IC3 2004 Internet Fraud - Crime Report

January 1, 2004—December 31, 2004

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

Contents

The Internet Crime Complaint Center
2004 Internet Fraud Crime Report:
January 1, 2004-December 31, 2004

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 criminal matters having a cyber (Internet) nexus. The 2004 Internet Fraud Report is the fourth annual compilation of information on complaints received and referred by the IC3 to law enforcement or regulatory agencies for appropriate action. From January 1, 2004 – December 31, 2004, the IC3 website received 207,449 complaint submissions. This is a 66.6% increase over 2003 when 124,509 complaints were received. These filings were composed of fraudulent and non-fraudulent complaints primarily related to the Internet.

IC3 referred 190,143 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 103,959 complaints of fraud, the majority of which were committed over the Internet or similar online service. This is a 64.2% increase over 2003 when 63316 complaints were referred. The total dollar loss from all referred cases of fraud was $68.14 million with a median dollar loss of $219.56 per complaint. Significant findings include:

- Internet auction fraud was by far the most reported offense, comprising 71.2% of referred complaints. Non-delivered merchandise and/or payment accounted for 15.8% of complaints. Credit/debit card fraud made up 5.4% of complaints. Check Fraud, investment fraud, confidence fraud, and identity theft round out the top seven categories of complaints referred to law enforcement during the year.

- Among those individuals who reported a dollar loss, the highest median dollar losses were found among check fraud ($3600), Nigerian letter fraud ($3000), and confidence fraud ($1000) complainants.

- Among perpetrators, nearly 74.7% were male and half resided in one of the following states: California, New York, Florida, Texas, Illinois, and Ohio. The majority of reported perpetrators were from the United States. However, perpetrators also had a representation in Canada, Nigeria, United Kingdom, Italy, and Greece.

- Among complainants, 67.2% were male, nearly half were between the ages of 30 and 50 (average age 38.6) 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 (ratio of $1.97 dollars lost per male to every $1.00 dollar lost per female). This may be a function of both online purchasing differences by gender and the type of fraudulent schemes by which the individuals were victimized.

- Electronic mail (E-mail) and web pages were the two primary mechanisms by which the fraudulent contact took place. In all, 63.5% of complainants reported that they had e-mail contact with the perpetrator and 23.5% 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 employ key participants in the growing number of Cyber Crime Task Forces. Since its inception, IFCC has received complaints across a wide variety 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. In 2004 the IC3 has seen an increase in several additional crimes that are exclusively related to the Internet. Phishing, spoofing, and spam complaints have increased over the past year.

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. RECOL is a collaboration similar to IC# in that the NW4C and the Royal Canadian Mounted Police (RCMP) formed an initiative for Internet crime referrals. "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 coordinated by the U.S. Department of Justice are Operation Cyber Sweep and Operation Web Snare. These operations represent coordinated initiatives targeting an expansive array of cyber crime schemes victimizing individuals and industry worldwide.

Overall, the "IC3 2004 Internet Fraud Crime Report" is the fourth 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, 2004 – December 31, 2004, there were 207,449 complaints filed online with IC3. This is a 66.6% increase over 2003 when 124,509 complaints were received. There was a steady increase in the number of complaints filed for the first three quarters and a slight decline in the fourth quarter. The third quarter had a record number of 54,652 complaints filed. Additionally, complaint submissions have increased annually (see Chart 1 and

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

2). The number of complaints filed per month averaged 17,287 and an average of 15,845 (both fraudulent and non-fraudulent) complaints were referred by IC3 Internet Fraud Analysts.

During 2004, there were 190,143 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

