

11/10/2008



Internet Fraud

What You Should Know



Internet Fraud

Internet Fraud

What You Should Know

The following information is a compilation of information and resources I found throughout my research that will give you a better understanding of what Internet Fraud is, types of Internet fraud and their statistics, examples of Internet fraud and news of what's going on in the world today concerning Internet fraud, and information regarding steps you can take to protect yourself and how to file a complaint, along with links to other information that can help you learn more about Internet fraud.

What Is Internet Fraud?

The term "Internet fraud" refers generally to 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 other connected with the scheme.

Major Types of Internet Fraud

While researching the different types of Internet fraud, I found that the list of types is enormous. Covering them all would make this research paper entirely too long. For this reason, I decided to cover five of the major types of Internet fraud. The ones I chose are as follows.

Online Auction and Retail Schemes

According to the Federal Trade Commission and Internet Fraud Watch, fraudulent schemes appearing on online auction sites are the most frequently reported form of Internet fraud. These schemes, and similar schemes for online retail goods, typically purport to offer high-value items - ranging from Cartier® watches to computers to collectibles such as Beanie Babies® - that are likely to attract many consumers. These schemes induce their victims to send money for the promised items, but then deliver nothing or only an item far less valuable than what was promised (e.g., counterfeit or altered goods). Auction fraud involves fraud via the misrepresentation of a product advertised for sale through an Internet auction site (like Ebay) or the non-delivery of products purchased through an Internet auction site. In other words, either the product you ordered isn't what the seller claimed it was, or the seller fails to deliver it, or the seller lies about some other aspect of the transaction. Auction fraud is the most prevalent of Internet crimes associated with Romania. Romanians, long famous in crime circles for gypsies and conmen, have saturated the Internet auctions and offer almost every in-demand product. Typically, they act more flexible than most sellers, allowing victims to send half the funds now, and the other half when the item arrives.

Online Auction and Retail Schemes in the News

[Middletown man charged in online auction scheme](#)

[Romanian cybercrime ring busted](#)

[Final day for massive auction of confiscated merchandise](#)

Online "Work-at-Home" Schemes

Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in "work-at-home" ventures. These schemes typically require the individuals to pay anywhere from \$35 to several hundred dollars or more, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business. Most individuals are attracted to these ads because they are very persuasive and make lavish claims about great income for a few hours of work each day. The victims buy into the deceptive work at home schemes consequently losing their money to unscrupulous promoters.

Online "Work at Home" Schemes in the News

["Work from Home" Scheme Busted](#)

[United States Attorney seeks victims of \\$2,000,000 "WORK AT HOME" scheme](#)

Identity Theft and Fraud

Some Internet fraud schemes also involve identity theft - the wrongful obtaining and using of someone else's personal data in some way that involves fraud or deception, typically for economic gain. The US Government defines it like this: "Identity theft occurs when someone appropriates your personal information without your knowledge to commit fraud or theft." To put that in more day-to-day terms, it works like this: Someone gets your name, address, social security number and credit card or other information, and uses them to run up big bills, pretending they're actually you. They skip on the bills and leave you with ruined credit and collectors hounding you. Internet identity theft can be much more devastating than

conventional identity theft because most victims of Internet identity theft are completely unaware that anything has been stolen from them until it is much too late. You may not know it, but your computer collects all kinds of information about you and stores it in files hidden deep on your hard drive. Files like cache, browser history and other temporary Internet files can be used to reconstruct you online habits. These files store information like logins and passwords, names addresses, and even credit card numbers. A thief can get at this information in one of two ways. Either he can grab it when it is being sent over an unsecured transmission, or he can install malicious software on your computer (like spyware) that will collect everything he needs and automatically send it back to him. The best way to protect oneself from Internet identity theft is to get an Internet security solution that is up to the challenge.

