IC3 2003 Internet Fraud Report

January 1, 2003—December 31, 2003

Prepared by the
National White Collar Crime Center
and the Federal Bureau of Investigation

Contents

The Internet Crime Complaint Center
2003 Internet Fraud Report:
January 1, 2003-December 31, 2003

Executive Summary

In December 2003, the Internet Fraud Complaint Center (IFCC) was renamed the Internet Crime Complaint Center (IC3) to better reflect the broad character of such matters having a cyber (Internet) nexus. The 2003 Internet Fraud Report is the third annual compilation of information on complaints received and referred by the IC3 to law enforcement or regulatory agencies for appropriate action. From January 1, 2003 – December 31, 2003, the IC3 and IFCC websites received 124,509 complaint submissions. These filings were composed of fraudulent and non-fraudulent complaints primarily related to the Internet.

IC3 referred 95,064 complaints to enforcement agencies on behalf of the filing individuals. These complaints were composed of many different fraud types such as auction fraud, non-delivery, and credit/debit card fraud, as well as non-fraudulent complaints, such as computer intrusions, spam/unsolicited e-mail, and child pornography.

From the submissions, IC3 referred 63,316 complaints of fraud, the majority of which were committed over the Internet or similar online service. The total dollar loss from all referred cases of fraud was $125.6 million with a median dollar loss of $329 per complaint. Significant findings include:

- Internet auction fraud was still by far the most reported offense, comprising 61.0% of referred complaints. Non-delivered merchandise and/or payment accounted for 20.9% of complaints. Credit/debit card fraud made up 6.9% of complaints. Check Fraud, identity theft, business fraud, and investment fraud round out the top seven categories of complaints referred to law enforcement during the year (all at 1.0% or more).

- Among those individuals who reported a dollar loss, the highest median dollar losses were found among Nigerian letter fraud, identity theft, and check fraud complainants.

- Among perpetrators, nearly 79% were male and half resided in one of the following states: California, New York, Florida, Texas, Pennsylvania, and Illinois. The majority of reported perpetrators were from the United States. However, perpetrators also had a representation in Canada, Nigeria, Italy, Spain, and Romania.

- Among complainants, 70% were male, half were between the ages of 30 and 50 (39.4 average age) and over one-third resided in one of the four most populated states: California, Florida, Texas, and New York. While most were from the United States, IC3 received a number of complaints from Canada, Australia, Great Britain, Germany, and Japan.

- Males lost more money than females. This may be a function of both online purchasing differences by gender and the type of fraudulent schemes the individual were victimized by.

- Electronic mail (E-mail) and web pages were the two primary mechanisms by which the fraudulent contact took place. In all, 64.8% of complainants reported that they had e-mail contact with the perpetrator and 19.4% had contact through a web page.

Overview

The Internet Fraud Complaint Center (IFCC), which began operation on May 8, 2000, 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. IFCC was intended and continues to emphasize serving the broader law enforcement community, including federal, state and local agencies, which employs key participants in the growing number of Cyber Crime Task Forces. Since its inception, IFCC has received complaints across a wide array of cyber crime matters, including online fraud in its many forms, intellectual property rights (IPR) matters, computer intrusions (hacking), economic espionage (theft of trade secrets), child pornography, international money laundering, identity theft, and a growing list of additional criminal matters. To better reflect the broad character of such matters having a Cyber (Internet) nexus referred to IFCC, and to further the growing partnerships with key sponsoring agencies, IFCC was renamed the Internet Crime Complaint Center (IC3) on December 1, 2003.

IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

Although IC3 primarily serves citizens of the United States it has also served as a model for other countries wishing to develop a regional, centralized Internet crime referral system. For example, the National White Collar Crime Center of Canada (NW4C) was initiated in 2003 as an online complaint system called RECOL, Reporting Economic Crime Online. "RECOL is an initiative that involves an integrated partnership between International, Federal and Provincial Law Enforcement agencies, as well as, with regulators and private commercial organizations that have a legitimate investigative interest in receiving a copy of complaints of economic crime."[1] The establishment of this agency directly meets the needs of Canadians who are victims of Internet crime.

Significant and supplemental to partnering with law enforcement and regulatory agencies, it will remain a priority objective of IC3 to establish effective alliances with industry. Such alliances will enable IC3 to leverage both intelligence and subject matter expert resources, pivotal in identifying and crafting an aggressive, proactive approach to combating cyber crime. Two examples of efforts coordinated by the U.S. Department of Justice are Operation Cyber Sweep and Operation Web Snare. These operations represent initiatives targeting an expansive array of cyber crime schemes victimizing individuals and businesses worldwide.

Overall, the IC3 2003 Internet Fraud Report is the third annual compilation of information on complaints received and referred by IC3 to law enforcement or regulatory agencies for appropriate action. The results provide an examination of key characteristics of 1) complaints, 2) perpetrators, 3) complainants, 4) interaction between perpetrators and complainants, and 5) success stories involving complaints referred by IC3. The results in this report are intended to enhance our general knowledge about the scope and prevalence of Internet fraud in the United States. This report does not represent all victims of Internet fraud, or fraud in general, because it is derived solely from the people who filed a report with IC3.

General IC3 Filing Information

Internet crime complaints are primarily submitted to IC3 online at www.ic3.gov or www.ifccfbi.gov. Complainants without Internet access can submit information via telephone. After a complaint is filed with IC3, the information is reviewed, categorized, and referred to the appropriate enforcement or regulatory agency.

From January 1, 2003 – December 31, 2003, there were 124,509 complaints filed online with IC3. This is a 60% increase over 2002 when 75,063 complaints were received. There was a steady increase in the number of complaints filed for each quarter of 2003 with the fourth quarter having a record number of 37,381. Additionally, complaint submissions have increased annually (see Chart 1 and 2). The number of complaints filed per month averaged

[1] RECOL.CA Reporting Economic Crime Online, Welcome to RECOL, 2004.

10,376 and an average of 7,922 (both fraudulent and non-fraudulent) complaints were referred by IC3 Internet Fraud Analysts.

During 2003, there were 95,064 complaints referred to enforcement and regulatory agencies on behalf of the complainants. This total includes various fraud types, such as auction fraud, non-delivery, and credit/debit card fraud, as well as non-fraudulent complaints, such as computer intrusions, spam, and child pornography.

