INTERNET CRIME COMPLAINT CENTER

2006

Internet Crime Report

January 1, 2006 - December 31, 2006

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

NATIONAL WHITE COLLAR CRIME CENTER

INTEGRITY QUALITY SERVICE

Contents

The Internet Crime Complaint Center
2006 Internet Fraud Crime Report:
January 1, 2006-December 31, 2006

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 2006 Internet Crime Report is the sixth annual compilation of information on complaints received and referred by the IC3 to law enforcement or regulatory agencies for appropriate action. From January 1, 2006 – December 31, 2006, the IC3 website received 207,492 complaint submissions. This is a 10.4% decrease when compared to 2005 when 231,493 complaints were received. These filings were composed of fraudulent and non-fraudulent complaints primarily related to the Internet.

In 2006, IC3 processed more than 200,481 complaints that support Internet crime investigations by law enforcement and regulatory agencies nationwide. 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. All of these complaints are accessible to federal, state, and local law enforcement to support active investigations, trend analysis, and public outreach and awareness efforts.

From the submissions, IC3 referred 86,279 complaints of crime to federal, state, and local law enforcement agencies around the country for further consideration. The vast majority of cases were fraudulent in nature and involved a financial loss on the part of the complainant. The total dollar loss from all referred cases of fraud was $198.44 million with a median dollar loss of $724.00 per complaint. This is up from $183.12 million in total reported losses in 2005. Other significant findings related to an analysis of referrals include:

- Internet auction fraud was by far the most reported offense, comprising 44.9% of referred complaints. Non-delivered merchandise and/or payment accounted for 19.0% of complaints. Check fraud made up 4.9% of complaints. Credit/debit card fraud, computer fraud, confidence fraud, and financial institutions fraud round out the top seven categories of complaints referred to law enforcement during the year.

- Of those individuals who reported a dollar loss, the highest median losses were found among Nigerian letter fraud ($5,100), check fraud ($3,744), and other investment fraud ($2,695) complainants.

- Among perpetrators, 75.2% were male and half resided in one of the following states: California, New York, Florida, Texas, Illinois, Pennsylvania and Tennessee. The majority of reported perpetrators were from the United States. However, a significant number of perpetrators where also located in United Kingdom, Nigeria, Canada, Romania, and Italy.

- Among complainants, 61.2% were male, nearly half were between the ages of 30 and 50 and one-third resided in one of the four most populated states: California, Texas, Florida, and New York. While most were from the United States, IC3 received a number of complaints from Canada, Great Britain, Australia, India, and Germany.

- Males lost more money than females (ratio of $1.69 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) (73.9%) and webpages (36.0%) were the two primary mechanisms by which the fraudulent contact took place.

- Recent high activity scams seen by IC3 include hit man scams, phishing attempts associated with spoofed sites, and counterfeit checking scams.

Overview

The Internet Crime Complaint Center (IC3), which began operation on May 8, 2000, as the Internet Fraud Complaint Center 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. IC3 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, IC3 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.

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. 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. In 2006 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.

Overall, the "IC3 2006 Internet Crime Report" is the sixth 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 law enforcement or regulatory agency.

From January 1, 2006 – December 31, 2006, there were 207,492 complaints filed online with IC3. This is a 10.4% decrease compared to 2005 when 231,493 complaints were received. The number of complaints filed per month, last year, averaged 17,291. Dollar loss of referred complaints was at an all time high in 2006, $198.44 million, compared to previous years (see Chart 4).

The number of referred complaints has seen a slight drop in the number of complaints referred in 2006 due, primarily, to a change in how zero dollar loss complaints are handled and the rise in complaints associated with federal investigations. These, 114,202 complaints that were not directly referred to law enforcement are accessible to law enforcement, used in trend analysis, and also help provide a basis for future outreach events and educational awareness programs. Typically, these complaints do not represent dollar loss but provide a picture of the types of scams that are emerging via the Internet. These complaints in large part are comprised of fraud involving reshipping, counterfeit checks, phishing, etc.

During 2006, there were 200,481 complaints processed on behalf of the complainants. This total includes various crime 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.

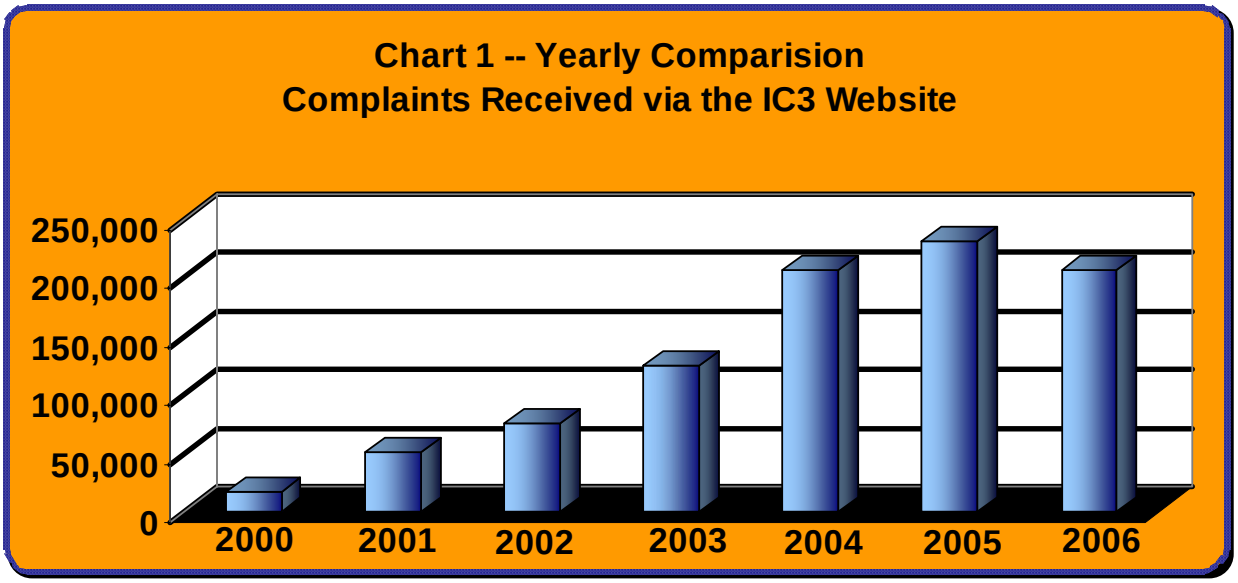


Chart 1 -- Yearly Comparision
Complaints Received via the IC3 Website
250,000
200,000
150,000
100,000
50,000
0
2000
2001
2002
2003
2004
2005
2006