Identity Theft and Fraud in the News

[FBI warns of latest expensive Internet traps and tricks](#)

[IRS Warns of New E-Mail and Telephone Scams Using the IRS Name](#)

[Identity Theft, Financial Fraud Remain Top Concerns for Consumers](#)

[US cracks 'biggest ID fraud case'](#)

[Identity Theft E-mail Scams a Growing Problem](#)

Online Investment Schemes

These schemes involve making an initial investment in a day trading operation that claims to offer huge returns. For example, "pump-and-dump" schemes involve the touting of a company's stock (typically microcap companies) through false and misleading statements to the marketplace. After pumping the stock, fraudsters make huge profits by selling their cheap stock into the market. These schemes often occur on the Internet where it is common to see messages posted that urge readers to buy a stock quickly or to sell before the price goes down

The Internet allows individuals or companies to communicate with a large audience without spending a lot of time, effort, or money. Anyone can reach tens of thousands of people by building an Internet web site, posting a message on an online bulletin board, entering a discussion in a live "chat" room, or sending mass e-mails. It's easy for fraudsters to make their messages look real and credible. But it's nearly impossible for investors to tell the difference between fact and fiction.

Online Investment Schemes in the News

[Online Investment Schemes: Fraud and Abuse in Cyberspace](#)

[VeriSign Reveals First of Its Kind Real-Time Protection against 'Pump and Dump' Stock Trading Fraud](#)

[Georgia man gets 3 years for Internet investment fraud](#)

[SEC Action Halts \\$72 Million International Internet Fraud Scheme](#)

[Multi-Million Dollar Pyramid Scheme -- BUSTED!](#)

Credit Card Schemes

There is an amazing amount of fraudsters out there who want your credit card number so that they can use it for their own profit. Credit card numbers have been stolen in a lot of different ways. For example, before the Internet, card numbers were stolen by store clerks. When you make a purchase at a store, your card is run through a machine that reads it and then authorizes the purchase. Upon completion of the transaction, two receipts are printed; one for you and one for the clerk to place in the register. It is very easy for the clerk to copy your credit card number from the receipt that was placed in the register. With the use of the Internet, ways of stealing credit card numbers have become highly sophisticated. For example, as online transaction volumes increase, new methods for hijacking identities for credit card fraud include

phishing and the use of spyware and botnets. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent which can collect various types of personal information. A botnet, also called a zombie army, is a collection of software bots that run autonomously and automatically. In other words, a bot is a zombie computer that is set up, without the owner knowing, to transmit spam or viruses to other computers on the Internet. A botnet is a collection of bots. Botnets are exploited for various purposes, including denial-of-service attacks, creation or misuse of SMTP mail relays for spam, click fraud, spamdexing, and the theft of application serial numbers, login IDs, and financial information such as credit card numbers.

Credit Card Schemes in the News

[US indicts 11 in credit card scheme](#)

[Global Trail of an Online Crime Ring](#)

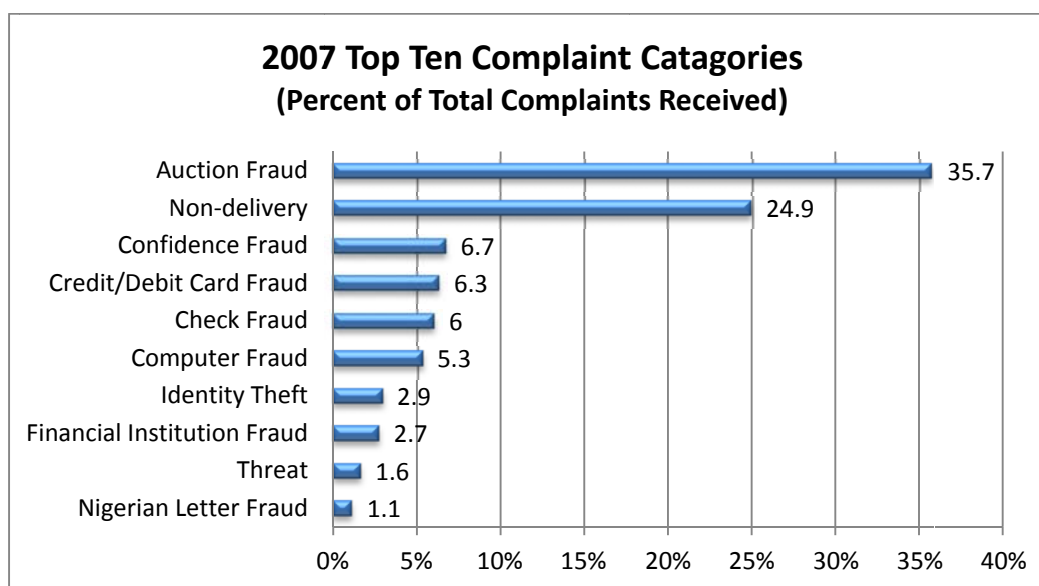
[Obama's Credit Card Scheme Gets Noticed](#)