Chart 1
Yearly Comparison of Complaints Received Via IC3 Website

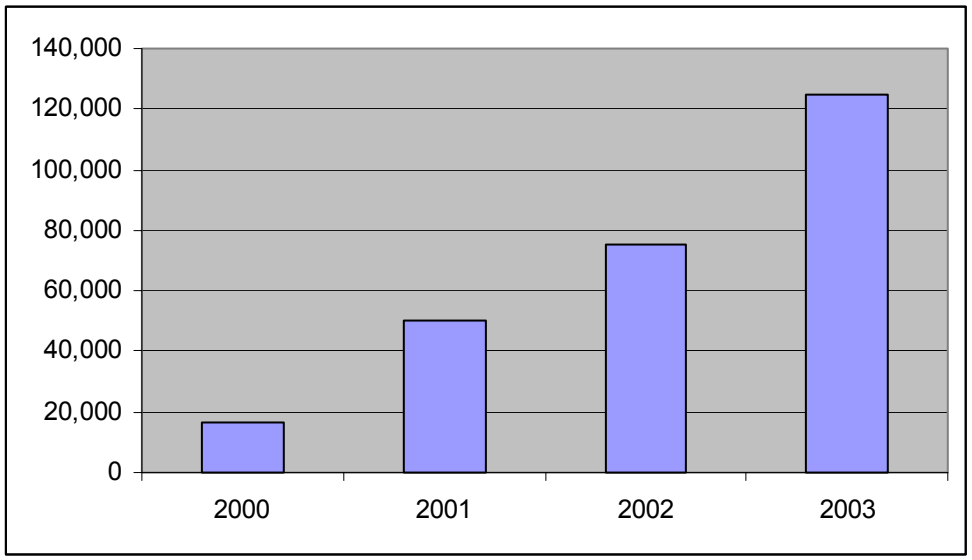
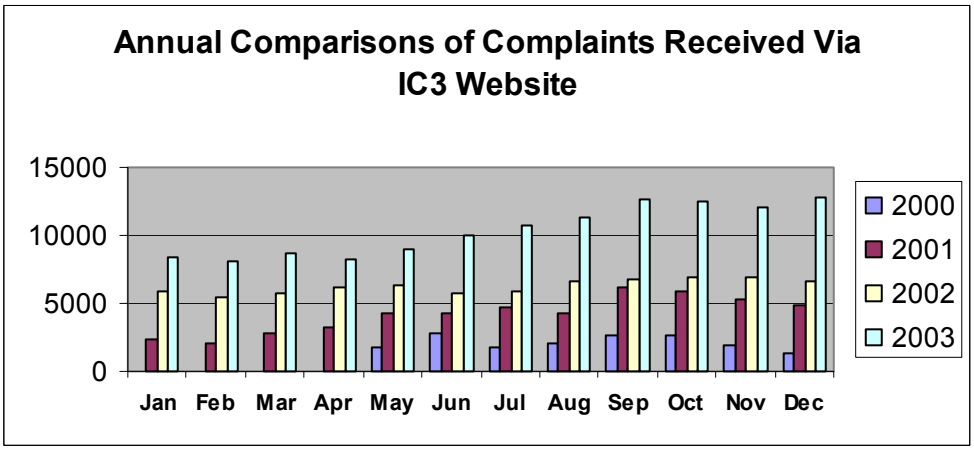


Chart 2



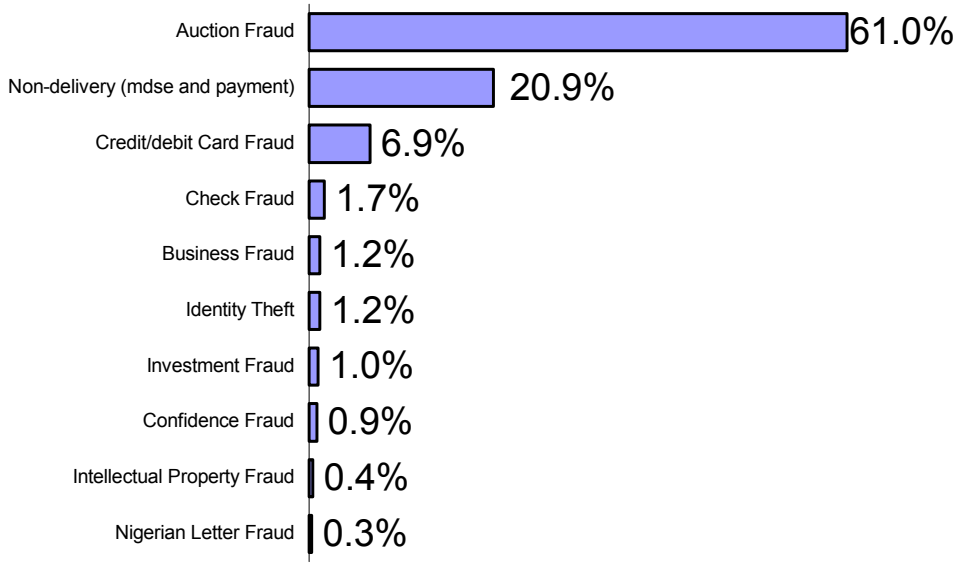
The results contained in this report were based on information that was provided to IC3 through the complaint forms submitted online at www.ic3.gov or www.ifccfbi.gov by complainants. While IC3's primary mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime, those complaints involving more traditional methods of contact (e.g., telephone and mail) were also referred. Using information provided by the complainant, it is estimated that just over 85% of all complaints were related to the Internet or online service. Criminal complaints were referred to law enforcement and/or regulatory agencies based on the residence of the

subject(s) and victims(s). In 2003, there were 15 Memorandums of Understanding (MOUs) from non-member agencies added to the Pyramid database system and an additional 50 member agencies added to the database.

Complaint Characteristics

During 2003, Internet auction fraud was by far the most reported offense, comprising 61% of referred fraud complaints. This represents a 32.3% increase from 2002 (46.1%) levels of auction fraud reported. In addition, during 2003, the non-delivery of merchandise and/or payment represented 20.9% of complaints (down 33.2% from 2002), and credit and debit card fraud made up an additional 6.9% of complaints (down 40.5% from 2002). Check fraud, business fraud, identity theft, and investment fraud complaints that remained within the IC3 structure represented a mere 5.1% of all remaining complaints. Confidence fraud, intellectual property fraud, and Nigerian letter fraud complaints represented less than 1.6% of all complaints combined.

Chart 3
Top Ten IC3 Complaint Categories



% of all referred fraudulent complaints, January 1, 2003-December 31, 2003

Due to relationships with enforcement and regulatory agencies, IC3 continues to refer specific fraud types to the appropriate agencies. Complaints received by IC3 included confidence fraud such as home improvement scams and multi-level marketing, investment fraud, business fraud, and other unspecified frauds. Identity theft complaints are referred to the Federal Trade Commission (FTC) as well as being addressed by other agencies. Compared to 2002, there were slightly lower reporting levels of confidence fraud, investment fraud, and business fraud in 2003. For a more detailed explanation on complaint categories used by IC3, refer to Appendix 1 at the end of this report.

A key area of interest regarding Internet fraud is the average monetary loss incurred by complainants contacting IC3. Such information is valuable because it provides a foundation for estimating average Internet fraud losses in the general population. To present information on average losses, two forms of averages are offered: the mean and the median. The mean represents a form of averaging familiar to the general public: the total dollar amount divided by the total number of complaints. Because the mean can be sensitive to a small number of extremely high or extremely low loss complaints, the median is also provided. The median represents the 50th percentile, or midpoint, of all loss amounts for all referred complaints. The median is less susceptible to extreme cases, whether high or low cost.

Of the 63,316 fraudulent referrals processed by IC3 during 2003, 49,756 involved a victim who reported a monetary loss. Other complainants who did not file a loss may have reported the incident prior to victimization (e.g., received a fraudulent business investment offer online or in the mail), or may have already recovered money from the incident prior to filing (e.g., zero liability in the case of credit/debit card fraud).

The total dollar loss from all referred cases of fraud in 2003 was $125.6 million. Of those complaints with a reported monetary loss, the mean dollar loss was $2,524 and the median was $329. Twenty-six percent (26%) of these complaints involved losses of less than $100, and nearly half (47.6%) reported a loss between $100 and $1,000. In other words, over two-thirds of these cases involved a monetary loss of less than $1,000. Very few of the complainants reported high dollar losses, with 21.2% indicating a loss between $1,000 and $5,000 and only 3% indicating a loss greater than $5,000. The highest dollar loss per incident was reported by Nigerian letter fraud victims, with a median loss of $5,496. Identity theft (median loss of $1,300) and check fraud (median loss of $4,550) were other high dollar loss categories. The lowest dollar loss was associated with intellectual property fraud (median loss of $120) and business fraud (median loss of $300) offenses.