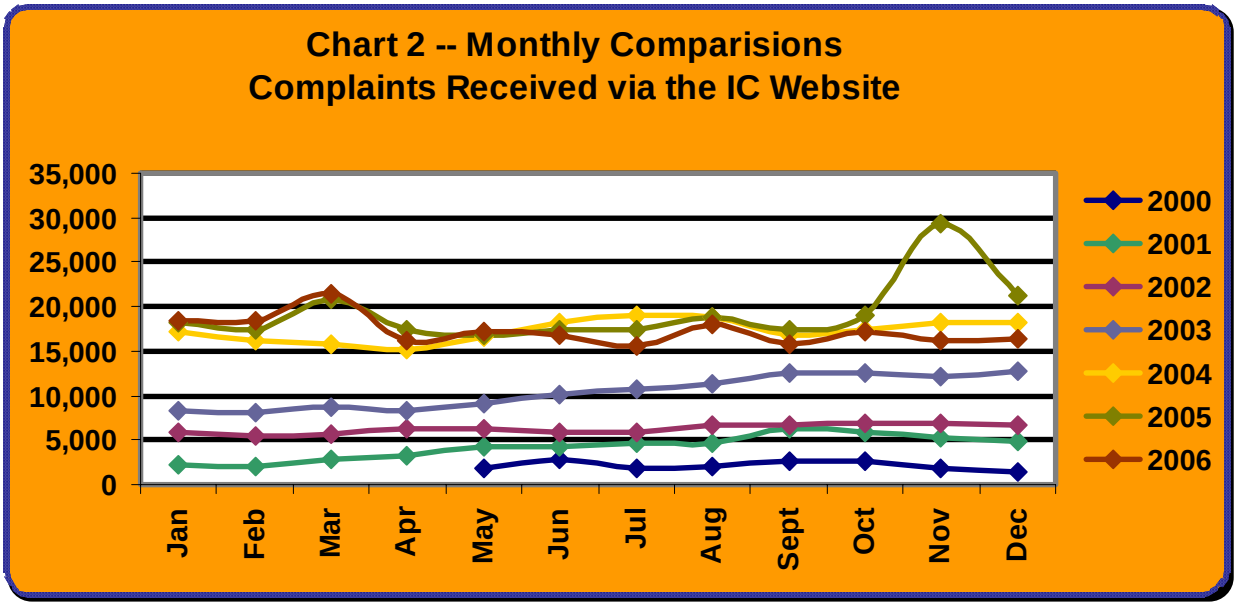
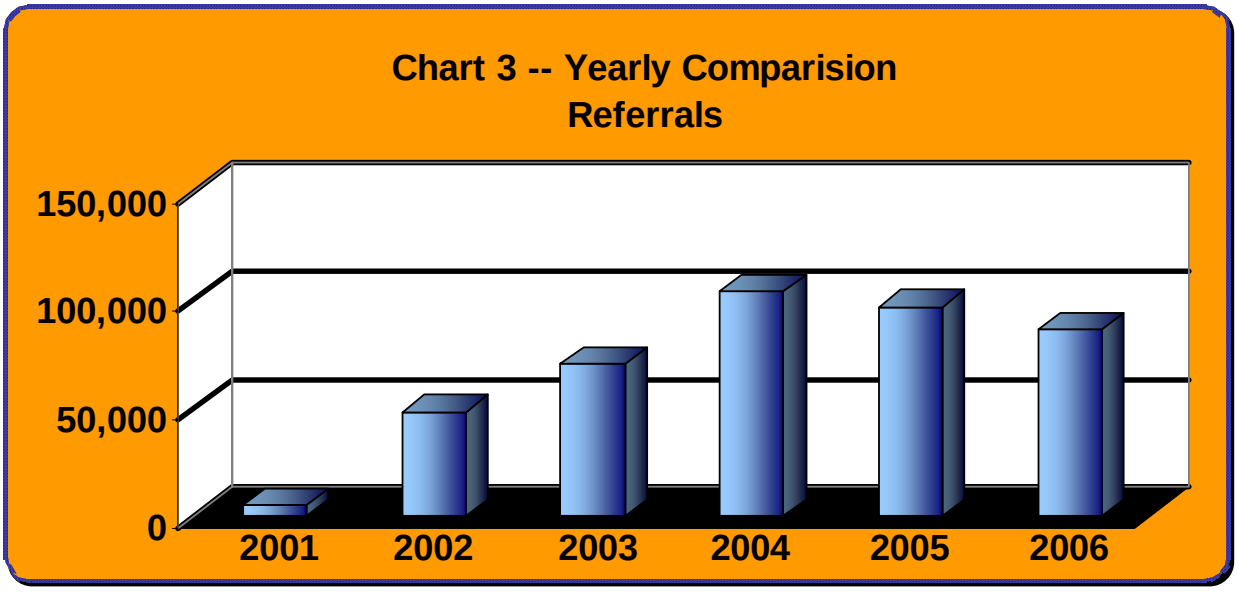
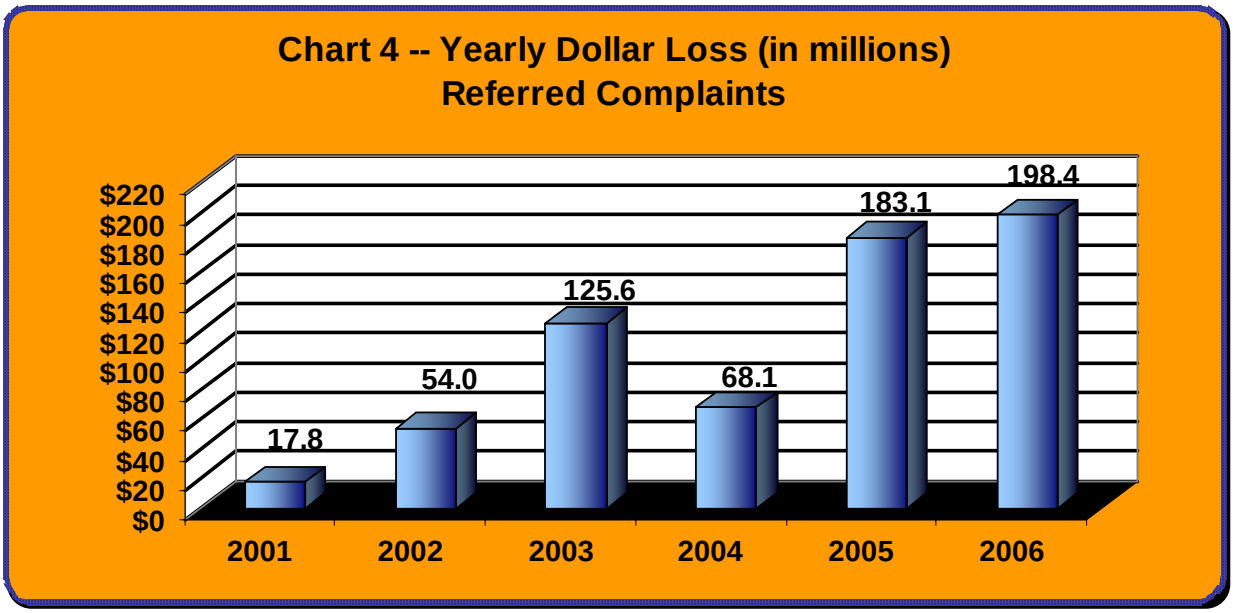


