**WCC Issue**

Internet Fraud

*(Last updated September 2002)*

**Definition**

Internet fraud is defined as any type of fraud scheme that uses one or more components of the Internet, such as chat rooms, e-mail, message boards, or Web sites, to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected to the scheme.¹

**How it Happens**

Fraud conducted through the Internet is as diverse as the Internet itself. According to the Web Developers™ Virtual Library, “the key protocols of the Internet are: News, Gopher, Telnet, Electronic mail (e-mail), File Transfer Protocol (FTP), and HTTP (World Wide Web).”² Experts estimate that the surface Web, primarily static and linked Web pages, contains over 1 billion documents, while the deep Web, largely generated from database-driven Web sites, contains nearly 550 billion individual documents.³ As reported by Dr. Egil Juliussen in the Internet Industry Almanac, “The number of Internet users surpassed 530 million in 2001 and will continue to grow strongly in the next five years. Most of the growth is coming from Asia, Latin America and parts of Europe. By year-end 2005 the number of worldwide Internet users will double to 1.12B.”⁴ Currently, no single law enforcement entity polices this vast expanse of information and users. Internet users, also known as “netizens,” must use caution when travelling the “information super highway” because it is easily utilized by fraudsters as a medium of communication, advertisement, or news information propagating a wide range of frauds at real time speed with relative anonymity.

There are various types of Internet fraud ranging from the interaction of buyer and seller in an electronic auction to the targeting of multiple victims with a “419” fraud. Malicious e-mail viruses that are utilized to extort money from companies, and deceptive Web sites that procure money for non-existent charities are other examples of Internet fraud. For practical purposes, Internet fraud should be addressed by the specific type of fraud committed, in order to make sense of the crime. The major types of Internet Fraud include:

**Auction Fraud**

Auction fraud is the most common form of Internet fraud (see cost/statistics section). On-line users visit sites such as Ebay, Yahoo Auctions, and Ubid.com to buy and sell various items in an on-line format that resembles a real-life auction. Prospective buyers bid on almost any item imaginable from virtual property to antique merchandise. Upon winning, the victim sends payment for the auction item. The fraud occurs when the victim does not receive the item or receives an item of far less value than advertised. When attempting to resolve the problem, the victim frequently has little information on the seller other than an e-mail address. Attempts to communicate with the seller are met with no response or lengthy excuses.
Non-Delivery of Merchandise, Payment, or Services

Non-delivery is easily facilitated with anonymity over the Internet. Various fraudulent on-line retail schemes induce victims to send payment for merchandise and then deliver nothing in return or an item of far less value than expected. Conversely, merchants often deliver merchandise in good faith prior to receiving payment, but never receive payment for their wares. The same non-delivery occurs with services. Services that request payment in advance, such as travel fees or moving costs, are paid via the Internet but then the actual service is never rendered. On the other hand, sometimes services are completed, such as Web site design, but never paid for by the recipient. Both consumers and merchants are victims of non-delivery in on-line frauds. Web sites, spam e-mails, message boards, chatrooms, and various combinations of all four are used to reel in potential victims.

Business Opportunity Scheme

The key word in this type of fraud is opportunity. The prospect of getting rich quickly is the lure that draws victims to business opportunity scams. Spam e-mails allow criminals to batch out thousands of various money-making opportunities. In one common scheme, victims are asked to invest anywhere from $5 to thousands of dollars for a chance to earn money while "working at home." Another scheme involves an Internet-based business opportunity to use your home computer to earn money. Often, the information and tools provided for alleged success in the aforementioned ventures are either fraudulent in nature or of minimal value.

Identity Theft

Identity theft is the illegal use of someone’s personal data such as name, social security number, or driver’s license to obtain money, merchandise, or services by deception. In conjunction with Internet usage, on-line identity theft occurs when someone appropriates your personal information without your knowledge to commit fraud or theft. Appropriating credit card numbers, ordering merchandise on-line with pilfered personal information, and stealing funds from an on-line account, such as Paypal, are some of the most common forms of identity theft on the Internet.