Chart 4
Percentage of Referrals by $ Loss

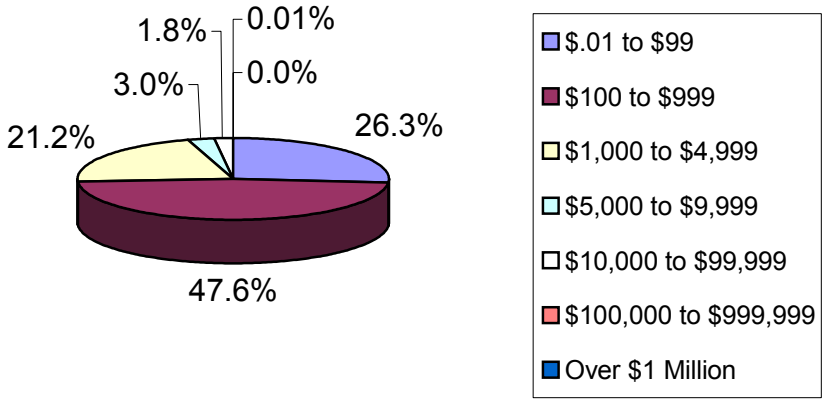


Table 1: Amount Lost by Fraud Type for Individuals Reporting Monetary Loss

Complaint Type	*% of Complainants Who Reported Dollar Loss*	*Of those who reported a loss the Average (median) $ Loss per Complaint*
Auction Fraud	86	$314
Non-delivery (mdse and payment)	83	$329
Nigerian Letter Fraud	73	$5496
Credit/debit Card Fraud	62	$309
Confidence Fraud	41	$6850
Investment fraud	76	$1385
Business Fraud	33	$300
Identity Theft	17	$1300
Check Fraud	39	$4550
Intellectual Property Fraud	6	$120

Perpetrator Characteristics

Equally important to presenting the prevalence and monetary impact of Internet fraud is providing insight into the demographics of fraud perpetrators. In those cases with a reported location, nearly 79% of the perpetrators were male and over half resided in one of the following states: California, New York, Florida, Texas, Pennsylvania, and Illinois (see Map 1). These locations are among the most populous in the country. Controlling for population, Nevada, New York, Florida, Arizona, California, and New Hampshire have the highest per capita rate of perpetrators in the United States. Perpetrators also have been identified as residing in Canada, Nigeria, Spain, Italy, and Romania (see Map 2). Inter-state and international boundaries are irrelevant to Internet criminals. Jurisdictional issues can enhance their criminal efforts by impeding investigations with multiple victims, multiples states/counties, and varying dollar losses.

The vast majority of perpetrators were in contact with the complainant through either e-mail or via the web. (Refer to Appendix III at the end of this report for more information about perpetrator statistics by state.) These statistics highlight the anonymous nature of the Internet. The gender of the perpetrator was reported only 65.5% of the time, and the state of residence for domestic perpetrators was reported only 71.1% of the time.

Chart 5
Gender of Perpetrator

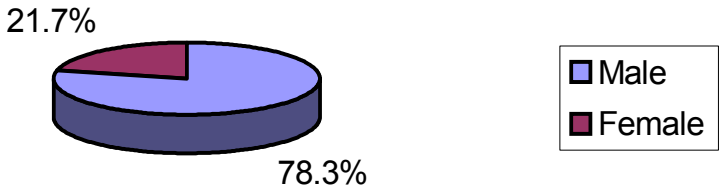
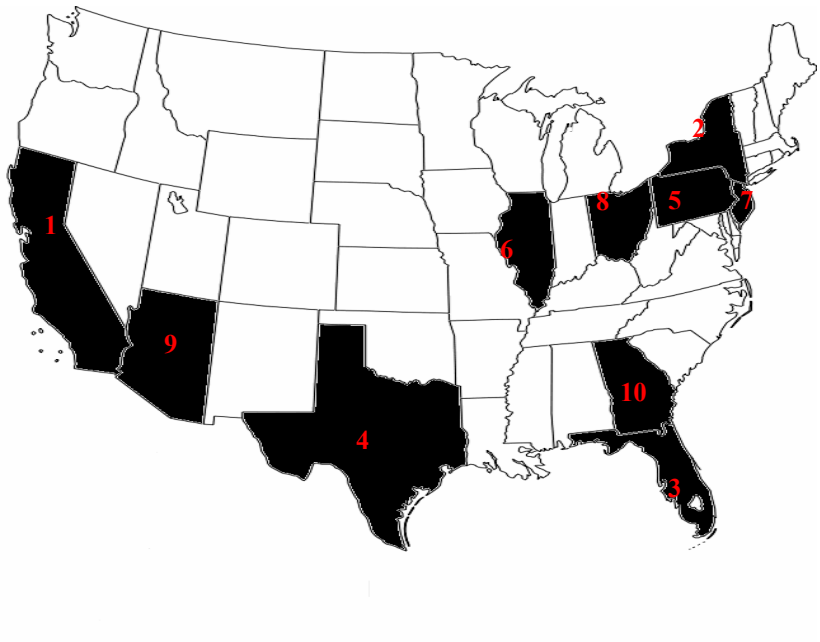


Table 2: Perpetrators per 100,000 population (based on 2003 Census figures)

1. Nevada – 41.85
2. New York – 21.34
3. Florida – 20.32
4. Arizona – 19.84
5. California – 17.04
6. New Hampshire – 16.15
7. Rhode Island – 15.33
8. Washington – 14.97
9. Maine – 14.09
10. New Jersey – 13.65

Map 1 - Top Ten States by Count: Individual Perpetrators (Number is Rank)



Top Ten States - Perpetrator

1. California – 16.1%
2. New York – 10.8%
3. Florida – 9.2%
4. Texas – 6.0%
5. Pennsylvania – 3.8%
6. Illinois – 3.7%
7. New Jersey – 3.1%
8. Ohio – 3.1%
9. Arizona – 3.0%
10. Georgia – 2.7%

Map 2 - Top Ten Countries by Count: Perpetrators (Number is Rank)

Top Ten Countries - Perpetrator

1. United States – 76.4%
2. Canada – 3.3%
3. Nigeria – 2.9%
4. Italy – 2.5%
5. Spain – 2.4%
6. Romania – 1.5%
7. Germany – 1.3%
8. United Kingdom – 1.3%
9. South Africa – 1.1%
10. Netherlands – .9%

Complainant Characteristics

The following graphs offer a detailed description of the individuals who filed an Internet fraud complaint through IC3. The majority of complainants were male, between 30 and 50 years of age, and a resident of one of the four most populated states: California, Florida, New York, and Texas. Hawaii and Alaska, while having a relatively small number of complaints (ranked 34th and 45th, respectively), had among the highest per capita rate of complainants in the United States (see Table 3). While most complainants were from the United States, IC3 has also received a number of filings from Canada, Australia, and Japan (see Map 4).