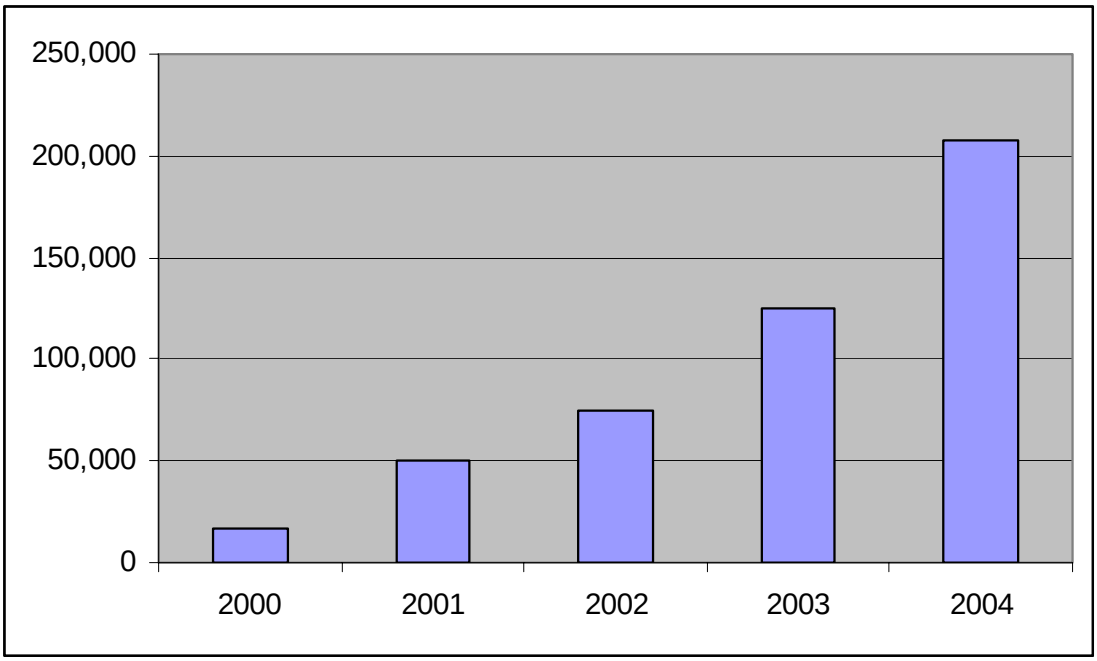
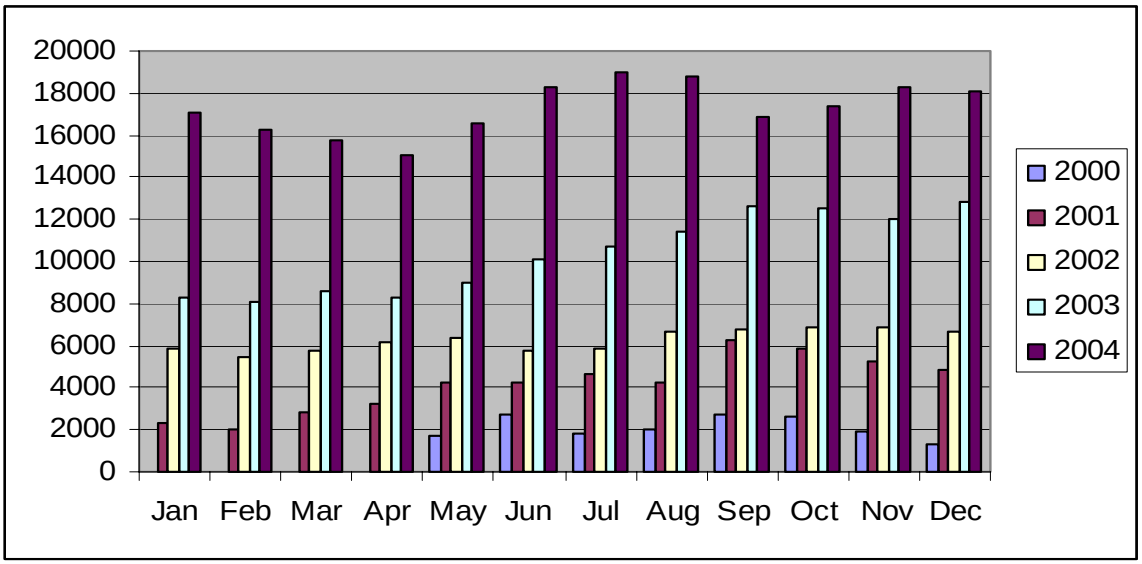


Chart 2
Monthly Comparison of Complaints Received Via IC3 Website

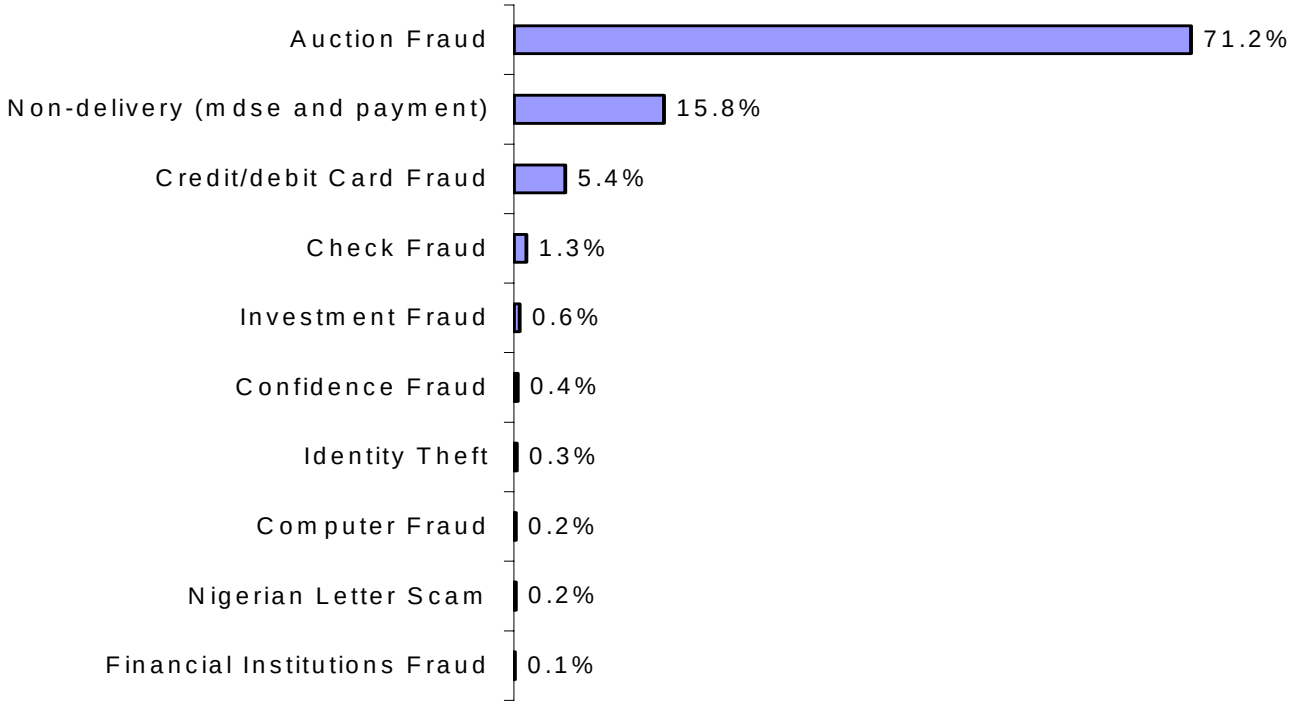


The results contained in this report were based on information that was provided to IC3 through the complaint forms submitted online at www.ic3.gov or www.ifccfbi.gov by complainants. While IC3's primary mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding cyber 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 87.7% 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 2004, there were 29 Memorandums of Understanding (MOUs) from non-NW3Cmember agencies added to the Pyramid database system and an additional 27 NW3C member agencies added to the database.

