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 cashiers 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 give 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

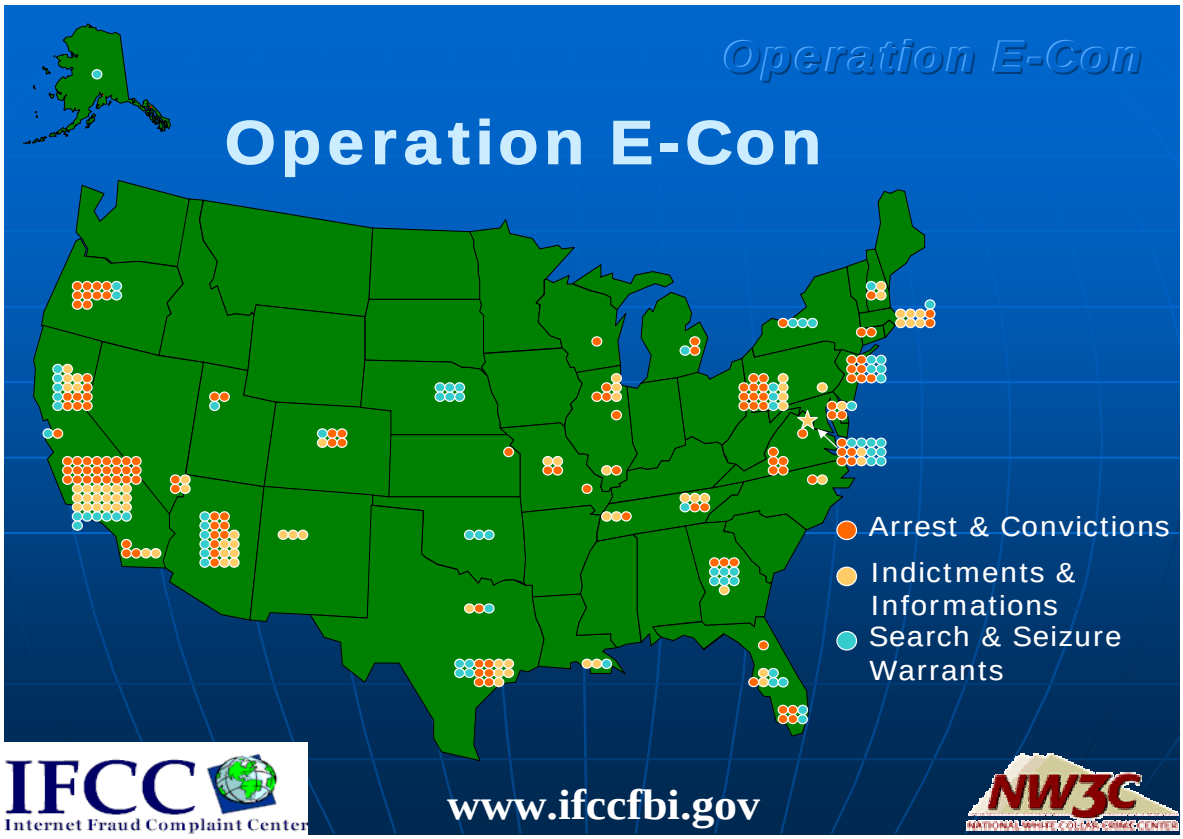
A victim is required to pay significant fees in advance of receiving a substantial amount of money. The fees are usually passed off as taxes, or processing fees, or charges for notarized documents. The victim pays these fees and receives nothing in return. Perhaps the most common example of this type 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.



Operation E-Con

- 90 + Investigations
- 89,000 Victims
- $176 Million in Losses
- $17 Million in Seizures & Recoveries

Operation E-Con

Operation E-Con

- 130 Arrest & Convictions
- 77 Indictments & Informations
- 73 Search & Seizure Warrants

IFCC Internet Fraud Complaint Center
www.ifccfbi.gov
NW3C NATIONAL WHITE COLLAR CRIME CENTER