Chart 6
Gender of Complainant

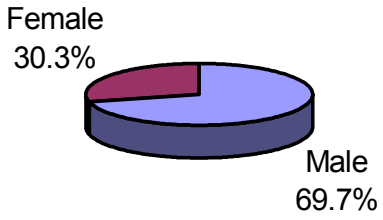


Table 3: Complainants per 100,000 population (based on 2003 Census figures)

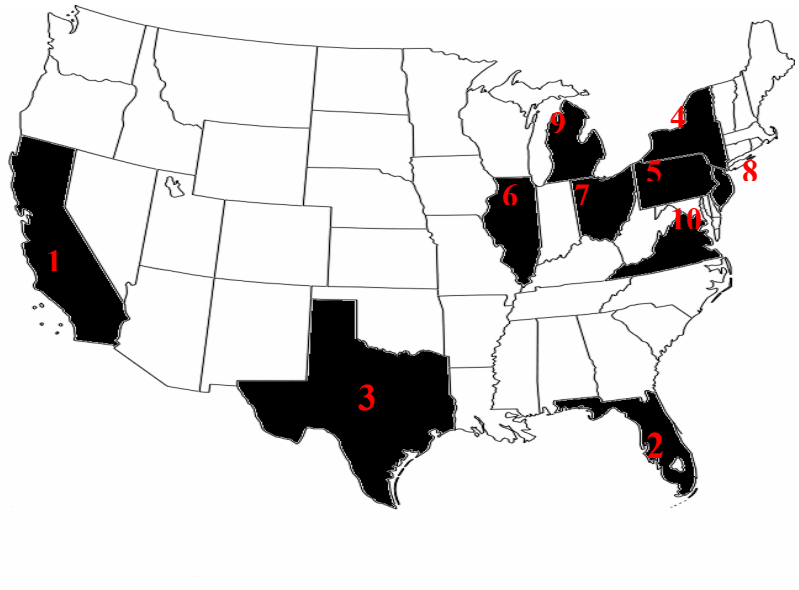
1. District of Columbia – 44.02
2. Hawaii – 43.50
3. Colorado – 40.57
4. Alaska – 40.00
5. Washington – 37.36
6. Florida – 37.33
7. Oregon – 37.14
8. Arizona – 36.61
9. New Hampshire – 34.71
10. California – 34.27

Table 4 compares differences between the dollar loss per incident and the various complainant demographics. Males reported greater dollar losses than females (ratio of over $2.00 dollars to every $1.00 dollar). Individuals between the ages of 20-29 reported higher losses than other age groups.

Table 4: Amount Lost Per Referred Complaint By Selected Complainant Demographics

Complainant Demographics	*Average (median) $ Loss per Typical Complaint*
Male	$385.00
Female	$178.00
Under 20	$300.00
20-29	$348.00
30-39	$299.00
40-49	$300.00
50-59	$318.00
60 and older	$308.50

Map 3 - Top Ten States by Count: Individual Complainants (Number is Rank)



Top Ten States - Complainant

1. California – 14.8%
2. Florida – 7.7%
3. Texas – 6.2%
4. New York – 6.2%
5. Pennsylvania – 4.0%
6. Illinois – 3.9%
7. Ohio – 3.2%
8. New Jersey – 3.2%
9. Michigan – 3.1%
10. Virginia – 2.9%

Map 4 - Top Ten Countries by Count: Individual Complainants (Number is Rank)

Top Ten Countries - Complainant

1. United States – 93.0%
2. Canada – 2.7%
3. Australia – .7%
4. Great Britain – .6%
5. Germany – .2%
6. Japan – .2%
7. Netherlands – .2%
8. France – .1%
9. Hong Kong – .1%
10. Singapore – .1%

Complainant-Perpetrator Dynamics

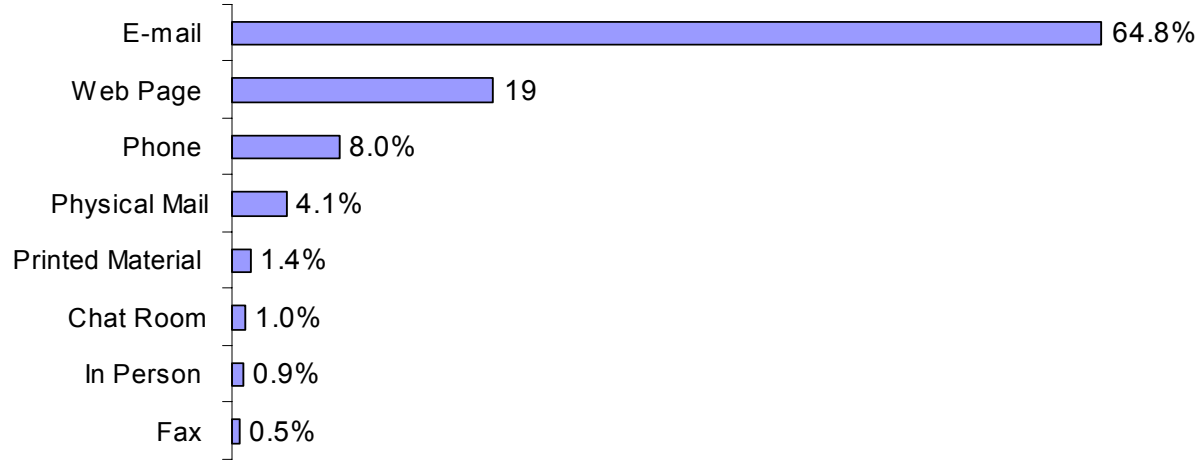
One of the components of fraud committed via the Internet that makes investigation and prosecution difficult is that the offender and victim may be located anywhere worldwide. This is a unique characteristic not found with many other types of "traditional" crime. These jurisdictional issues often require the cooperation of multiple agencies to resolve a given case. Table 5 highlights this truly "borderless" phenomenon. Even in California, where most fraud of the reported fraud cases originated, only 20.3% of all cases involved both a complainant and perpetrator residing in the same state. Other states have an even smaller percentage of complainant-perpetrator similarities in residence. These patterns not only indicate "hot spots" of perpetrators (California for example) that target potential victims from around the world, but also indicate that complainants and perpetrators may not have a relationship prior to the incident.

Table 5: Perpetrators From Same State as Complainant (Other top three locations in parentheses)

State	*%*	*1*	*2*	*3*
1. California	21.0%	1. New York (10.9%)	1. Florida (8.2%)	1. Texas (6.4%)
2. Florida	13.6%	2. California (13.7%)	2. New York (11.0%)	2. Texas (6.2%)
3. Texas	10.7%	3. California (14.3%)	3. New York (9.8%)	3. Florida (8.8%)
4. New York	13.0%	4. California (15.7%)	4. Florida (9.1%)	4. Texas (5.4%)
5. Pennsylvania	6.7%	5. California (14.8%)	5. Florida (10.1%)	5. New York (9.6%)
6. Illinois	6.7%	6. California (15.4%)	6. New York (11.1%)	6. Florida (8.7%)
7. Ohio	6.0%	7. California (14.4%)	7. New York (10.0%)	7. Florida (9.3%)
8. New Jersey	5.5%	8. California (15.8%)	8. New York (11.1%)	8. Florida (8.9%)
9. Michigan	7.4%	9. California (13.9%)	9. New York (10.6%)	9. Florida (8.4%)
10. Virginia	4.5%	10. California (15.5%)	10. New York (11.8%)	10. Florida (10.3%)

Another factor that impedes the investigation and prosecution of Internet crime is the anonymity afforded by the Internet. Chart 7 illustrates how complainants and perpetrators in the cases reported rarely interacted face-to-face. The majority of perpetrators were in contact with the complainant through e-mail (64.8%) or a webpage (19.4%). A mere 8.0% had phone contact with the complainant and 4.1% had corresponded through the physical mail. Interaction through chat rooms (1.0%) and in-person meetings (0.9%) was rarely reported. The anonymous nature of an e-mail address or website allows perpetrators to solicit a large number of victims with a keystroke.