Credit Card Fraud

Credit card fraud committed on-line is a multi-faceted crime. Initially, stolen or forged credit card numbers are used to purchase items from Web sites. In good faith, the merchant ships the merchandise to the suspect. Upon discovery that the credit card number has been used illegally, a "charge-back" is made by the credit card issuer to the merchant. Since the merchandise has already been shipped, the merchant is left without the merchandise and without payment. The owner of the credit card must dispute the purchases with the credit card issuer and resolve any resultant credit issues on their credit report. In many credit card fraud cases, there are actually multiple victims: the Web site merchant, the card-holder, and the card issuer. All who are affected must spend time and/or money resolving the fraudulent issue. There is also the additional crime that was committed in obtaining or stealing the credit card number in the first place.

On-line Investment Schemes/Securities Fraud

Stock market news and information that is posted real-time on the Internet is often taken at face value by investors without additional research. Consequently, on-line investment schemes thrive when victims rush to take advantage of an on-line opportunity with the hopes of multiplying their money. Criminals use different methods of "pump and dump" schemes disseminated via Spam e-mail or Internet message boards in an effort to dramatically increase prices in thinly traded stocks. Once the price doubles or triples, the perpetrators sell off their holdings for significant profit margins. Victims are then left with lesser-valued stocks once the price falls back to its minimal original value. Conversely, the Internet can also be used to
devalue stock with unfounded rumors or purposeful lies. The victims include both the stock holder and the company whose reputation is tarnished or even destroyed.

**Urban Legends/Hoaxes**

Urban legends and hoaxes are brief stories that contain a grain of truth shrouded in a sensational or heartrending narrative. The global nature of the Internet has created an ideal environment for these stories to be routinely forwarded in e-mails by well-intentioned netizens. While not a fraud in the strictest sense, urban legends and hoaxes waste the time and resources of Internet users who read and forward these e-mails over and over to other unsuspecting netizens.

**Costs and Statistics**

While no exact cost can be specifically attributed to the realm of Internet fraud, several surveys exist which give a feel for the enormity of the situation.

The Internet Fraud Complaint Center compiled Internet fraud statistics based upon the 49,711 complaints received in 2001. Internet auction fraud comprised 43 percent of referred complaints. The total dollar loss from all referred cases of fraud was $17.8 million with a median dollar loss of $435 per complaint. Electronic mail and Web sites were the two primary mechanisms by which the fraudulent contact took place.\(^7\)

The Internet Fraud Watch cited on-line auction fraud as 70 percent of the fraud committed on the Internet for the year 2001. The amount of money consumers lost to Internet fraud also increased. Losses overall in 2001 were $6,152,070, up from $3,387,530 in 2000. The average loss per person rose from $427 in 2000 to $518 in 2001. In addition, Web sites were the most prominent medium utilized for conducting fraud.\(^8\)

Gartner Inc.’s G2 research service recently compiled on-line sales statistics for 2001. More than 1 percent of total on-line sales, or $700 million, was lost due to fraudulent activity in 2001. The $700 million, which represents 1.14 percent of total on-line sales of $62 billion, is nearly 20 times higher than the dollar value of fraud losses related to offline sales, Gartner G2 said. In an Internet survey of 1,000 adult on-line consumers in the U.S., Gartner found 5.2 percent were the victims of credit card fraud in 2001, while 1.9 percent were victims of identity theft.\(^9\)

Complaints filed with the Federal Trade Commission’s (FTC) Consumer Sentinel indicated that identity theft comprised 42 percent of the 204,334 complaints filed in 2001. While a general “other” category was the second largest type of complaint, Internet auction fraud was the third largest identifiable crime type that included 10 percent of all the complaints filed with the FTC.\(^10\)

