's description of the item or service, and if a photograph is posted, look at it. Read the fine print. Look for words like "refurbished," "close out," "discontinued," or "off-brand" - especially when shopping for computer or electronic equipment - to get a better idea of the condition of the item being auctioned.
- Try to determine the relative value of an item before you bid. Be skeptical if the price sounds too low to be realistic. "Brick-and-mortar" stores and price comparison sites may be good for reality checks.
- Find out all you can about the seller. Avoid doing business with sellers you can't identify, especially those who try to lure you off the auction site with promises of a better deal. Be aware that some fraudulent sellers may use a forged email header that makes follow-up difficult, if not impossible. Get the seller's telephone number so that you have another way to get in touch. Dial the number to confirm that it is correct. Some auction sites post feedback ratings of sellers based on comments by other buyers. Check them out. Although these

comments and ratings may give you some idea of how you'll be treated, know that sometimes, comments may be submitted by the seller or "shills" paid by the seller.

- Consider whether the item comes with a warranty and whether follow-up service is available if you need it. Many sellers don't have the expertise or facilities to provide services for the goods they sell. If this is the case with your seller, be sure you're willing to forfeit that protection before placing a bid.
- Find out who pays for shipping and delivery. Generally, sellers specify the cost of shipping and give buyers the option for express delivery at an additional cost. If you're uncertain about shipping costs, check with the seller before you bid.
- Check on the seller's return policy. Can you return the item for a full refund if you're not satisfied with it? If you return it, are you required to pay shipping costs or a restocking fee?
- Email or call the seller if you have any questions. Don't place any bids until you get straight - and satisfactory - answers.

When Bidding

- Establish a top price and stick to it. This can help ensure that you get a fair price and protect you from "shill bidding." Don't bid on an item you don't intend to buy. If you're the highest bidder, you're obligated to follow through with the transaction. Some auction sites bar "non-paying" bidders, also known as "deadbeats," from future bidding.
- Save all transaction information. Print the seller's identification; the item description; and the time, date and price you bid on the item. Print and save every email you send and receive from the auction company or the seller.

Before Paying

- Know and understand what form of payment the seller accepts. If the seller accepts only cashier's checks or money orders, decide whether you're willing to risk sending your payment before you receive the product.
- Protect your privacy. Never provide your Social Security number, driver's license number, credit card number, or bank account information until you have checked out the seller and the online payment or escrow service, if you're using one, to ensure legitimacy.
- If the seller insists on using a particular escrow or online payment service you've never heard of, check it out. Visit its Web site. A site that is generally of poor quality with, say, misspelled words or claims that the service is affiliated with the government, is suspect. Call the customer service line. If there isn't one or if you call and can't reach someone, don't use the service.
- Before you agree to use any online payment or escrow service, read the service's terms of agreement:
 - If it's an online payment service, find out whether it offers buyers any recourse if sellers don't keep their end of the bargain, whether it prevents sellers from accessing their funds if buyers are not satisfied with the product, and who is responsible for paying for credit card charge backs or transaction reversal requests. If the online payment service cannot recover the loss from the seller, it might try to recover its loss from you, using the credit card or bank account information in its file. To limit your exposure, consider reserving a separate credit card, stored-value card or bank account to use just for online transactions.
 - Examine the online payment and escrow service's privacy policy and security measures. Never disclose financial or personal information unless you know why it's being collected, how it will be used, and how it will be safeguarded.

- Be suspicious of an online escrow service that cannot process its own transactions and requires you to set up accounts with online payment services. Legitimate escrow services never do this.
- Check with the Better Business Bureau, state attorney general or consumer protection agency - where you live and where the online payment or escrow service is based - to see whether there are any unresolved complaints against the service. Keep in mind that a lack of complaints doesn't necessarily mean that a service has no problems.

Tips for Sellers...