Chart 2 -- Monthly Comparisions
Complaints Received via the IC Website
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sept
Oct
Nov
Dec
2000
2001
2002
2003
2004
2005
2006

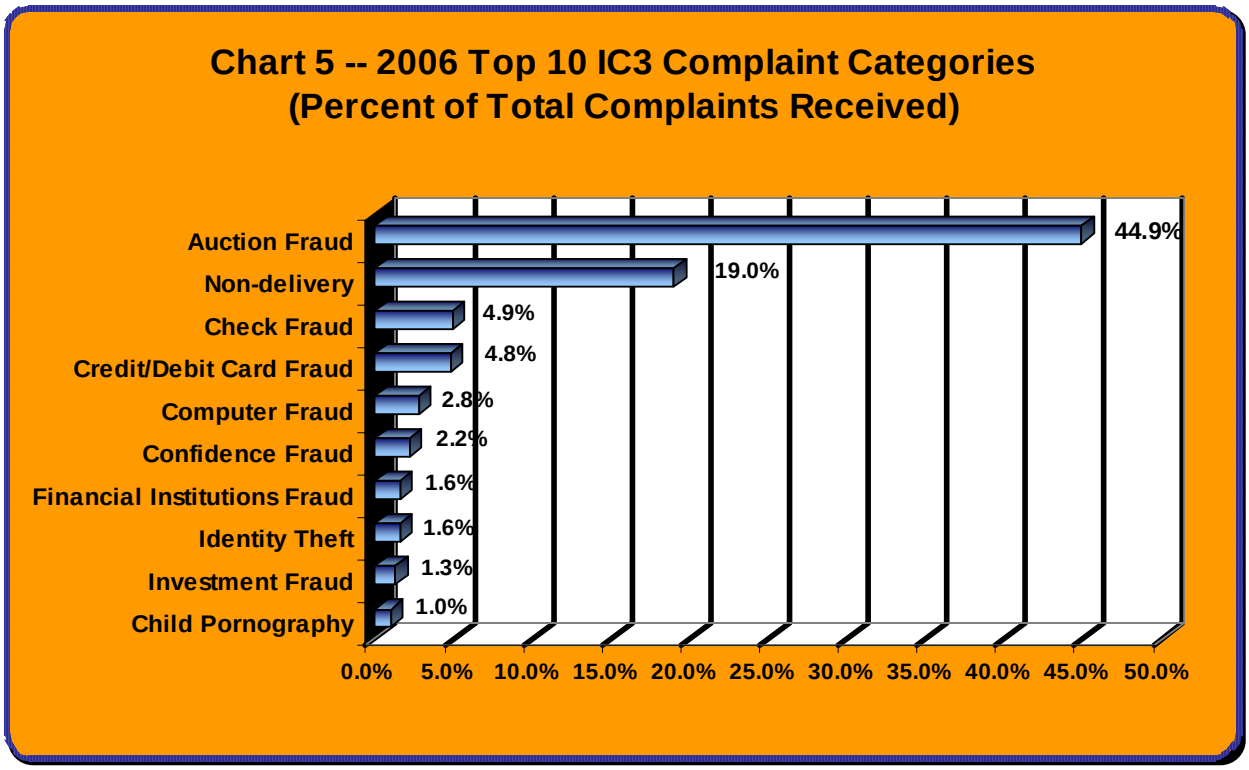




The results contained in this report were based on information that was provided to IC3 through the complaint forms submitted online at www.ic3.gov or www.ifccfbi.gov by complainants, however the data represents a sub-sample comprised of those complaints that have been referred to law enforcement. While 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 over 90% 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 2006, there were 6 Memorandums of Understanding (MOUs) from non-NW3C member agencies added to the Pyramid database system and an additional 10 NW3C member agencies added to the database.