[Baton Rouge Credit Card Scheme Uncovered at Zachary Business](#)

2007 Top Ten Internet Fraud Statistics

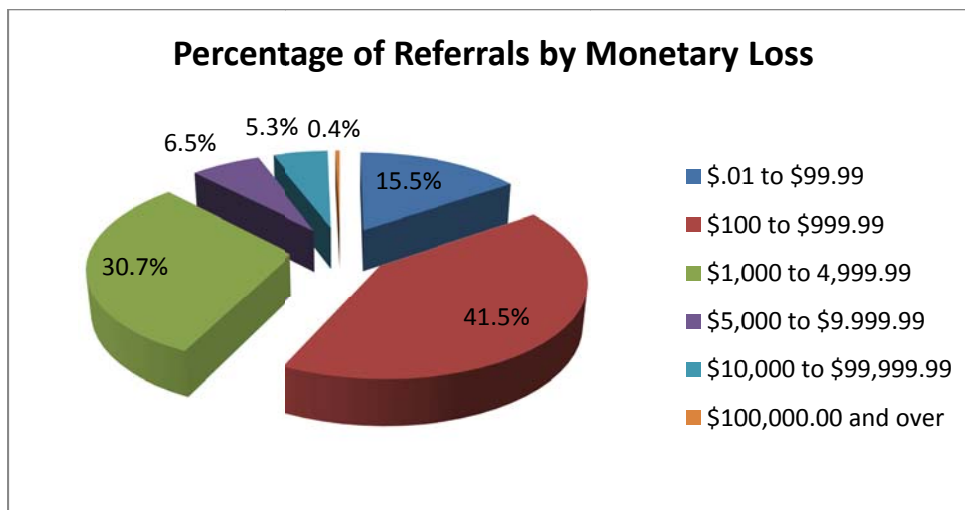
According to Consumer Fraud Reporting, Web crime statistics are notoriously difficult to obtain, with many sources each calculating them in a different manner and different time frame, using a different source. Because the year 2008 is not yet over, I have not been able to find any reliable statistics on Internet fraud for this year. To provide the best picture, I have decided to

use the FBI/IC3 2007 statistics. The IC3 began operation on May 8, 2000, as the Internet Fraud Complaint Center and was established as a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI) to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime.



According to the Internet Crime Complaint Center's 2007 Internet Crime Report, during 2007, Internet auction fraud was by far the most reported offense, comprising 35.7% of referred crime complaints. This represents a 20.5% decrease from the 2006 levels of auction fraud reported to IC3. In addition, during 2007, the non-delivery of merchandise and/or payment represented 24.9% of complaints (up 31.1% from 2006). Confidence fraud made up an additional 6.7% of complaints (see Chart 5). Credit and debit card fraud, check fraud, and computer fraud complaints represented 17.6% of all referred complaints. Other complaint

categories such as identity theft, financial institutions fraud, threats, and Nigerian letter fraud complaints together represented less than 8.3% of all complaints.



The total dollar loss from all referred cases of fraud in 2007 was \$239.09 million. That loss was greater than 2006 when a total loss of \$198.44 million was reported. Of those complaints with a reported monetary loss, the mean dollar loss was \$2,529.90 and the median was \$680.00. Nearly sixteen percent (15.5%) of these complaints involved losses of less than \$100.00, and forty one and a half percent (41.5%) reported a loss between \$100.00 and \$1,000.00. In other words, over half of these cases involved a monetary loss of less than \$1,000.00. Nearly a third (30.7%) of the complainants reported losses between \$1,000.00 and \$5,000.00 and only 12.2% indicated a loss greater than \$5,000.00. The highest dollar loss per incident was reported by Investment Fraud (median loss of \$3,547.94). Check fraud victims, with a median loss of \$3,000.00 and Nigerian letter fraud (median loss of \$1,922.99) were other high dollar loss

categories. The lowest dollar loss was associated with credit/debit card fraud (median loss of \$298.00).

Amount Lost by Selected Fraud Type for Individuals Reporting Monetary Loss

Complaint Type	% of Reported Total Loss	Of those who reported a loss the Average (median) \$ Loss per Complaint
Investment Fraud	6.1%	\$3,547.94
Check Fraud	9.9%	\$3,000.00
Nigerian Letter Fraud	6.4%	\$1,922.99
Confidence Fraud	12.6%	\$1,200.00
Auction Fraud	22.4%	\$483.95
Non-delivery (merchandise and payment)	17.8%	\$466.00
Credit/Debit Card Fraud	4.6%	\$298.00

By visiting the Internet Crime Complaint Center, you can also view their statistic reports for each state. The following was taken from their statistical report on Ohio.