Know Your Legal Obligations

- Under federal law, you're required to advertise your product or service and the terms of the sale honestly and accurately. You can't place "shill" bids on your item to boost the price or offer false testimonials about yourself in the comment section of Internet auction sites.
- You're prohibited from auctioning illegal goods. While many auction sites monitor their sites to ensure that illegal items are not being offered, the responsibility for ensuring that a sale is legal rests with the seller and buyer. Some auction sites post a list of prohibited items as a guide.
- You are required to ship merchandise within the time frame specified during the auction, or, if a time frame is not specified, within 30 days. If you can't meet the shipping commitment, you must give the buyer an opportunity to cancel the order for a full refund or agree to the new shipping date. To learn more about your responsibilities when shipping products, see [*A Business Guide to the Federal Trade Commission's Mail or Telephone Order Merchandise Rule.*](#)

Advertising Your Product

- When describing your item and its condition, state whether it's new, used or reconditioned.
- Anticipate questions buyers might have and address them in the description of your item or service.
- When possible, include a photograph of the item. The saying that a picture is worth a thousand words is especially relevant in Internet auctions.
- Specify the minimum bid at the lowest fair price you're willing to accept.
- Specify who will pay for shipping, and note whether you'll ship internationally.
- State your return policy, including who's responsible for paying for shipping costs or restocking fees if the item is returned.
- Let prospective bidders know whether you provide follow-up service; if you don't, tell them where they can get it.

Dealing with Bidders

- Respond as quickly as possible to bidders' questions about the item you're auctioning or the sales terms.
- When the auction closes, print all information about the transaction, including the buyer's identification; a description of the item; and the date, time and price of the bid. Save a copy of every email you send and receive from the auction site or the successful bidder.
- Contact the "winning" bidder as soon after the auction closes as possible; confirm the final cost, including shipping charges, and tell the buyer where to send payment.

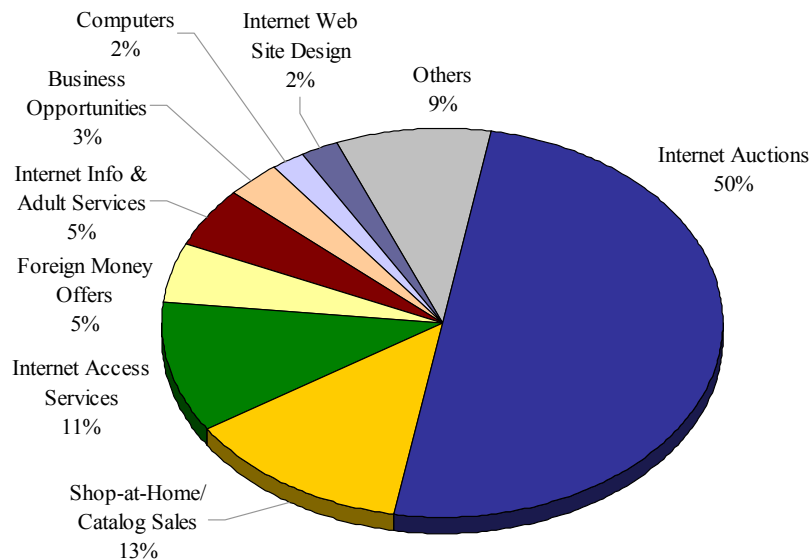
Arranging for Payment

- If you accept credit card payments from the buyer directly, bill the credit card account only once you've shipped the product.

- If a buyer insists on using a particular escrow or online payment service that you've never heard of, check it out. Visit its Web site. Be suspicious of claims about being affiliated with a government agency. Call the customer service line. If there isn't one, or if you call and can't reach someone, don't use the service.
- Before agreeing to use an online payment or escrow service, read the terms of agreement:
 - If it's an online payment service, find out who pays for credit card charge backs or transaction reversal requests if the buyer seeks them.
 - Examine the service's privacy policy and security measures. Never disclose financial or personal information unless you know why it's being collected, how it will be used, and how it will be safeguarded.
- Be suspicious of an online escrow service that cannot process its own transactions and requires you to set up accounts with online payment services. Legitimate escrow services never do this.
- Check with the Better Business Bureau, state attorney general or consumer protection agency - where you live and where the online payment or escrow service is based - to see whether there are any unresolved complaints against the service. Be mindful that a lack of complaints doesn't necessarily mean that the service has no problems.