Complaint Characteristics

During 2006, Internet auction fraud was by far the most reported offense, comprising 44.9% of referred crime complaints. This represents a 28.4% decrease from the 2005 levels of auction fraud reported to IC3. In addition, during 2006, the non-delivery of merchandise and/or payment represented 19.0% of complaints (up 21.0% from 2005), Check fraud made up an additional 4.9% of complaints which is up 2.1% from 2005 levels. Credit and debit card fraud, computer fraud, and confidence fraud complaints represented 9.8% of all remaining complaints. Other financial institutions fraud, identity theft, investment fraud, and child pornography confidence fraud complaints together represented less than 5.5% of all complaints.



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. 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.

Through its relationships with law enforcement and regulatory agencies, IC3 continues to refer specific fraud types to the appropriate agencies. Complaints received by IC3 included confidence fraud, 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. Also the Nigerian letter fraud or 419 scams are referred to the United States Secret Service. Compared to 2005, there were slightly higher reporting levels of all complaint types, except for auction fraud and credit card fraud, in 2006. For a more detailed explanation of 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 86,279 fraudulent referrals processed by IC3 during 2006, 79,230 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 2006 was $198.44 million. That loss was greater than 2005 which reported a total loss of $183.12 million. Of those complaints with a reported monetary loss, the mean dollar loss was $2529.90 and the median was $724.00. Sixteen percent (15.6%) of these complaints involved losses of less than $100.00, and (39.4%) reported a loss between $100.00 and $1,000.00. In other words, over half of these cases involved a monetary loss of less than $1,000.00. Nearly a third (31.6%) of the complainants reported losses between $1,000.00 and $5,000.00 and only 13.3% indicated a loss greater than $5,000.00. The highest dollar loss per incident was reported by Nigerian Letter Fraud (median loss of $5,100.00). Check fraud victims, with a median loss of $3,744.00 and investment fraud (median loss of $2,694.99) were other high dollar loss categories. The lowest dollar loss was associated with credit/debit card fraud (median loss of $427.50).

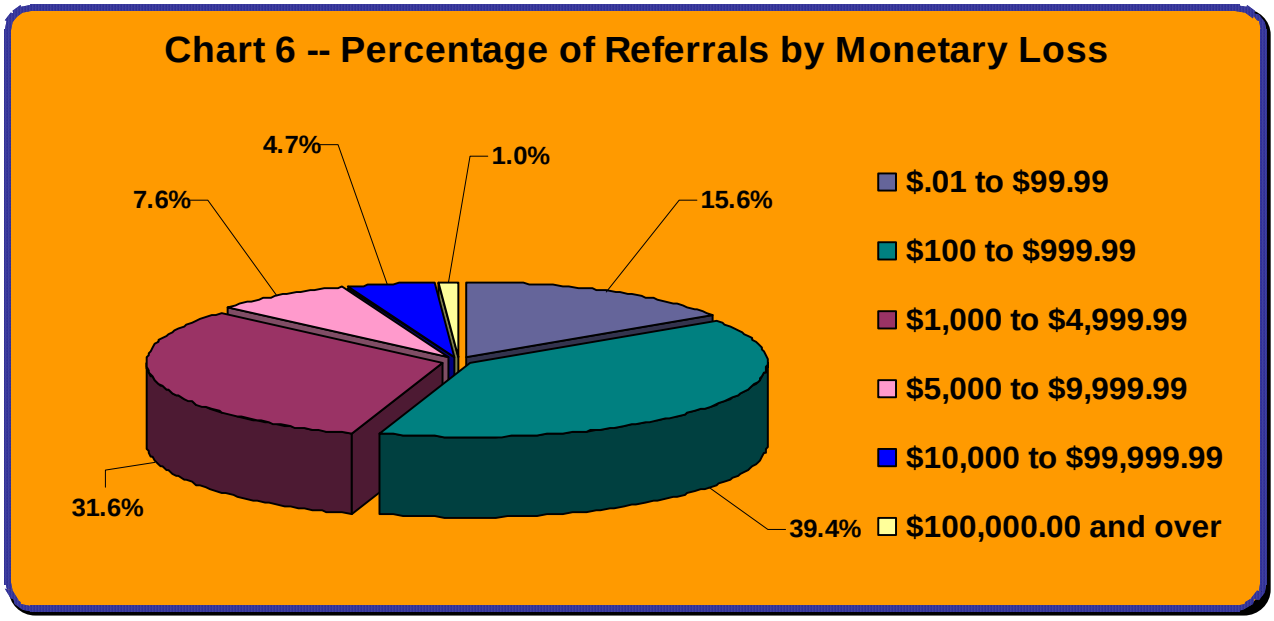


Table 1: Amount Lost by Selected Fraud Type for Individuals Reporting Monetary Loss

Complaint Type	% of Reported Total Dollar Loss	Of those who reported a loss the Average (median) $ Loss per Complaint
Nigerian Letter Fraud	1.7%	$5,100.00
Check Fraud	11.1%	$3,744.00
Investment Fraud	4.0%	$2,694.99
Confidence Fraud	4.5%	$2400.00
Auction Fraud	33.0%	$602.50
Non-delivery (mdse and payment)	28.1%	$585.00
Credit/debit Card Fraud	3.6%	$427.50

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, over 75% of the perpetrators were male and over half resided in one of the following states: California, New York, Florida, Texas, Illinois, Pennsylvania, and Tennessee (see Map 1). These locations are among the most populous in the country. Controlling for population, District of Columbia, Nevada, New York, Tennessee, Maine, and Florida have the highest per capita rate of perpetrators in the United States. Perpetrators also have been identified as residing in United Kingdom, Nigeria, Canada, Romania, and Italy (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 45.6% of the time, and the state of residence for domestic perpetrators was reported only 50.7% of the time.