Ohio's IC3 2007 Internet Crime Report Complaint Characteristics			
In 2007 IC3 received a total of 5640 complaints from the state of Ohio.			
Top 10 Complaint Categories from Ohio		Percent of Referrals by Monetary Loss	
Auction Fraud	37.6%	\$.01 - \$99.99	18.6%
Non Delivery of Merchandise /Payment	25.0%	\$100.00 - \$999.99	45.0%
Confidence Fraud	8.1%	\$1000.00 - \$4999.99	27.3%
Credit Card Fraud	5.9%	\$5000.00 - \$9999.99	5.1%
Check Fraud	5.5%	Over 10000	4.0%
Computer Fraud	3.9%	The top dollar loss complaint involved non-delivery and totaled \$445,000.00 while reported losses throughout the state exceeded \$6.8 million.	
Financial Institutions Fraud	3.8%		
Identity Theft	2.5%		
Nigerian Letter Fraud	2.4%		
Threat	1.0%		

Amount Lost by Fraud Type for Individuals Reporting Monetary Loss		
Complaint Type	% who reported a loss	Median loss per complaint
Auction Fraud	99.5%	\$354.00
Non-delivery	99.3%	\$350.00
Confidence Fraud	95.7%	\$970.00
Credit Card Fraud	98.8%	\$250.00
Check Fraud	100%	\$2997.50

Internet Fraud

Computer Fraud	13.6%	\$3000.00
Financial Institutions Fraud	99.1%	\$200.00
Identity Theft	77.1%	\$534.00
Nigerian Letter Fraud	94.1%	\$1324.00
Threats	20.7%	\$200.00
The total median dollar loss for all complaints reporting a dollar loss was \$498.11.		

Ohio Perpetrator Characteristics	
Gender	% of Perpetrators
Male	74.2%
Female	25.8%
Perpetrator Statistics within the United States Per 100,000 population Ohio ranks 35 th highest at 18.09 while ranking 8 th on total number of perpetrators identified as residing in Ohio. This total accounts for 2.8% of all complaints where the perpetrator was identified.	

Ohio Complainant Characteristics	
Gender	% of Perpetrators
Male	54.2%
Female	45.8%

Complaint Demographics	
Under 20	3.2%
20-29	20.7%
30-39	24.6%
40-49	24.7%
50-59	19.0%
Over 60	7.8%

Amount Lost Per Referred Complaint By Selected Complainant Demographics	
Under 20	\$285.00
20-29	\$480.00
30-39	\$515.00
40-49	\$500.00
50-59	\$462.99
60 and older	\$578.00
Complainant Statistics within the United States Per 100,000 population Ohio ranks 18 th highest at 62.24 while also ranking 7 th on total number of complainants identified as residing in Ohio. This total accounts for only 3.1% of all complainants in the United States.	

Complainant-Perpetrator Dynamics From Same State as Complainant and the top three locations	
State	Percent
Ohio	7.8%
1. California	13.3%

2. Florida	9.3%
3. New York	9.2%

How to Protect Yourself

The following information is a brief list of things you can do to protect yourself from the above mentioned types of Internet fraud. Following each will be a list of Internet resources that you can visit for more information.

Online Auction and Retail Schemes

Evaluate how soon you need to receive the item you're bidding on, and whether you can tolerate it being delivered late, or even not delivered. Whether you're a buyer or a seller, read each auction site's Terms of Use, carefully consider your method of payment, don't reply to "phishing" emails, know who you're dealing with, and know exactly what you're bidding on. Visit the following link to view more detailed information regarding these warnings.

[Internet Auctions: Quick Facts](#)
[How to Avoid Online Auction Fraud](#)

Online "Work-at-Home" Schemes

Know who you're dealing with, don't believe that you can make big profits easily, be cautious about emails offering work-at-home opportunities, get all the details before you pay, find out if there is really a market for your work, get references for other people who are doing the work, be aware of legal requirements, know the refund policy, beware of the old "envelope stuffing" scheme, be wary of offers to send you an "advance" on your "pay", and do your own research

about work-at-home opportunities. Visit the following link to view more detailed information regarding these warnings.