Chart 7
Contact Method



Additional Information About IC3 Referrals

Although IC3 is dedicated to specifically addressing complaints about Internet crime, it also receives complaints about other crimes. These include violent crimes, robberies, burglaries, threats, and many other violations of law. The people submitting these types of complaints are generally directed to make immediate contact with their local law enforcement agency in order to secure a timely and effective response to their particular needs. If warranted, the IC3 personnel may make contact with local law enforcement authorities on behalf of the complainant. IC3 also receives a substantial number of computer-related offenses that are not fraudulent in nature. It is estimated that 3.6% of all complaints received are computer intrusion/hacking, 5.4% are related to spam, and 0.6% involve child pornography.

For those complaints that *are* computer-related but not considered Internet fraud, IC3 routinely refers these to agencies and organizations that handle those particular violations. For example, if IC3 receives an allegation of the distribution of child pornography via the Internet, the complaint information would immediately be forwarded to the National Center for Missing and Exploited Children (http://www.ncmec.org/) and to the Baltimore FBI office, which coordinates all child pornography investigations nationwide through the Innocent Images initiative. Likewise, allegations of computer intrusion would be passed on to the National Infrastructure Protection Center, Department of Defense, FBI and other agencies. Spam complaints and cases of identity theft are forwarded to the Federal Trade Commission and referred to other government agencies with venue. Because the aforementioned complaints are forwarded to agencies, they are not tracked as fraud referrals in the IC3 database. All complaints are reviewed and handled with importance. Every effort is made to direct the complainant's information to the appropriate responding agency.

Results of IC3 Referrals

IC3 routinely receives updates on the disposition of referrals from agencies receiving complaints. This includes documented arrests and restitution, as well as updates related to ongoing investigations, pending cases, and arrest warrants. However, IC3 can only gather this data from the agencies that voluntarily return enforcement results, and it has no authority to require agencies to submit or return status forms.

IC3 has assisted law enforcement with many successful case resolutions. Some of the most recent cases include the following:

- Cody Hill was arrested and charged with grand theft and having a weapons violation from a previous arrest.[2] Sonoma County Sheriff's detectives began their investigation after receiving complaint referrals from IC3 and consumers who never received cars they had sent money for.[3] According to authorities, Hill would post bogus cars and truck ads on eBay and right before the auction would close he would contact bidders asking if they would like to buy the vehicle directly from him rather than going through eBay. After a price was negotiated the victims would then wire the money to banks in Sonoma County.[4] Detectives from Sonoma County believe Hill probably worked with other Internet scam artists and that there are probably more victims who may have lost hundreds of thousands of dollars. So far it is believed that Hill has bilked victims for over $100,000, but investigators say that figure could rise by the end of the investigation.[5]

- IC3 has learned that a complaint regarding Robert Fulcher has now been resolved. IC3 started receiving complaints about Fulcher in early February 2004. The complaints were analyzed and sent to Officer Sha King for investigation. Police Officer Sha King from the Stephenville Police Department in Texas said that 80 people throughout the United States lost more than $30,000 by sending money orders and cashiers checks to Fulcher, but never received any of the computers they were promised. Fulcher's auction site, which carried his name and address, offered Dell Computers varying in prices from $260 to as much as $4,600.[6] Officer King

[2] http://www.nctimes.com/articles/2004/04/07/news/state/4_6_0422_26_18.prt
[3] Ibid.
[4] http://www.eauctiontimes.com/
[5] http://www.nctimes.com/articles/2004/04/07/news/state/4_6_0422_26_18.prt
[6] http://www.dfw.com/mld/dfw/news/state/8606007.htm?1c

went to Fulcher's house to make sure his account was not being used without his knowledge and to see if he had any of the alleged merchandise that was being sold. After determining that Fulcher's account had not been jeopardized, Officer King asked to see the merchandise that was being sold through eBay which Fulcher could not produce.[7] Since then, the 23 year old suspect from Texas was released on bail and is awaiting trail on suspicion of theft of over $30,000.

- United States Postal inspectors arrested Scott Winingear, of Mobile, Alabama, for a suspected Internet fraud ring involving nearly $20,000 in laptop computers that were never delivered to their buyers.[8] Last spring, Winingear started an elaborate Internet scheme by advertising Toshiba computers for sale and allegedly using the name of his then roommate "T.J. Walsh" as an alias. Buyers were then duped to send the checks or money orders to a post office box in Mobile, Alabama from which Winingear then deposited the money into a savings account.[9] Investigators believe that at least 20 people around the country paid between $850-$900 for the laptops using the auction site eBay.com.[10] Complaints against Winingear, aka "TJ Walsh," started arriving at IC3 in May of 2003 and were sent to the Mobile Police Department for investigation. Winingear's arraignment is set for February 11, 2004 in the U.S. District Court in Mobile.[11]

- Police have arrested Bradley Godin and Robert Hollingsworth of Jackson County, Mississippi. The two were at the post office picking up mail that contained checks and money orders from eBay customers. Investigators allege the pair advertised video game systems and other merchandise online and had victims send checks and money orders to two addresses in Jackson County.[12] Investigators also reported that the pair is responsible for breaking into mail collection boxes outside the post office and taking mail from individual roadside mailboxes. Investigators say that the two kept any cash they found and used personal financial information they found to set up other eBay accounts.[13] Sheriff's Department Investigator Sgt. Ricky Jones said the arrests were made after a lengthy investigation into reports of fraud. Sgt. Jones reported that the pair took at least $10,000 from 100 victims during the scam and that the number of victims and money lost may be greater and other counts may be pending.[14] IC3 first started receiving complaints about the two back in April of 2003. The information was then sent to the Jackson FBI office where it ultimately reached detectives in Jackson County. Currently Godin and Hollingsworth are being held at the Jackson County Jail on $50,000 bond each.

- Based on IC3 complaints, the Sacramento Valley Hi-Tech Crime Task Force was able to develop enough probable cause to obtain a search warrant for 3848 McHenry Ave Modesto, California, the residence of Wayne Christopher Mitchell. After executing the warrant, detectives were able to recover stolen property, narcotics, computers, identity theft materials and $10,000 in cash.[15] Police say that a fraud investigation into phony digital camera sales on the Internet led them to a different type of crime. After police entered the residence as part of their fraud investigation, officers were overwhelmed by the heat lamps being used to grow marijuana. After a search of the residence, investigators found mature plants and other packaged marijuana ready for distribution. The raid also turned up evidence of Internet fraud, which included information that Mitchell had victimized more than 20 people from across the United States. Mitchell was then arrested and booked at the Stanislaus County Jail on suspicion of drug charges, theft and fraud. His trial date has not been set.

[7] Ibid.
[8] http://www.al.com/news/mobileregister/index.ssf?/base/news/1075457904286070.xml
[9] Ibid.
[10] Ibid.
[11] Ibid.
[12] http://www.leadercall.com/articles/2004/01/11/news/news07.txt
[13] Ibid.
[14] Ibid.
[15] Detective Sergeant Adam E. Christianson

Conclusion

The IC3 report has outlined many of the current trends and patterns in Internet crime. The data indicate that fraud reports are increasing, with 124,515 complaints in 2003, up from 75,063 in 2002. This total includes many different fraud types and non-fraudulent complaints. Yet, research indicates that only one in ten incidents of fraud ever make their way to the attention of enforcement or regulatory agencies[16]. Additionally, IC3 referred 1.31% as many complaints of fraud for investigation in 2003, the majority of which was committed over the Internet or similar online service. The total dollar loss from all referred cases of fraud was more than twice as high as in 2002, up to $125.6 million from $54 million in 2002.