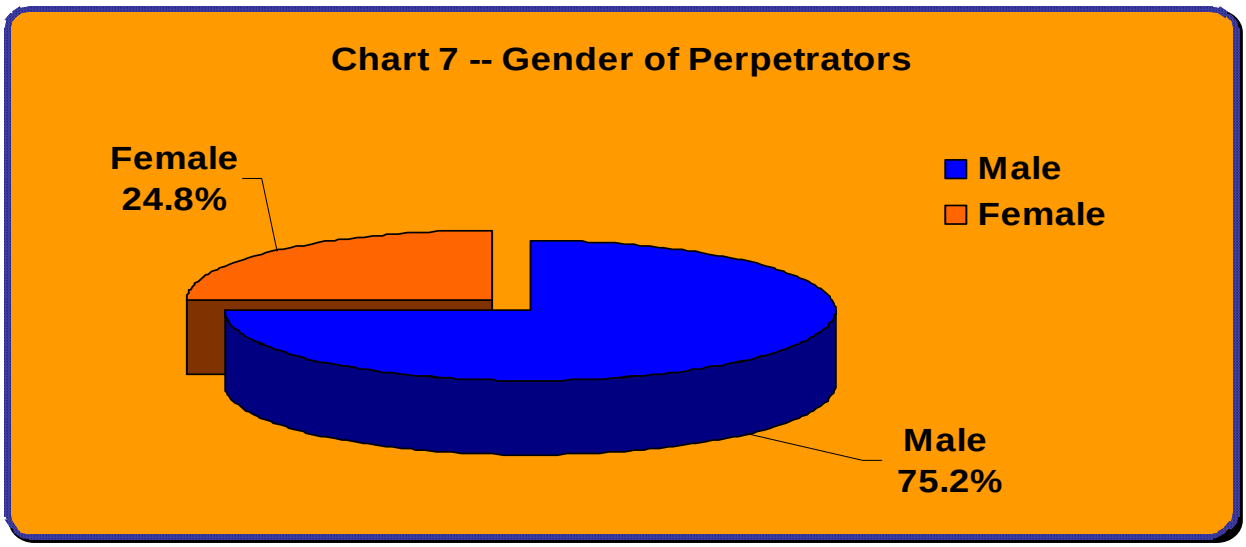
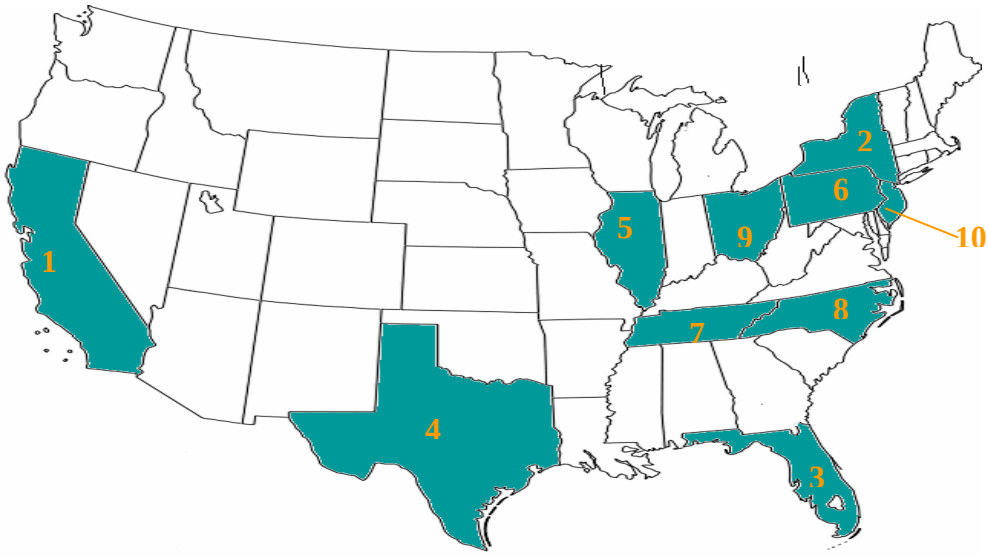


Table 2: Perpetrators per 100,000 people (based on 2006 Census figures)

1	District of Columbia	74.97
2	Nevada	73.05
3	Tennessee	40.49
4	Maine	40.33
5	Florida	39.06
6	New York	37.76
7	Utah	32.86
8	Delaware	32.57
9	Washington	31.96
10	California	31.92

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



Top Ten States - Perpetrator

1. California – 15.2%
2. New York – 9.5%
3. Florida – 9.3%
4. Texas – 6.5%
5. Illinois – 4.5%
6. Pennsylvania – 3.3%
7. Tennessee – 3.2%
8. North Carolina – 3.1%
9. Ohio – 3.1%
10. New Jersey – 3.0%

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

Top Ten Countries - Perpetrator

1. **United States – 60.9%**
2. **United Kingdom – 15.9%**
3. **Nigeria – 5.9%**
4. **Canada – 5.6%**
5. **Romania – 1.6%**
6. **Italy – 1.2%**
7. **Netherlands – 1.2%**
8. **Russia– 1.1%**
9. **Germany – 0.7%**
10. **South Africa – 0.6%**

Complainant Characteristics

The following graphs offer a detailed description of the individuals who filed an Internet fraud complaint through IC3. The average complainant was male, between 30 and 40 years of age, and a resident of one of the four most populated states: California, Texas, Florida, and New York. The Alaska, Utah, and Colorado, while having a relatively small number of complaints (ranked 31st, 24th and 15th 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, United Kingdom, and Australia (see Map 4).