Complaint Characteristics

During 2004, Internet auction fraud was by far the most reported offense, comprising 71.2% of referred fraud complaints. This represents a 16.7% increase from the 2003 levels of auction fraud reported. In addition, during 2004, the non-delivery of merchandise and/or payment represented 15.8% of complaints (down 24.4% from 2003), and credit and debit card fraud made up an additional 5.4% of complaints (down 21.7% from 2003). Check fraud, investment fraud, and confidence fraud complaints that remained within the IC3 structure represented a mere 2.3% of all remaining complaints. Identity theft, computer fraud, Nigerian letter fraud, and financial institutions fraud complaints represented less than 0.8% of all complaints combined.

Chart 3
Top 10 IC3 Complaint Categories



Statistics contained within the complaint category must be viewed as a snapshot which may produce a misleading picture due to the perception of consumers and how they characterize their particular victimization within a broad range of complaint categories. It is also important to realize IC3 has actively sought support from many key Internet

E-Commerce stake holders and as part of these efforts many of these companies, such as eBay, have provided their customers links to the IC3 website. As a direct result an increase in referrals depicted as auction fraud has emerged.

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 2003, there were slightly lower reporting levels of all complaint types, except for auction fraud, in 2004. 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 103,959 fraudulent referrals processed by IC3 during 2004, 76,196 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 2004 was $68.14 million. That loss was significantly lower than 2003 which reported a total loss of $125.6 million, however this was a direct result of a number of cases in 2003 that reported losses in the millions of dollars. Of those complaints with a reported monetary loss, the mean dollar loss was $894.26 and the median was $219.56. Thirty-two percent (31.95%) of these complaints involved losses of less than $100, and over half (52.72%) reported a loss between $100 and $1,000. In other words, over three-fourths of these cases involved a monetary loss of less than $1,000. Very few of the complainants reported high dollar losses, with 12.31% indicating a loss between $1,000 and $5,000 and only 3.01% indicating a loss greater than $5,000. The highest dollar loss per incident was reported by check fraud victims, with a median loss of $3600. Nigerian Letter Fraud (median loss of $3000) and confidence fraud (median loss of $1000) were other high dollar loss categories. The lowest dollar loss was associated with auction fraud (median loss of $200) and Non-delivery (mdse and payment) (median loss of $264.95) offenses.

Chart 4
Percentage of Referrals by Monetary Loss

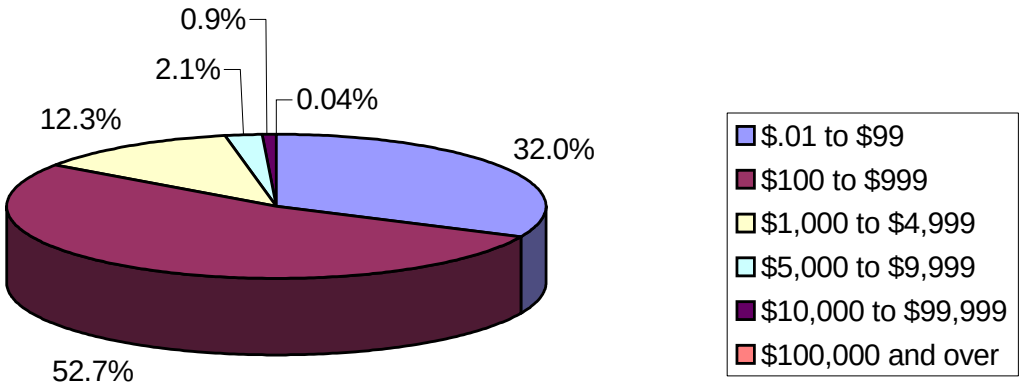


Table 1: Amount Lost by Fraud Type for Individuals Reporting Monetary Loss

Complaint Type	*% of Complainants Who Reported Dollar Loss*	*Of those who reported a loss the Average (median) $ Loss per Complaint*
Auction Fraud	87	$200.00
Non-delivery (mdse and payment)	82	$264.95
Nigerian Letter Fraud	52	$3000.00
Credit/debit Card Fraud	82	$240.00
Confidence Fraud	46	$1000.00
Investment Fraud	75	$625.57
Financial Institutional Fraud	67	$968.00
Identity Theft	30	$907.30
Check Fraud	52	$3600.00
Computer Fraud	6	$391.20

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 75% of the perpetrators were male and over half resided in one of the following states: California, New York, Florida, Texas, Illinois, and Ohio (see Map 1). These locations are among the most populous in the country. Controlling for population, Nevada, Florida, New York, Arizona, California, and Oklahoma have the highest per capita rate of perpetrators in the United States. Perpetrators also have been identified as residing in Canada, Nigeria, United Kingdom, Italy, and Greece (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, multiple 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 59.0% of the time, and the state of residence for domestic perpetrators was reported only 57.2% of the time.