Internet auction fraud was again the most reported offense followed by non-deliverable merchandise/payment, and credit/debit card fraud. Among those individuals who reported a dollar loss from the fraud, the highest median dollar losses were found among Nigerian letter fraud victims ($5,496), confidence fraud victims ($6,850), and check fraud victims ($4,550). Male complainants reported greater losses than female complainants, which may be a function of both online purchasing differences by gender and the type of fraud. Comparing data from the 2002 and the 2003 reports, e-mail and web pages were the two primary mechanisms by which the fraudulent contact took place. In all, almost two-thirds of all complainants reported they had e-mail contact with the perpetrator.

Although this report can provide a snapshot of the prevalence and impact of Internet fraud, care must be taken to avoid drawing conclusions about the "typical" victim or perpetrator of these types of crimes. Anyone who utilizes the Internet is susceptible, and IC3 has received complaints from both males and females ranging in age from ten to one hundred years old. Complainants can be found in all fifty states, in dozens of countries worldwide, and have been affected by everything from work-at-home schemes to identity theft. Although the ability to predict victimization is limited, particularly without the knowledge of other related risk factors (e.g., the amount of Internet usage or experience), many organizations agree that education and awareness are major tools to protect individuals. Despite the best proactive efforts, some individuals may find themselves the victims of computer-related criminal activity even when following the best prevention strategies (see Appendix II).

Over the past year, the IC3 has begun to update/change its method of gathering data regarding complaints, in recognition of the constantly changing nature of cyber crime, and to more accurately reflect meaningful trends. You will soon see a change to the IC3 website and complaint form with this in mind.

In reviewing statistics contained in this report, it is recognized that consumers may characterize crime problems with an easier "broad" character, which may be misleading. For instance, a consumer that gets lured to an auction site, which appears to be eBay, may later find that they were victimized through a cyber scheme. The scheme may in fact have involved SPAM, unsolicited e-mail inviting them to a site, and a "spoofed" website which only imitated the true legitimate site. The aforementioned crime problem could be characterized as SPAM, phishing, possible identity theft, credit card fraud or auction Fraud. In such scenarios, many complainants have depicted schemes such as auction fraud even though that label may be incomplete or misleading.

It is also important to note that the IC3 has actively sought support from many key Internet E-Commerce stake holders over the past several years. With these efforts companies like eBay have adopted a very pro-active posture in teaming with the IC3 to identify and respond to cyber crime schemes. As part of these efforts, eBay and other companies have provided guidance and/or links for their customers to the IC3 website. This activity has no doubt also contributed to an increase in referrals regarding schemes depicted as "auction fraud".

Whether a bogus investment offer, a dishonest auction seller, or a host of other Internet crimes, the Internet Crime Complaint Center is in the position to offer assistance. Through the online complaint and referral process, victims of Internet crime are provided with an easy way to alert authorities, at many different jurisdictional levels, of a suspected criminal or civil violation.

[16] National White Collar Crime Center, *The National Public Survey on White Collar Crime*, February 2000.

Appendix I
Explanation of Complaint Categories

Although the transition to IC3 better reflects the processing of Internet crime complaints, the fraud complaint categories were still used during 2003 to categorize complaint information. IC3 Internet Fraud Analysts determined a fraud type for each Internet fraud complaint received and sorted complaints into one of nine fraud categories.

- Financial Institution Fraud - Knowing misrepresentation of the truth or concealment of a material fact by a person to induce a business, organization, or other entity that manages money, credit, or capital to perform a fraudulent activity. [17] Credit/debit card fraud is an example that ranks among the most commonly reported offenses to IC3. Identity theft also falls into this category; cases classified under this heading tend to be those where the perpetrator possesses the complainants true name identification (in the form of a social security card, driver's license, or birth certificate), but there has not been a credit or debit card fraud committed.

- Gaming Fraud - To risk something of value, especially money, for a chance to win a prize when there is a misrepresentation of the odds or events.[18] Sports tampering and claiming false bets are two examples of gaming fraud.

- Communications Fraud - A fraudulent act or process in which information is exchanged using different forms of media. Thefts of wireless, satellite, or landline services are examples of communications fraud.

- Utility Fraud - When an individual or company misrepresents or knowingly intends to harm by defrauding a government regulated entity that performs an essential public service, such as the supply of water or electrical services.[19]

- Insurance Fraud - A misrepresentation by the provider or the insured in the indemnity against loss. Insurance fraud includes the "padding" or inflating of actual claims, misrepresenting facts on an insurance application, submitting claims for injuries or damage that never occurred, and "staging" accidents.[20]

- Government Fraud - A knowing misrepresentation of the truth, or concealment of a material fact to induce the government to act to its own detriment.[21] Examples of government fraud include tax evasion, welfare fraud, and counterfeit currency.

- Investment Fraud - Deceptive practices involving the use of capital to create more money, either through income-producing vehicles or through more risk-oriented ventures designed to result in capital gains.[22] Ponzi/Pyramid schemes and market manipulation are two types of investment fraud.

- Business Fraud - When a corporation or business knowingly misrepresents the truth or conceals a material fact.[23] Examples of business fraud include bankruptcy fraud and copyright infringement.

- Confidence Fraud - The reliance on another's discretion and/or a breach in a relationship of trust resulting in financial loss. A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.[24] Auction fraud and non-delivery of payment or merchandise are both types of confidence fraud and are the most reported offenses to IC3. The Nigerian Letter Scam is another offense classified under confidence fraud.

---

[17] Black's Law Dictionary, Seventh Ed., 1999.
[18] Ibid.
[19] Ibid.
[20] Fraud Examiners Manual, Third Ed., Volume 1, 1998.
[21] Black's Law Dictionary, Seventh Ed., 1999. The Merriam Webster Dictionary, Home and Office Ed., 1995.
[22] Barron's Dictionary of Finance and Investment Terms, Fifth Ed., 1998.
[23] Black's Law Dictionary, Seventh Ed., 1999.
[24] Ibid.

Appendix II
Best Practices to Prevent Internet Crime

Internet Auction Fraud

Prevention tips:

- Understand as much as possible about how Internet auctions works, 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 30 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 (http://www.usps.com/websites/depart/inspect).
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 web sites regarding this person/company.
- Do not judge a person/company by their fancy web site; 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.
- Make sure the web site 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 site 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 the site, check out the security software it uses make sure 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 web sites 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:

- Don't 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. Sending an e-mail requesting additional information before you process the order asking for: a non-free 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're 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:

- Don't invest in anything based on appearances. Just because an individual or company has a flashy web site 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.
- Don't 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 web sites 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
- 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 throw out, especially those with sensitive or identifying information.
- Be suspicious of telephone solicitors. Never provide information unless you have initiated the call.
- Delete without replying to any suspicious e-mail requests.

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 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, 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 net 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.