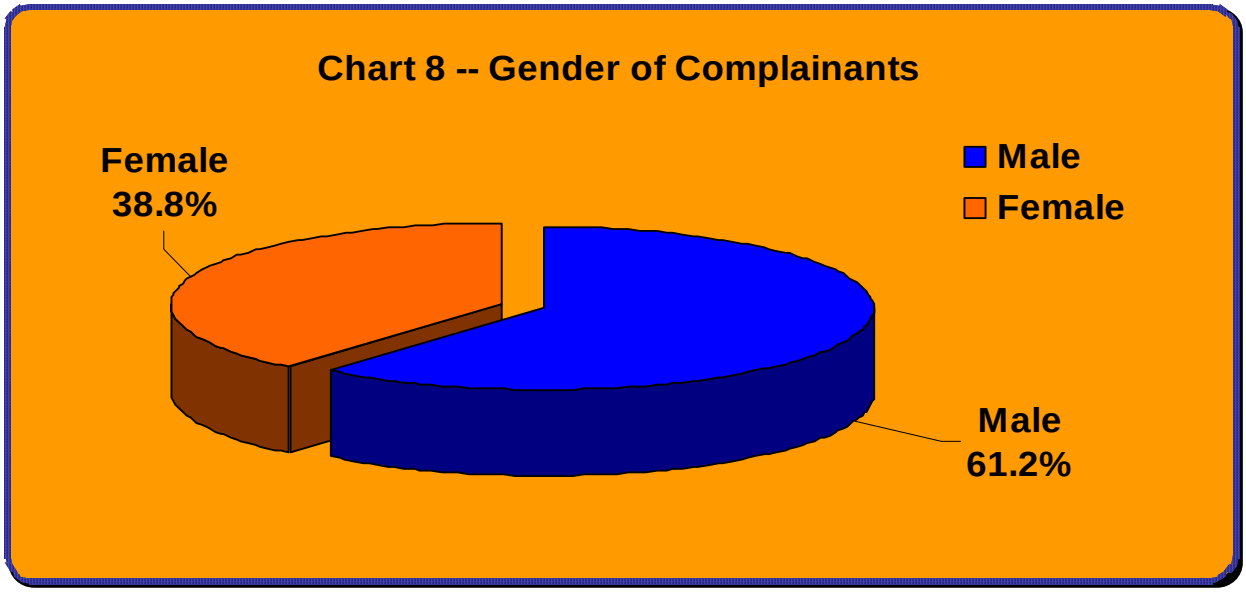


Table 3: Complainants per 100,000 people (based on 2006 Census figures)

1	Alaska	276.55
2	Utah	98.55
3	Colorado	84.36
4	Nevada	82.11
5	District of Columbia	78.59
6	Oregon	74.96
7	Washington	74.92
8	Arizona	72.60
9	New Jersey	72.59
10	Idaho	70.92

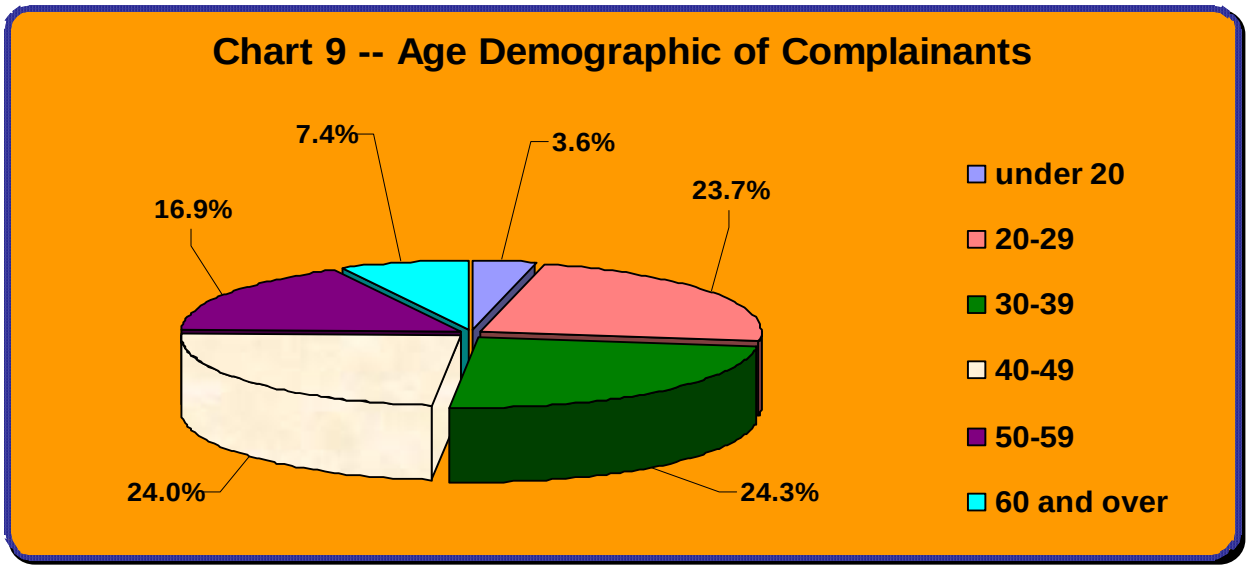
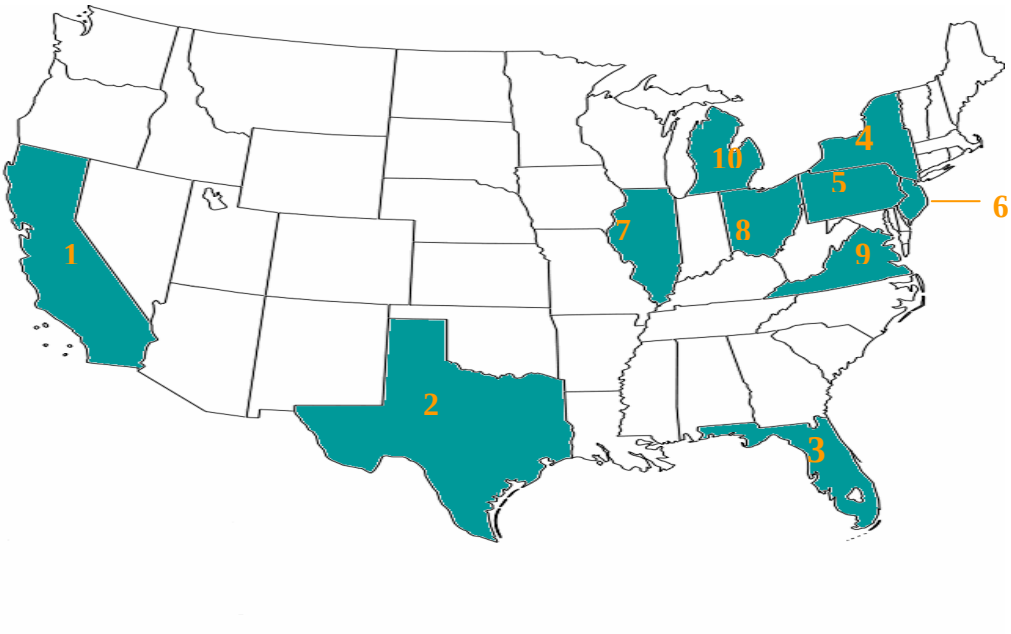