Chart 5

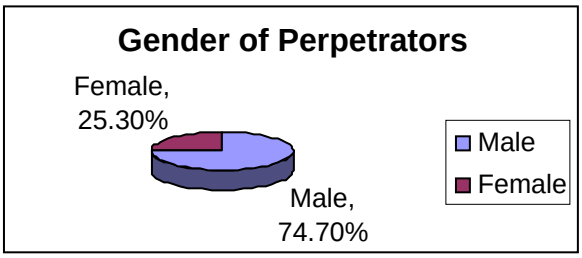
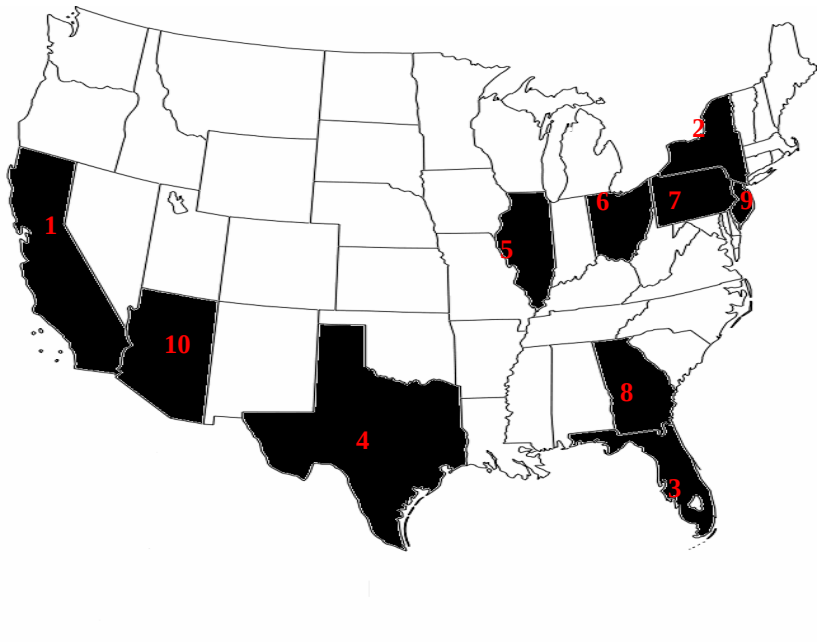


Table 2: Perpetrators per 100,000 population (based on 2004 Census figures)

1	Nevada	33.96
2	Florida	24.07
3	New York	22.49
4	Arizona	22.27
5	California	18.92
6	Oklahoma	18.16
7	Illinois	17.12
8	Delaware	16.86
9	Washington	16.80
10	Georgia	16.25

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



Top Ten States - Perpetrator

1. California – 14.9%
2. New York – 9.5%
3. Florida – 9.2%
4. Texas – 7.0%
5. Illinois – 4.8%
6. Ohio – 3.8%
7. Pennsylvania – 3.8%
8. Georgia – 3.2%
9. New Jersey – 2.9%
10. Arizona – 2.8%

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

Top Ten Countries - Perpetrator

1. United States – 78.75%
2. Canada – 3.03%
3. Nigeria – 2.87%
4. United Kingdom – 2.32%
5. Italy – 2.01%
6. Greece – 1.04%
7. Romania – .92%
8. France– .86%
9. Spain – .6%
10. China – .58%

Complainant Characteristics

The following graphs offer a detailed description of the individuals who filed an Internet fraud complaint through IC3. The complainant's average age was 38.6 years and 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, New York, Texas and Florida. Wyoming, Alaska, and Hawaii, while having a relatively small number of complaints (ranked 51st, 44th and 36th 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 Great Britain (see Map 4).

Chart 6

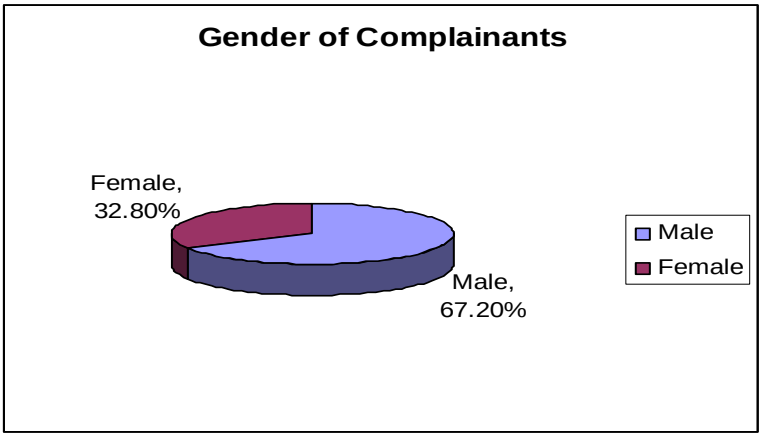


Table 3: Complainants per 100,000 population (based on 2004Census figures)

1. Alaska – 44.25
2. Arizona – 40.97
3. Washington – 39.70
4. Colorado – 39.47
5. Hawaii – 38.09
6. District of Columbia – 35.59
7. Nevada – 35.42
8. Oregon – 34.72
9. Wyoming – 34.35
10. California – 34.33