Appendix III
Complainant/Perpetrator Statistics, by State

Complainants By State
Represents % of total individual complainants where state is known

1	California	14.8	**27**	Louisiana	1.1
2	Florida	7.7	**28**	South Carolina	1.0
3	Texas	6.2	**29**	Alabama	1.0
4	New York	6.2	**30**	Kansas	1.0
5	Pennsylvania	4.0	**31**	Utah	.9
6	Illinois	3.9	**32**	Nevada	.8
7	Ohio	3.2	**33**	Iowa	.8
8	New Jersey	3.2	**34**	Hawaii	.7
9	Michigan	3.1	**35**	West Virginia	.6
10	Virginia	2.9	**36**	Arkansas	.6
11	Washington	2.8	**37**	New Hampshire	.5
12	Georgia	2.5	**38**	New Mexico	.5
13	Arizona	2.5	**39**	Mississippi	.5
14	Massachusetts	2.3	**40**	Nebraska	.5
15	Colorado	2.2	**41**	Idaho	.5
16	North Carolina	2.1	**42**	Maine	.4
17	Maryland	2.1	**43**	Rhode Island	.4
18	Indiana	1.9	**44**	Montana	.3
19	Missouri	1.8	**45**	Alaska	.3
20	Wisconsin	1.8	**46**	District of Columbia	.3
21	Tennessee	1.7	**47**	Delaware	.3
22	Oregon	1.6	**48**	Vermont	.2
23	Minnesota	1.5	**49**	North Dakota	.2
24	Connecticut	1.4	**50**	Wyoming	.2
25	Kentucky	1.2	**51**	South Dakota	.2
26	Oklahoma	1.1			

- Please note that percentages contained in the table above may not add up to 100%. The table above only represents statistics from 50 states and District of Columbia. The table above does not represent statistics from other U.S. territories or Canada.

Perpetrators By State

Represents % of total individual perpetrators where state is known

1	California	16.1	**27**	Connecticut	1.0
2	New York	10.8	**28**	Minnesota	1.0
3	Florida	9.2	**29**	Louisiana	.9
4	Texas	6.0	**30**	Oklahoma	.8
5	Pennsylvania	3.8	**31**	Utah	.7
6	Illinois	3.7	**32**	Kansas	.7
7	New Jersey	3.1	**33**	New Hampshire	.6
8	Ohio	3.1	**34**	Iowa	.5
9	Arizona	3.0	**35**	Maine	.5
10	Georgia	2.7	**36**	Idaho	.5
11	Michigan	2.7	**37**	Arkansas	.5
12	Nevada	2.5	**38**	Rhode Island	.4
13	Washington	2.4	**39**	West Virginia	.4
14	Tennessee	2.1	**40**	Mississippi	.4
15	North Carolina	2.0	**41**	Hawaii	.3
16	Maryland	1.9	**42**	Nebraska	.3
17	Virginia	1.8	**43**	New Mexico	.2
18	Indiana	1.6	**44**	Delaware	.2
19	Missouri	1.6	**45**	Montana	.2
20	Massachusetts	1.4	**46**	District of Columbia	.2
21	Colorado	1.4	**47**	Vermont	.2
22	Oregon	1.3	**48**	Alaska	.2
23	Wisconsin	1.2	**49**	Wyoming	.1
24	Alabama	1.2	**50**	South Dakota	.1
25	South Carolina	1.1	**51**	North Dakota	.09
26	Kentucky	1.0			

- Please note that percentages contained in the table above may not add up to 100%. The table above only represents statistics from 50 states and District of Columbia. The table above does not represent statistics from other U.S. territories or Canada

Complainants per 100,000 population (based on 2003 Census figures)

1	District of Columbia	44.02	**27**	Pennsylvania	26.96
2	Hawaii	43.50	**28**	Delaware	26.79
3	Colorado	40.57	**29**	New York	26.45
4	Alaska	40.00	**30**	Wisconsin	26.42
5	Washington	37.36	**31**	Indiana	25.78
6	Florida	37.33	**32**	Missouri	25.73
7	Oregon	37.14	**33**	Illinois	25.62
8	Arizona	36.61	**34**	Michigan	25.57
9	New Hampshire	34.71	**35**	Minnesota	25.54
10	California	34.27	**36**	Oklahoma	24.95
11	Connecticut	33.96	**37**	Georgia	24.03
12	Virginia	32.44	**38**	Kentucky	23.97
13	Utah	31.98	**39**	Tennessee	23.66
14	Maryland	31.73	**40**	Texas	23.22
15	Wyoming	31.12	**41**	Ohio	23.16
16	Rhode Island	30.85	**42**	Nebraska	22.77
17	New Jersey	30.63	**43**	Iowa	22.15
18	Nevada	30.61	**44**	New Mexico	22.03
19	Massachusetts	29.92	**45**	North Carolina	21.05
20	Kansas	28.93	**46**	South Carolina	19.92
21	Montana	28.77	**47**	Louisiana	19.33
22	Vermont	28.75	**48**	South Dakota	18.97
23	Idaho	28.69	**49**	Alabama	18.44
24	West Virginia	28.45	**50**	Arkansas	18.34
25	Maine	27.57	**51**	Mississippi	13.99
26	North Dakota	27.45			

- Please note that percentages contained in the table above may not add up to 100%. The table above only represents statistics from 50 states and District of Columbia. The table above does not represent statistics from other U.S. territories or Canada.

Perpetrators per 100,000 population (based on 2003 Census figures)

1	Nevada	41.85	**27**	Hawaii	10.10
2	New York	21.34	**28**	Alabama	10.04
3	Florida	20.32	**29**	Delaware	10.03
4	Arizona	19.84	**30**	Indiana	9.96
5	California	17.04	**31**	Michigan	9.87
6	New Hampshire	16.15	**32**	Wyoming	9.58
7	Rhode Island	15.33	**33**	South Carolina	9.55
8	Washington	14.97	**34**	Virginia	9.37
9	Maine	14.09	**35**	Kentucky	9.23
10	New Jersey	13.65	**36**	Montana	8.94
11	Tennessee	13.52	**37**	Oklahoma	8.89
12	Oregon	13.51	**38**	North Carolina	8.81
13	Idaho	13.32	**39**	Alaska	8.79
14	Maryland	12.71	**40**	Massachusetts	8.38
15	District of Columbia	12.60	**41**	Wisconsin	8.28
16	Utah	11.78	**42**	West Virginia	8.23
17	Colorado	11.56	**43**	Louisiana	7.76
18	Georgia	11.49	**44**	Minnesota	7.25
19	Pennsylvania	11.42	**45**	Iowa	6.96
20	Illinois	10.88	**46**	Arkansas	6.57
21	Vermont	10.66	**47**	Nebraska	6.15
22	Connecticut	10.62	**48**	North Dakota	5.36
23	Missouri	10.61	**49**	South Dakota	4.97
24	Ohio	10.29	**50**	New Mexico	4.96
25	Texas	10.23	**51**	Mississippi	4.72
26	Kansas	10.13			

- Please note that percentages contained in the table above may not add up to 100%. The table above only represents statistics from 50 states and District of Columbia. The table above does not represent statistics from other U.S. territories or Canada.

Appendix IV
Operation Cyber Sweep – Executive Summary

Operation Cyber Sweep represents a coordinated initiative targeting an expansive array of Cyber Crime schemes victimizing individuals and industry worldwide. This initiative highlights numerous investigations that have been successfully advanced through cooperation and coordination of law enforcement, and a growing list of industry partners.