Table 4 compares differences between the dollar loss per incident and the various complainant demographics. Males reported greater dollar losses than females (ratio of $1.69 dollars to every $1.00 dollar). Individuals over 60 years of age reported higher losses than other age groups.

Table 4: Amount Lost per Referred Complaint by Selected Complainant Demographics

Complainant Demographics	Average (median) $ Loss per Typical Complaint
Male	$920.00
Female	$544.73
Under 20	$500.00
20-29	$702.00
30-39	$786.00
40-49	$827.00
50-59	$860.00
60 and older	$866.00

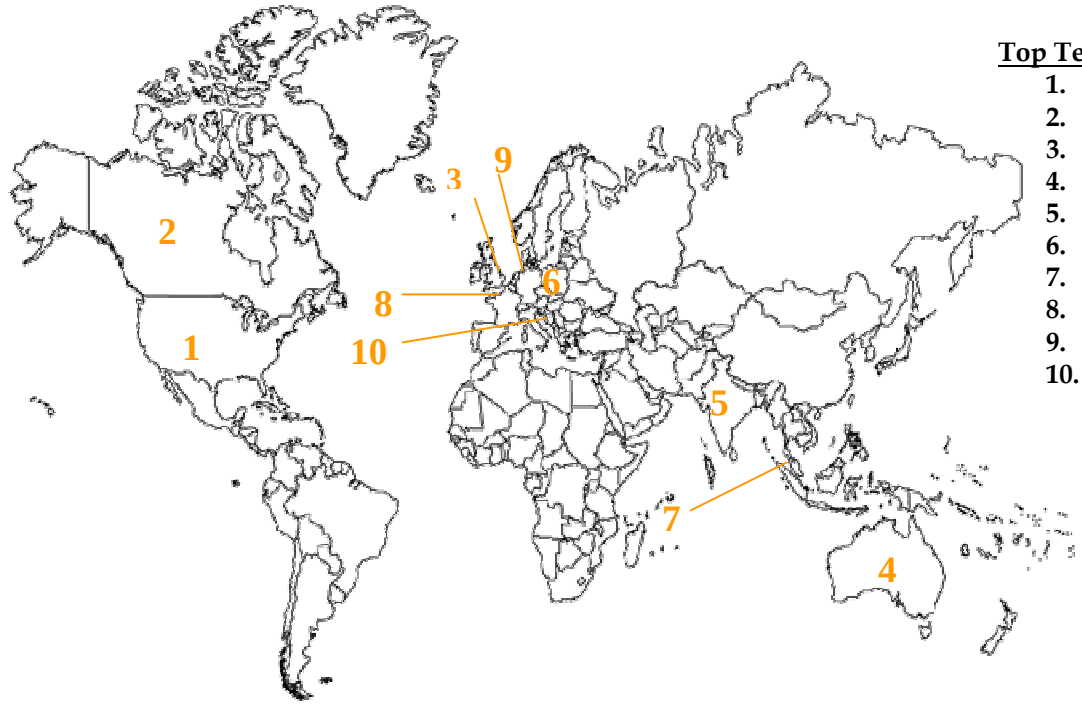
Map 3 - Top Ten States by Count: Individual Complainants (Number Rank)



Top Ten States - Complainant

1. California – 13.5%
2. Texas – 7.2%
3. Florida – 7.1%
4. New York – 5.5%
5. Pennsylvania – 4.0%
6. New Jersey – 3.6%
7. Illinois – 3.5%
8. Ohio – 3.3%
9. Virginia – 3.0%
10. Michigan – 2.9%

Map 4 - Top Ten Countries by Count: Individual Complainants



Top Ten Countries - Complainant

1. United States – 90.70%
2. Canada – 2.40%
3. United Kingdom – 1.10%
4. Australia – .70%
5. India – .30%
6. Germany – .18%
7. Singapore – .18%
8. France – .17%
9. Netherlands – .15%
10. Italy – .13%