Chart 7

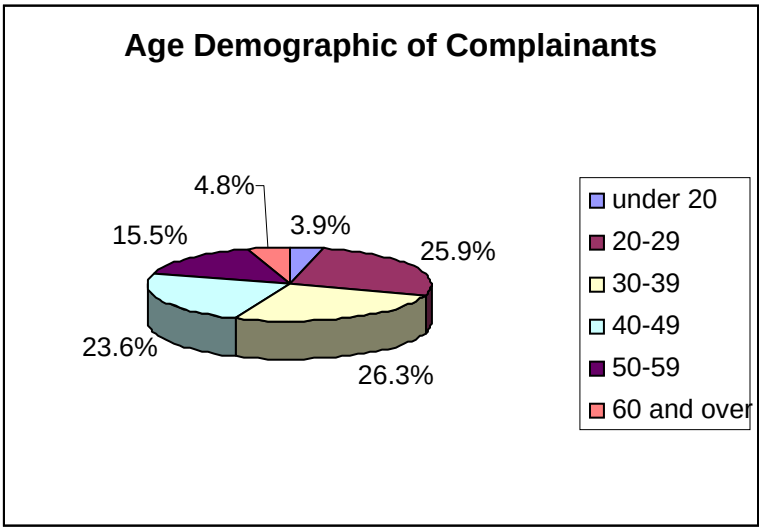
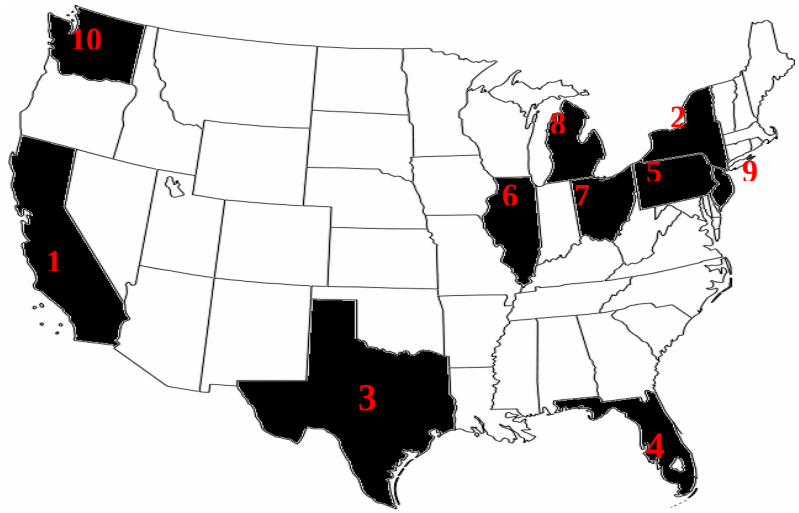


Table 4 compares differences between the dollar loss per incident and the various complainant demographics. Males reported greater dollar losses than females (ratio of $1.97 dollars to every $1.00 dollar). Individuals between the ages of 60 and older reported higher losses than other age groups.

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

Complainant Demographics	*Average (median) $ Loss per Typical Complaint*
Male	$285.00
Female	$144.00
Under 20	$225.00
20-29	$242.50
30-39	$219.99
40-49	$208.50
50-59	$212.50
60 and older	$252.50

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



Top Ten States - Complainant

1. California – 14.4%
2. New York – 6.4%
3. Texas – 6.4%
4. Florida – 6.3%
5. Pennsylvania – 4.2%
6. Illinois – 4.1%
7. Ohio – 3.4%
8. Michigan – 3.2%
9. New Jersey – 3.1%
10. Washington – 2.9%

Map 4 - Top Ten Countries by Count: Individual Complainants

Top Ten Countries - Complainant

1. United States – 92.34%
2. Canada – 2.94%
3. Australia – .74%
4. United Kingdom – .50%
5. Germany – .18%
6. Italy – .17%
7. Singapore – .16%
8. France – .15%
9. Japan – .15%
10. Netherlands – .13%

Complainant-Perpetrator Dynamics

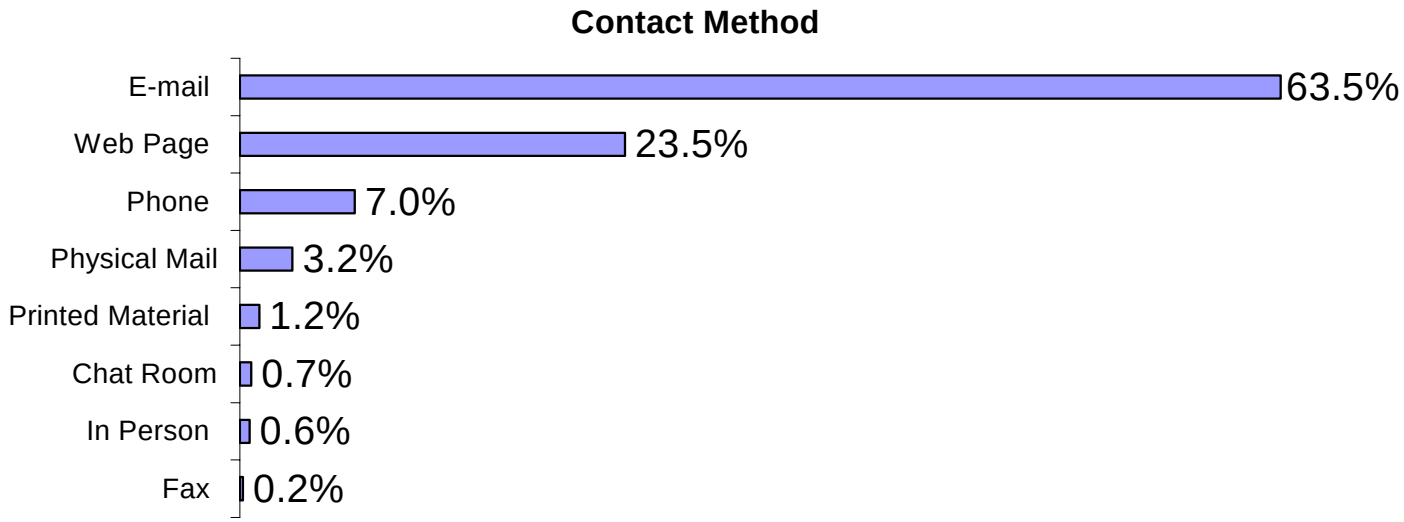
One of the components of fraud committed via the Internet that makes investigation and prosecution difficult is that the offender and victim may be located anywhere worldwide. This is a unique characteristic not found with many other types of "traditional" crime. These jurisdictional issues often require the cooperation of multiple agencies to resolve a given case. Table 5 highlights this truly "borderless" phenomenon. Even in California, where most of the reported fraud cases originated, only 21.5% 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 had 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	21.5%	1. New York (9.7%)	1. Florida (8.3%)	1. Texas (7.2%)
2. Florida	14.9%	2. California (14.4%)	2. New York (9.0%)	2. Texas (6.6%)
3. Arizona	14.6%	3. California (14.4%)	3. Texas (8.0%)	3. New York (7.1%)
4. New York	13.4%	4. California (13.7%)	4. Florida (8.8%)	4. Texas (7.3%)
5. Texas	11.7%	5. California (13.4%)	5. Florida (9.2%)	5. New York (8.7%)
6. Nevada	9.3%	6. California (16.0%)	6. Texas (9.3%)	6. New York (8.6%)
7. Washington	7.3%	7. California (15.0%)	7. Florida (8.6%)	7. Texas (7.8%)
8. Illinois	6.8%	8. California (14.4%)	8. New York (9.1%)	8. Florida (7.9%)
9. North Carolina	6.8%	9. California (13.6%)	9. New York (9.0%)	9. Florida (7.4%)
10. Tennessee	6.8%	10. California (13.1%)	10. Florida (9.2%)	10. New York (8.6%)