Cases included in Operation Cyber Sweep exemplify the growing volume and character of Internet facilitated crimes confronting law enforcement, and also underscores the continuing commitment of law enforcement to aggressively pursue cyber criminals, both domestically and abroad. Historically, Cyber criminals abroad have perceived themselves as beyond the reach of U.S. authorities, and in some instanced, untouchable by their own country's law enforcement. Until recently, law enforcement and industry were consistently frustrated with the inability to effectively pursue matters in certain countries. That situation is rapidly changing, due to a concerted emphasis within DOJ to train and equip law enforcement in many of these countries, including Ghana, Nigeria and Romania. Due in large part to these efforts, certain noteworthy international successes included in Operation Cyber Sweep became possible.

Criminal schemes included in this initiative include: International re-shipping schemes, auction fraud, spoofing/phishing, credit card fraud, work at home schemes, cyber-extortion, Intellectual Property Rights (IPR), computer intrusions (hacking), economic espionage (Theft of Trade Secrets), International Money Laundering, Identity Theft, and a growing list of "traditional crimes" that have migrated on-line.

The substantial accomplishments included in this initiative are attributable to the growing number of joint cyber-crime task forces established across the U.S. Over the past year, more than 50 such task forces have either been established or significantly augmented with resources from numerous federal, state and local agencies. Enhanced industry partnerships developed in coordination with associations such as the Merchants Risk Council (MRC), the Business Software Alliance (BSA), the Software and Information Industry Association (SIIA) and the Motion Picture Association of America (MPAA) also contributed significantly to the success of this initiative. Operation Cyber Sweep has been coordinated at the Federal level with the Department of Justice, the FBI, the U.S. Postal Inspection Service, the U.S. Secret Service, the Federal Trade Commission and the Bureau of Immigration and Customs Enforcement. Numerous state and local law enforcement agencies contributed significantly to this initiative as well. State and Local participation in this effort was amplified in coordination with the National White Collar Crime Center (NW3C).

Operation Cyber Sweep included more than 100 investigations, in which more than 125,000 victims lost more than $100 million dollars. Through these investigations more than 350 subjects were targeted, resulting in 125 arrests/convictions, 70+ indictments and the execution of more than 90 search/seizure warrants. Although significant in number, these investigations represent only a fraction of the cyber crime problem, underscoring not only the need for sustained law enforcement focus, but the continuing development of expanded industry partnerships as well.

Appendix V
Operation Web Snare – Executive Summary

Operation Web Snare represents a coordinated initiative targeting an expansive array of Cyber Crime schemes victimizing individuals and industry worldwide. This initiative highlights numerous investigations that have been successfully advanced through cooperation and coordination of law enforcement, and a growing list of industry partners.

Cases included in Operation Web Snare exemplify the growing volume and character of Cyber crimes confronting law enforcement, and also underscores the continuing commitment of law enforcement to aggressively pursue Cyber criminals, both domestically and abroad. Focused efforts to pursue Cyber criminals internationally, has led to the development of enhanced proactive capabilities in several countries, and numerous investigative successes highlighted within this initiative. The development of international resources is closely coordinated with the DOJ, the U.S. State Department and a growing list of E-Commerce industry partners.

Criminal schemes included in this initiative include: criminal spam, phishing, spoofed or hijacked accounts, international re-shipping schemes, Cyber-extortion, auction fraud, credit card fraud, Intellectual Property Rights (IPR), computer intrusions (hacking), economic espionage (Theft of Trade Secrets), International Money Laundering, Identity Theft, and a growing list of "traditional crimes" that continue to migrate on-line.

The substantial accomplishments captured in this initiative are attributable to the growing number of joint Cyber-crime task forces established across the U.S. Over the past year, more than 50 such task forces have either been established or significantly augmented with resources from numerous federal, state, and local agencies. Substantial industry partnerships developed in coordination with associations such as the Direct Marketing Association (DMA), the Merchants Risk Council (MRC), the Business Software Alliance (BSA),and the Software and Information Industry Association (SIIA) also contributed significantly to the success of this initiative. Operation Web Snare has been coordinated at the Federal level with the Department of Justice, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3), the U.S. Postal Inspection Service, the U.S. Secret Service, the Federal Trade Commission and the Bureau of Immigration and Customs Enforcement. Numerous state and local law enforcement agencies contributed significantly to this initiative as well. State and Local participation in this effort was amplified in coordination with the National White Collar Crime Center (NW3C).

Operation Web Snare includes more than 150 investigations, in which more than 870,000 victims lost more than $210 million dollars. Through these investigations more than 300 subjects were targeted, resulting in 100 arrests/convictions, 116 indictments, and the execution of more than 130 search/seizure warrants. Although significant in number, these investigations represent only a fraction of the Cyber crime problem, underscoring not only the need for sustained law enforcement focus, but the continuing development of expanded industry partnerships as well.

Appendix VI
Operation Web Snare – Common Internet Fraud Schemes

Advance Fee Fraud Schemes
The victim is required to pay significant fees in advance of receiving a substantial amount of money or merchandise. 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.

Business/Employment Schemes
Typically incorporate identity theft, freight forwarding, and counterfeit check schemes. The fraudster posts 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. The fraudster uses that information to purchase merchandise on credit. The merchandise is sent to another respondent who has been hired as a freight forwarded by the fraudster. The merchandise is then reshipped out of the country. The fraudster, who has represented himself as a foreign company, then pays the freight forwarder with a counterfeit check containing a significant overage amount. The overage is wired back to the fraudster, usually in a foreign country, before the fraud is discovered.

Counterfeit Check Schemes
A counterfeit or fraudulent cashier's check or corporate check is utilized 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. One popular variation of this scam involves the purchase of automobiles listed for sale in various Internet classified advertisements. The sellers are contacted about purchasing the autos and shipping them to a foreign country. The buyer, or person acting on behalf of a buyer, then sends the seller a cashier's check for an amount several thousand dollars over the price of the vehicle. The seller is directed to deposit the check and wire the excess back to the buyer so they can pay the shipping charges. Once the money is sent, the buyer typically comes up with an excuse for canceling the purchase, and attempts to have the rest of the money returned. Although the seller does not lose the vehicle, he is typically held responsible by his bank for depositing a counterfeit check.

Credit/Debit Card Fraud
Is the unauthorized use of a credit/debit card 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
The receiving and subsequent reshipping of an on-line ordered merchandise to locations usually abroad. 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.

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.

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.

Non-delivery of Goods/Services
Merchandise or services that were purchased or contracted by individuals on-line are never delivered.

Online Auction/Retail
The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

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.

Ponzi/Pyramid Schemes
Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits. However, no investments are actually made by the so called "investment firm." Early investors are paid returns with the investment capital received from subsequent investors. The system eventually collapses and investors do not receive their promised dividends and lose their initial investment.

Spoofing/Phishing
A technique whereby a fraudster pretends to be someone else's email or web site. This is typically done by copying the web content of a legitimate web site to the fraudster's newly created fraudulent web site. Phishing refers to the scheme whereby the perpetrators use the spoofed web sites in an attempt to dope the victim into divulging sensitive information, such as passwords, credit card and bank account numbers. The victim, usually via email is provided with a hyperlink that directs him/her to a fraudster's web site. This fraudulent web site's name (Uniform Resource Locator) closely resemble the true name of the legitimate business. The victim arrives at the fraudulent web site and is convinced by the sites content that they are in fact at the company's legitimate web site and are tricked into divulging sensitive personal information. Spoofing and phishing are done to further perpetrate other schemes, including identity theft and auction fraud.