**Top Products/Services for Internet-Related Fraud Complaints¹
Received by the Federal Trade Commission
January 1 – December 31, 2002**



Definition of "Internet-related": A fraud complaint is "Internet-related" if: it concerns an Internet product or service, the company initially contacts the consumer via the Internet, or the consumer responds via the Internet.

¹Percentages are based on the total number of Internet-related fraud complaints (102,517) received between January 1 and December 31, 2002.

Going Shopping? Go Global! A Guide for E-Consumers.

Shopping online opens up a whole world of goods and services. With the simple click of a computer mouse, you can order tulip bulbs directly from Holland, exotic spices from Turkey or handwoven wall hangings from Mexico or Morocco.

The World Wide Web has expanded the international marketplace in a way never before possible, giving consumers unlimited choices.

But shopping electronically-especially when you're dealing with vendors in other countries-opens up a whole world of questions. Are the prices posted in U.S. dollars or some other currency? Does the company ship internationally? How long will it take for an order to be delivered? Will unexpected taxes or duties be added to the price? If there's a problem, where can you get it resolved?

The Federal Trade Commission offers these tips to help you when you "go global":

1. Know who you're dealing with.

Do some homework to make sure a company is legitimate before doing business with it. Identify the company's name, its physical address, including the country where it is based, and an e-mail address or telephone number, so you can contact the company with questions or problems. And consider dealing only with vendors that clearly state their policies. Is the company affiliated with industry groups, seal programs or other self-regulatory programs you trust?

2. Know what you're buying.

Look for accurate, clear and easily accessible information about the goods or services being offered, and contact the company to clear up any questions before you place an order.

3. Understand the terms, conditions and costs involved in the sale.

Find out up front what you're getting for your money-and what you're not. Get a full, itemized list of costs involved in the sale, with a clear designation of the currency involved, terms of delivery or performance, and terms, conditions and methods of payment.

Look for information about restrictions, limitations or conditions of the purchase; instructions for proper use of products, including safety and health care warnings; warranties and guarantees; cancellation, return, or refund policies; and the availability of after-sale service.

4. Protect yourself when paying online.

Look for information posted online that describes the company's security policies, and check whether the browser is secure and encrypts your personal and financial information during online transmission. That makes the information less vulnerable to hackers.

5. Look out for your privacy.

All businesses require information about you to process an order. Some use it to tell customers about products, services or promotions, but others share or sell the information to other vendors-a practice with which you may not be comfortable.

Shop only from online vendors that respect your privacy. Look for the vendor's privacy policy on the web site. The policy statement should reveal what personal identifying information is collected about you and how it will be used, and give you the opportunity to refuse having your information sold or shared with other vendors. It also should tell you whether you can correct or delete information the company already has about you.

6. Understand what recourse you have if you run into problems with your purchase.

Do business only with companies that state their commitment to customer satisfaction and their policy to resolve consumer complaints or difficulties quickly and fairly, without imposing excessive charges or inconvenience.

7. **Get smart about e-commerce. Demand consumer-friendly policies and procedures.** Look for information from businesses, consumer representatives and governments about your rights and responsibilities when you participate in international electronic commerce. Take an active role in advancing an electronic marketplace that promotes fair and effective policies and procedures that protect businesses as well as consumers.

A Checklist

Is the business you're buying from "consumer-friendly" for international e-commerce?

Does Its Web Site Clearly Disclose Information:

About the Company:

- what kind of business it is and what it sells?
- where it is located, including the country?
- how you can contact the business?