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 (63.5%) or a webpage (23.5%). A mere 7.0% had phone contact with the complainant and 3.2% had corresponded through the physical mail. Interaction through chat rooms (0.7%) and in-person meetings (0.6%) 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



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.

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 is immediately forwarded to the National Center for Missing and Exploited Children (http://www.ncmec.org/). Likewise, allegations of computer intrusion are 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. 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:

- Based upon a complaint received by IC3 in January 2004, the Newton Police Department (Newton, Kansas) started an investigation concerning Lisa Valdez. In the complaint, the victim claimed that Valdez had sold her an item that was never received by the victim, and the Newton Police Department began investigating the non-delivery of goods. When confronted, Valdez claimed that she had simply not had the time to ship the item because of the holidays. Valdez subsequently shipped the item, and the case was closed; however, more complaints kept coming. Additional victims filed in the following months, and Valdez's case was reopened. Further investigation revealed a complex scheme to defraud in which Valdez used multiple names to post auctions on eBay for Louis Vuitton purses that she did not have in her possession. When a bid came in, Valdez searched the Internet hoping to find purses at a lower price than that of the winning bid. However, Valdez was not able to keep up with the all the auctions that she had posted and had difficulty finding less expensive purses to send to the winning bidders. After multiple interviews, Valdez confessed to the extent of her criminal activity; she had scammed multiple victims out of a documented amount of $18,000. Additionally, a search of Valdez's banking records showed large deposits that she could not explain, except that they were the result of the fraudulent sales of the unsent purses. The eight month investigation is ongoing, but the Harvey County Attorney's Office has reviewed the case to date and expects to charge Valdez with sixteen counts of theft.

- Investigators from the Computer Crime Unit at the Baltimore Police Department (Baltimore, Maryland) were first alerted to Clark's activities by a phone call on June 7, 2004. Officers advised the victim to file a complaint on the IC3 website and to ask any other victims he was in contact with to file also. Within a two day period the department received six more IC3 complaints via the referral process. Based on these complaints, an investigation was initiated into the allegations of Clark's fraudulent use of the auction site eBay, where items were offered up for sale and then not provided to the winning bidder. The preliminary police investigation revealed that Clark had numerous homes listed in his name; however, a more thorough investigation revealed Clark's exact whereabouts, and a search and seizure warrant was issued. The warrant was executed on June 27, 2004 and Clark's eMachine was confiscated and forensically imaged in effort to support potential charges. To date the suspect has not been charged but the victims have been reimbursed.

- As a result of a complaint filed with the IC3, the Fayette County Sheriff's Office (Fayetteville, West Virginia) was able to uncover a large scale fraud scheme. After receiving an IC3 complaint about non-delivery of goods in June 2003, investigators contacted the victim and were able to obtain enough information to subpoena the records of their suspect, Bobby Joe Graham, from eBay. A review of these records found that the person, or persons, using the Graham eBay account had engaged in 271 transactions between January 1 and June 11, 2003. These transactions involved the sale of DVDs and/or VHS tapes which generated $18,448.76 in sales for the account holder. In reviewing the seller's feedback, investigators noticed that there were not only multiple buyers complaining of non-delivery of auction items but also complaints concerning the receiving of merchandise that was either copied or poor quality. Using contact information from eBay, investigators secured the cooperation of several more victims and obtained a search warrant for Graham's residence, where case supporting evidence was obtained. Faced with the evidence seized in the search and the complaints filed against him, Graham confessed solely to the fraudulent activities, even though various names and email addresses were used to perpetrate the crimes. Graham was subsequently arrested and charged with five counts of computer fraud and five counts of unlawful transfer of recorded sound for the sale and transfer of illegally copied, copyrighted material, all of these being felony charges. Graham plead guilty to one count of computer fraud and one count of the

unlawful transfer of sounds after reaching an agreement with the prosecuting attorney. On June 11, 2004 Graham was sentenced to one year in prison for each of these charges, to be served concurrently. Graham's sentence was suspended by the judge, and Graham was placed on supervised probation for three years and ordered to pay a $100 fine as well as all court costs. In addition, Graham must perform 500 hours of community service and pay restitution to his victims. Also assisting in this investigation were officers from the Mt. Hope Police Department (Mount Hope, West Virginia), the FBI and the US Attorney's Office for the Southern District of WV.