[National Consumers League's Internet Fraud Watch: Work-At-Home Scams Tips](#)

Identity Theft and Fraud

The following links will take you to resources that will help you prevent identity theft and provide information on what to do if you are a victim of identity theft.

[National Consumers League's Internet Fraud Watch: ID Theft Victims Tips](#)

[Identity Theft Victim's Guide](#)

[Consumer Facts for Older Americans](#)

Online Investment Schemes

Don't believe claims that there is no risk, beware of promises that you'll make big profits fast, get the details in writing, don't agree to anything on the spot, understand your investments, don't act on testimonials from strangers, be especially wary of investments in commodities, steer clear of "offshore investments", be cautious about emails for investments, and take the time to check out investment offers. Visit the following link to view more detailed information regarding these warnings.

[National Consumers League's Internet Fraud Watch: Investment Fraud Tips](#)

[How to Avoid Internet Investment Scams](#)

Credit Card Schemes

You should always keep your credit card close. Never give your credit card number to someone else over the phone unless you know for sure who the person is. Do not provide your credit card number to anyone through emails. Legitimate companies will not send you emails requesting your card number. When giving out information on a website, make sure the site is

secure. You should see a small lock icon on secure pages or the address in the address bar should start with “https” instead of “http”. More tips can be found by visiting the following links.

[Credit Card Fraud and Online Scam Resources](#)

[Credit Card Fraud: How to protect yourself](#)

Reporting Internet Fraud and Other Resources to Help Avoid It

The following links are provided to help you know how you can and when you should report Internet fraud.

[Reporting Internet Fraud](#)

[Steps To Take When Reporting Internet Fraud](#)

[Fraud Avoidance and Reporting Resources](#)

[Internet Fraud Tips from the National Consumers League’s Internet Fraud Watch](#)

[How to Avoid Internet Fraud](#)

[What to Do If I Am a Victim](#)

[Cybercrime: What to Do If You're a Victim](#)

[Fraud Avoidance and Reporting Resources](#)

[What to do if you're a victim of fraud](#)

Works Cited

1. United States Department of Justice (2008). *Internet and Telemarketing Fraud*. Retrieved November 1, 2008, from <http://www.usdoj.gov/criminal/fraud/internet/>
2. U.S. Securities and Exchange Commission (2007). *Internet Fraud: How to Avoid Internet Investment Scams*. Retrieved November 1, 2008, from <http://www.sec.gov/investor/pubs/cyberfraud.htm>
3. Winferno Software (2006). *Internet Identity Theft*. Retrieved October 28, 2008, from <http://articles.winferno.com/computer-fraud/internet-identity-theft/>
4. Robert Longley (2008). 'Spoofing' and 'Phishing' and Stealing Identities. Retrieved October 28, 2008, from <http://usgovinfo.about.com/cs/consumer/a/aaspoofing.htm>
5. ScamBusters.org (2008). "Internet Scams, Identity Theft, and Urban Legends: Are You at Risk?". Retrieved October 30, 2008, from <http://www.scambusters.org/>
6. Wikipedia (2008). Internet Fraud. *Wikipedia*. Retrieved October 30, 2008, from http://en.wikipedia.org/wiki/Internet_fraud
7. B. B. Lee (2008). *Work at Home Opportunities: Beware of Misleading Home Business Schemes*. Retrieved October 30, 2008, from http://smallhomebusiness.suite101.com/article.cfm/work_at_home_opportunities
8. Consumer Fraud Reporting (2008). *Internet Fraud, Scam and Crime Statistics - 2008*. Retrieved October 30, 2008, from http://www.consumerfraudreporting.org/internet_scam_statistics.htm
9. Internet Crime Complaint Center (2007). *2007 IC3 Annual Reports*. Retrieved November 1, 2008, from <http://www.ic3.gov/media/annualreports.aspx>
10. National Consumers League's Internet Fraud Watch (2008). *Internet Fraud Tips*. Retrieved November 1, 2008, from <http://www.fraud.org/internet/inttip/inttip.htm>
11. Peter Kenny (2007). *Credit Card Fraud: How to protect yourself*. Retrieved November 1, 2008, from <http://www.articlesbase.com/finance-articles/credit-card-fraud-how-to-protect-yourself-203127.html>