About the Product or Service:

- what's being sold, with enough details for you to know exactly what you're buying?
- the cost of the product or service, and the currency used?

About the Sale:

- the costs, in addition to the price of the product or service, if any, like costs for shipping and handling, taxes and duties?
- any restrictions or limitations on the sale?
- any warranties or guarantees?
- the availability of convenient and safe payment options?
- an estimation of when you will receive the order?

About its Consumer Protections:

- the opportunity for you to print or save a record of the transaction?
- safeguards for protecting your payment information when it is transmitted online?
- policies on what personal identifying information is being collected about you, what the company does with it and whom it shares it with?
- an opportunity for you to "opt out" of having information about yourself collected?
- policies on sending unsolicited email, including an option for you to decline these offers?
- the return policy, including an explanation of how you can return an item, get a refund or credit or make an exchange?
- where you should call, write or email with complaints or problems?

Law Enforcement Agencies Participating in this Initiative Include:

Agency Name
Alaska State Troopers
Albany Oregon Police Department
Allegheny County District Attorney's Office
Anchorage Alaska Police Department
Anne Arundle County Police Department
Arizona Attorney General's Office
Arlington County Virginia Police Department
Arvada Colorado Police Department
Atlanta Georgia Police Department
Augusta Maine Police Department
Australian Federal Police, Australia
Buffalo FBI Cyber Crimes Task Force
Canonsburg Pennsylvania Police Department
Canton Michigan Police Department
Cherokee County Georgia Sheriff's Office
Cherry Hill New Jersey Police Department
Cleveland Police Department
Cobb County Georgia Sheriff's Office
Connecticut Computer Crimes Task Force
Defense Criminal Investigative Services (DCIS)
Denver Colorado Police Department
District Attorney's Office-4th Judicial District, Colorado Springs, CO
Drug Enforcement Administration
Erie County Pennsylvania Office of the District Attorney-Erie County Detectives
Federal Bureau of Investigation
Federal Trade Commission
Floyd County Georgia Sheriff's Office
Georgia Governor's Office of Consumer Affairs
Georgia Secretary of State's Office
Germantown Wisconsin Police Department
Grandview Missouri Police Department
Gwinnett County Georgia District Attorney's Office
Gwinnett County Georgia Police Department
Harris County Texas District Attorney's Office
Independence Oregon Police Department

Agency Name
Internal Revenue Service
Interpol-Ottawa, Canada
Jefferson County Colorado District Attorney's Office
Keyport New Jersey Police Department
Lebanon Oregon Police Department
Linn County Oregon Sheriff's Office
Lynchburg Virginia Police Department
Maricopa County Arizona District Attorney's Office
Maricopa County Arizona Sheriff's Office
Matteson Illinois Police Department
Memphis Tennessee Police Department
Missouri Attorney General's Office
National Aeronautics and Space Administration (NASA)
National White Collar Crime Center
New Jersey State Police High-Tech Crimes Task Force
New York City Police Department
New York State Attorney General's Office
New York State Police
Norwalk Connecticut Police Department
Pennsylvania State Police
City of Pittsburgh Police Dept
Pittsburgh High Tech Crimes Task Force
Office of the County Prosecutor, Monmouth County, New Jersey
Polk County Oregon District Attorney
Prince William County Police Department
Salt Lake City Utah Police Department
Securities and Exchange Commission
Seldovia Police Department
Southern California High Tech Task Force
Staunton Virginia Police Department
Sutherlin Police Department
Tempe Arizona Police Department
Tennessee Police Department
Ticonderoga New York Police Department
Toronto Metropolitan Police Department
United States Attorney's Office
United States Bureau of Customs and Border Protection

Agency Name
United States Postal Inspection Service
United States Secret Service
Utah Attorney General's Office
Virginia Attorney General's Office
Virginia State Police
Warner Robins Georgia Police Department
Waterville Maine Police Department
West Valley City Utah Police Department
Whitehall Pennsylvania Police Department

[See .ppt array, slide 13]