- As the result of a single large dollar complaint, the Fayette County Sheriff's Office (Fayetteville, West Virginia0 initiated an investigation into the activities of Duane Hammock. Hammock initially auctioned an airplane on the eBay auction site for $16,200; however, the winning bidder became suspicious after Hammock was sent a $2,000 deposit and was then unable to be contacted to arrange delivery of the plane. Hammock initially refused to respond to the buyer's emails, and when Hammock finally responded, he accused the bewildered buyer of harassment and announced his intention to keep the deposit and not deliver the plane. The plane was then re-listed on eBay and subsequently sold to another buyer. Further investigation revealed that Hammock had purchased the plane earlier that year for $11,000, still owing $4,000 on the balance; the title of the aircraft was in the previous owner's name, pending Hammock's payment. In addition, an inspection of the plane at a local airport also revealed that it was not in the condition described in the auction. Instead of being in "showroom" or "like-new" condition, the plane was in need of multiple repairs. Warrants were subsequently obtained charging Hammock with computer fraud. Despite numerous attempts to locate Hammock, he remained at large until an anonymous tip led police to his whereabouts. When officers of the Mt. Hope Police Department (Mount Hope, West Virginia) and the Fayette County Sheriff's Office tried to arrest Hammock he fled on a motorcycle, resulting in a chase that reached speeds in excess of 100mph before Hammock was finally apprehended at a road block set up by the Sheriff's Office. Hammock was arrested and charged with computer fraud as well as several other charges stemming from the chase. On June 15^{t}, 2004 Hammock plead guilty to a lesser charge of obtaining money under false pretenses; he was sentenced to six months in jail and fined $250 plus court costs. In addition, he was ordered to pay restitution to his victim within six months of his release from jail Hammock's jail sentence has been suspended pending payment of victim restitution.

Conclusion

The IC3 report has outlined many of the current trends and patterns in Internet crime. The data indicates that fraud reports are increasing with 207,449 complaints in 2004, up from 124,515 complaints in 2003 and 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[2]. IC3 referred 147% more complaints of fraud for investigation in 2004 when compared to 2003. The majority of which were committed over the Internet or similar online service. The total dollar loss from all referred cases of fraud was $68.14 million down from $125.6 million in 2003.

Internet auction fraud was again the most reported offense followed by non-delivered 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 check fraud victims ($3,600), confidence fraud victims ($1,000), and Nigerian Letter fraud victims ($3,000). 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 2003 and the 2004 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. With this in mind changes to the IC3 website and complaint form are forthcoming.

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 IC3 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.

[2] 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 2004 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. [3] 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.[4] 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.[5]

- 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.[6]

- Government Fraud - A knowing misrepresentation of the truth, or concealment of a material fact to induce the government to act to its own detriment.[7] 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.[8] 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.[9] 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.[10] 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.

---

[3] Black's Law Dictionary, Seventh Ed., 1999.
[4] Ibid.
[5] Ibid.
[6] Fraud Examiners Manual, Third Ed., Volume 1, 1998.
[7] Black's Law Dictionary, Seventh Ed., 1999. The Merriam Webster Dictionary, Home and Office Ed., 1995.
[8] Barron's Dictionary of Finance and Investment Terms, Fifth Ed., 1998.
[9] Black's Law Dictionary, Seventh Ed., 1999.
[10] Ibid.

Appendix II
Best Practices to Prevent Internet Crime

Internet Auction Fraud

Prevention tips:

- Understand as much as possible about how Internet auctions work, 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, after conducting thorough research on the escrow 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 website 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 a site, check out the security software it uses to make sure that 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:

- Do not 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 are 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:

- Do not invest in anything based upon 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.
- Do not 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 (Experian, Transunion, and Equifax)
- 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 discard, especially those with sensitive or identifying information.
- Be suspicious of telephone solicitors. Never provide information unless you have initiated the call.
- Delete any suspicious e-mail requests without replying.

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 that 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, Instant messages (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 Internet 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 within the United States where state is known

1	California	14.4	**27**	Alabama	1.1
2	New York	6.4	**28**	Louisiana	1.0
3	Texas	6.4	**29**	Oklahoma	1.0
4	Florida	6.3	**30**	Nevada	1.0
5	Pennsylvania	4.2	**31**	Kansas	.9
6	Illinois	4.1	**32**	Utah	.9
7	Ohio	3.4	**33**	Iowa	.9
8	Michigan	3.2	**34**	Arkansas	.7
9	New Jersey	3.1	**35**	New Mexico	.6
10	Washington	2.9	**36**	Hawaii	.6
11	Virginia	2.8	**37**	West Virginia	.5
12	North Carolina	2.8	**38**	Nebraska	.5
13	Arizona	2.7	**39**	Mississippi	.5
14	Georgia	2.4	**40**	New Hampshire	.5
15	Colorado	2.1	**41**	Idaho	.5
16	Massachusetts	2.1	**42**	Maine	.4
17	Indiana	2.1	**43**	Rhode Island	.3
18	Maryland	2.0	**44**	Alaska	.3
19	Wisconsin	1.8	**45**	Montana	.3
20	Missouri	1.8	**46**	South Dakota	.3
21	Tennessee	1.7	**47**	Delaware	.3
22	Minnesota	1.7	**48**	District of Columbia	.2
23	Oregon	1.5	**49**	Vermont	.2
24	Connecticut	1.4	**50**	North Dakota	.2
25	South Carolina	1.4	**51**	Wyoming	.2
26	Kentucky	1.2			