**High Profile Examples/Case Studies**

- In 2002, an old e-mail scam with a new face started circulating on the Internet. Purported to originate from an American Special Forces Commando in Afghanistan, the requestor claimed to need help getting terrorist drug money out of the country. The victim is promised a cut of the total amount of money for paying a fee, bribe or other cost incurred in transporting the money out of the country. This scam is a chameleon that has evolved with technology and current events. It is better known as a “419” or an “advance fee fraud”.\(^11\)

- Also in 2002, the FTC joined eight state law enforcers in the United States and four Canadian agencies in investigating and bringing 63 actions against a wide range of Internet scams for allegedly sending
deceptive, unsolicited e-mail and engaging in fraud on the Internet. The spam e-mail targeted kids and their parents with a message which claimed that consumers had won a free Sony PlayStation 2 or other prize through a promotion purportedly sponsored by Yahoo, Inc. Instead, consumers were routed to an adult Internet site via a 900-number modem connection that charged them up to $3.99 a minute, according to a complaint filed by the Federal Trade Commission. The complaint was brought as part of the International Netforce law enforcement effort.12

- In February 2002, Pennsylvania state police arrested two Beaver County residents and were seeking a third person for stealing user identifications from the eBay Internet auction site and pretending to sell items to unsuspecting buyers.13 The three Russians had allegedly collected money for non-existent items that they auctioned on-line. Authorities filed racketeering charges against Tasiana Zverava and Viachaslau Charnashei, both 20, in addition to charges of theft, criminal conspiracy and criminal use of a computer. One participant told state police she was promised 10 percent of the estimated $10,000 in proceeds each week, while the rest was to be forwarded to ringleaders.14

### The Response/Current Efforts

The Department of Justice is responding to the need with critical efforts to combat Internet fraud. "The global nature of the Internet, and law enforcement experience in conducting Internet fraud investigations, have made it increasingly clear that law enforcement authorities need to work in closer coordination to have a substantial effect on all forms of Internet fraud. Two major steps that the Department has taken to foster national coordination and cooperation among law enforcement authorities on Internet fraud matters are the Internet Fraud Initiative and the Internet Fraud Complaint Center."15 The Internet Fraud Initiative, which the Attorney General approved in 1999, is a national initiative by the Department of Justice intended to provide a comprehensive approach to combating Internet fraud.16 The Internet Fraud Complaint Center (IFCC) is a partnership between the National White Collar Crime Center and the Federal Bureau of Investigation. The IFCC's mission is to address fraud committed over the Internet. For victims of Internet fraud, IFCC provides a convenient and easy-to-use reporting mechanism that alerts authorities to a suspected criminal or civil violation. For law enforcement and regulatory agencies at all levels, IFCC offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends.17

There are several prevention methods for individuals to implement in order to avoid Internet fraud victimization. The most important step is to stay informed about current crime trends. On-line news sources provide timely crime information. Several of the aforementioned surveys are updated annually with trend information. In addition, government and private Web sites provide specific prevention tips for different types of crime. Also, a general awareness of accepted business practices in an industry, such as securities and investments, provides a critical frame of reference for conducting on-line transactions. Often, crime victims who relied upon false product or service information provided by the offender could have found truthful information with a little independent research. Lastly, it is important know who you are dealing with when conducting a financial transaction or other agreement via the Internet. Gather registrant information about a Web site by conducting a "Whois" search on the Internet. Use search engines to perform independent research on company and product names. Maintain copies of all electronic correspondence, including the full header information with the origin and routing details (sent to and received from), from an individual or company. Individuals who take the time to seek detailed information will be better informed and will protect themselves from becoming a victim of Internet fraud.

### “For More Information” Links

- Internet Fraud Complaint Center — [http://www1.ifccfbi.gov/index.asp](http://www1.ifccfbi.gov/index.asp)
▪ United States Department of Justice — http://www.internetfraud.usdoj.gov/
▪ National Consumer League — http://www.fraud.org/
▪ Symantec — http://securityresponse.symantec.com/avcenter/hoax.html

Authors: Sandy Haantz, NW3C Research Assistant, and Aaron Naternicola, NW3C Internet Fraud Analyst


Endnotes