Perpetrators By State
Represents % of total individual perpetrators within the United States (where state is known)

1	California	14.9	**27**	South Carolina	1.0
2	New York	9.5	**28**	Alabama	1.0
3	Florida	9.2	**29**	Connecticut	0.9
4	Texas	7.0	**30**	Kansas	0.8
5	Illinois	4.8	**31**	Louisiana	0.8
6	Ohio	3.8	**32**	Utah	0.6
7	Pennsylvania	3.8	**33**	Iowa	0.6
8	Georgia	3.2	**34**	Arkansas	0.5
9	New Jersey	2.9	**35**	Mississippi	0.5
10	Arizona	2.8	**36**	Maine	0.5
11	Michigan	2.5	**37**	West Virginia	0.5
12	North Carolina	2.4	**38**	Idaho	0.4
13	Washington	2.3	**39**	Nebraska	0.3
14	Tennessee	2.0	**40**	Rhode Island	0.3
15	Virginia	1.9	**41**	Delaware	0.3
16	Maryland	1.8	**42**	New Mexico	0.3
17	Missouri	1.7	**43**	New Hampshire	0.3
18	Nevada	1.7	**44**	Hawaii	0.3
19	Indiana	1.7	**45**	Vermont	0.2
20	Massachusetts	1.5	**46**	Montana	0.2
21	Oklahoma	1.4	**47**	District of Columbia	0.2
22	Oregon	1.3	**48**	Alaska	0.2
23	Colorado	1.3	**49**	South Dakota	0.1
24	Wisconsin	1.2	**50**	North Dakota	0.1
25	Minnesota	1.2	**51**	Wyoming	0.1
26	Kentucky	1.2			

Complainants per 100,000 population (based on 2004 Census figures)

1	Alaska	44.25	**27**	South Carolina	28.30
2	Arizona	40.97	**28**	Massachusetts	28.27
3	Washington	39.70	**29**	Minnesota	27.94
4	Colorado	39.47	**30**	North Dakota	27.90
5	Hawaii	38.09	**31**	Illinois	27.82
6	District of Columbia	35.59	**32**	Michigan	27.41
7	Nevada	35.42	**33**	Rhode Island	27.30
8	Oregon	34.72	**34**	Montana	27.19
9	Wyoming	34.35	**35**	Missouri	26.38
10	California	34.33	**36**	Nebraska	26.10
11	Connecticut	34.31	**37**	Delaware	26.01
12	New Hampshire	33.55	**38**	West Virginia	25.89
13	Utah	32.77	**39**	New Mexico	25.64
14	Virginia	31.98	**40**	Ohio	25.32
15	Vermont	31.22	**41**	Iowa	25.18
16	Maryland	31.09	**42**	Maine	25.05
17	Florida	30.93	**43**	Oklahoma	24.83
18	New Jersey	30.74	**44**	Tennessee	24.83
19	Kansas	29.61	**45**	Kentucky	24.51
20	Idaho	29.14	**46**	Texas	24.20
21	Pennsylvania	28.76	**47**	Georgia	23.56
22	New York	28.54	**48**	Alabama	21.50
23	South Dakota	28.54	**49**	Arkansas	20.63
24	Wisconsin	28.53	**50**	Louisiana	19.89
25	North Carolina	28.49	**51**	Mississippi	15.67
26	Indiana	28.47			

(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 the District of Columbia. The table above does not represent statistics from other U.S. territories or Canada.)

Perpetrators per 100,000 population (based on 2004 Census figures)

1	Nevada	33.96	**27**	Indiana	12.26
2	Florida	24.07	**28**	Idaho	12.20
3	New York	22.49	**29**	Connecticut	12.16
4	Arizona	22.27	**30**	Alaska	11.75
5	California	18.92	**31**	Utah	11.64
6	Oklahoma	18.16	**32**	West Virginia	11.29
7	Illinois	17.12	**33**	Virginia	11.29
8	Delaware	16.86	**34**	South Carolina	11.20
9	Washington	16.80	**35**	Michigan	11.04
10	Georgia	16.25	**36**	Massachusetts	10.77
11	Oregon	16.25	**37**	Hawaii	10.69
12	Maine	15.56	**38**	Minnesota	10.65
13	District of Columbia	15.54	**39**	New Hampshire	10.62
14	Tennessee	15.51	**40**	Wisconsin	9.97
15	New Jersey	15.08	**41**	Alabama	9.62
16	Ohio	15.03	**42**	Montana	9.49
17	Maryland	14.93	**43**	Iowa	9.41
18	Vermont	14.16	**44**	Nebraska	8.93
19	Rhode Island	14.16	**45**	Arkansas	8.83
20	Texas	14.15	**46**	Wyoming	8.09
21	Pennsylvania	13.87	**47**	Louisiana	7.84
22	Missouri	13.80	**48**	Mississippi	7.72
23	Kansas	13.09	**49**	North Dakota	7.57
24	Kentucky	13.02	**50**	New Mexico	7.36
25	North Carolina	12.87	**51**	South Dakota	6.49
26	Colorado	12.45			

(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 the District of Columbia. The table above does not represent statistics from other U.S. territories or Canada.)

Appendix IV
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 V
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 website's name (Uniform Resource Locator) closely resembles the true name of the legitimate business. The victim arrives at the fraudulent website and is convinced by the site's content that they are in fact at the company's legitimate website and are tricked into divulging sensitive personal information. Spoofing and phishing are done to further perpetrate other schemes, including identity theft and auction fraud.