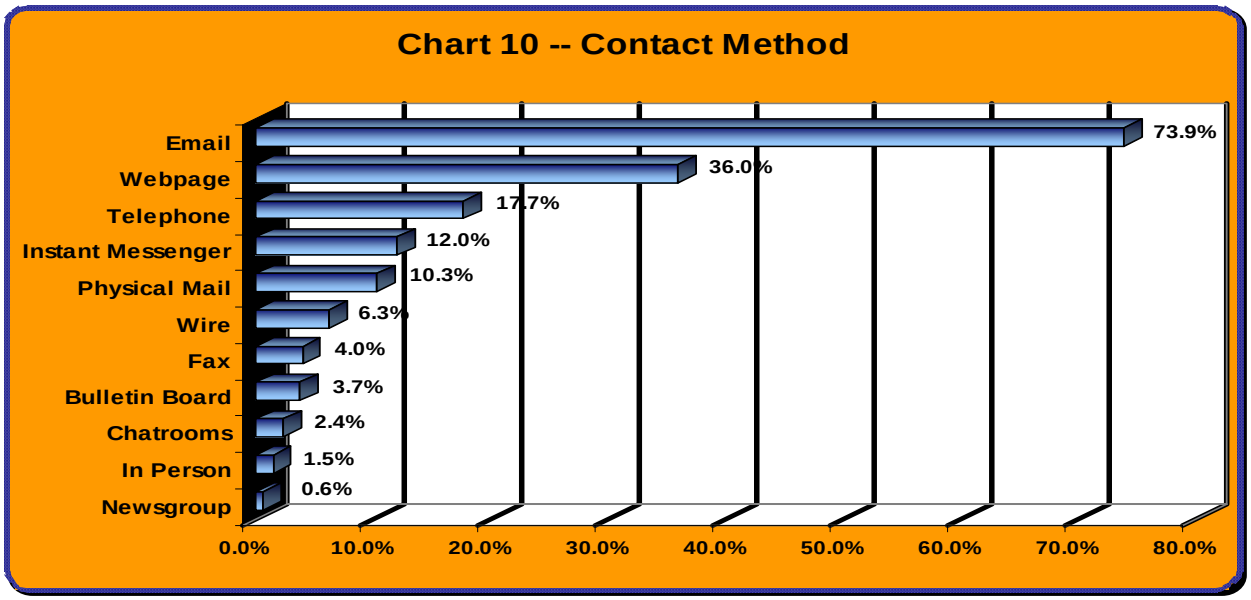
Complainant-Perpetrator Dynamics

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 in the world. This is a unique characteristic not found with other types of "traditional" crime. This jurisdictional issue often requires 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 29.77% 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	29.8%	1. New York (8.5%)	1. Florida (7.5%)	1. Texas (5.2%)
2. Florida	19.9%	2. California (12.2%)	2. New York (9.0%)	2. Texas (5.9%)
3. New York	18.5%	3. California (12.7%)	3. Florida (9.4%)	3. Texas (5.6%)
4. Texas	15.7%	4. California (12.6%)	4. New York (8.8%)	4. Florida (8.0%)
5 Nevada	14.7%	5. California (13.6%)	5. New York (9.2%)	5. Florida (8.5%)
6. Arizona	14.4%	6. California (14.5%)	6. Florida (8.7%)	6. New York (7.7%)
7. Washington	14.4%	7. California (13.5%)	7. New York (8.7%)	7. Florida (6.9%)
8. Oregon	14.0%	8. California (14.5%)	8. Florida (7.2%)	8. New York (7.2%)
9. Vermont	13.4%	9. California (12.7%)	9. New York (10.5%)	9. Michigan (6.0%)
10. North Carolina	13.0%	10. California (12.3%)	10. Florida (8.8%)	10. New York (8.3%)

Another factor that impedes the investigation and prosecution of Internet crime is the anonymity afforded by the Internet. Although complainants in these cases may report multiple contact methods, few reported interacting face-to-face with the vast majority of perpetrators but rather being in contact with them through e-mail (73.9%) or a webpage (36.0%). Others reportedly had phone contact (17.7%) with the perpetrator or corresponded through physical mail (10.3%). Interaction through chat rooms (2.4%) and in-person (1.5%) meetings were rarely reported. The anonymous nature of an e-mail address or a website allows perpetrators to solicit a large number of victims with a keystroke.



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 information related to a threat on the President of the United States, the complaint information is immediately forwarded to the United States Secret Service. Spam complaints and cases of identity theft are forwarded to the Federal Trade Commission and referred to other government agencies with jurisdiction.

Results of IC3 Referrals

IC3 routinely receives updates on the disposition of referrals from agencies receiving complaints. These include 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 cases include the following:

- The Monmouth County Prosecuting Attorney's Office has informed the Internet Crime Complaint Center (IC3) that Richard J. Gorman has been sentenced to five years in state prison and ordered to pay restitution in the amount of $2479.40. Complaints filed with IC3 alleged that Gorman listed multiple vehicles on EBay which he accepted money for and did not deliver. Victim-witness coordinator, Pamela A. Schott, expressed appreciation for the IC3's efforts on behalf of the Prosecuting Attorney's Office. Schott added that without the assistance and cooperation of IC3 and others, they would not have been able to secure a conviction in the case.

- More than twenty suspects have been indicted as the result of an ongoing, multi-agency investigation into a Romanian crime ring. Representatives from the Chicago Field Office of the Federal Bureau Investigation (FBI), the Chicago Office of Immigration and Customs Enforcement (ICE), and the Chicago Police

Department announced the charges together on December 12th, 2006. Altogether, the defendants and others allegedly illegally obtained more then $5 million dollars from victims in a variety of schemes.
The majority of victims believed they were purchasing an item from the EBay auction site. After unsuccessfully bidding on items, they were told they were receiving a second chance offer from the seller. Victims then wired money one of the defendants who posed as the seller or the seller's agent. Investigators believe the fraudulent solicitations originated from, and a substantial portion of the proceeds were transmitted to, unidentified co-schemers located outside the United States, most believed to be in Romania. Most of the money was collected at Western Union locations in Chicago, where many of the alleged perpetrators lived.
Other victims were sent an email from the crime ring informing them that their EBay accounts would be terminated if they didn't reply back with their password and other account information. They would then use this information to take over the victim's account and use it to rip off other EBay users. EBay sellers were victimized as well. The thieves would bid on an item but would not pay through PayPal. Instead, they would persuade the seller to put the money into a fake escrow account. The seller would ship the product and the escrow account would vanish.
Eight defendants were arrested in the Chicago area the day of the announcement, five were already in custody, one is expected to surrender later, and six are fugitives at this time. Each of the defendants is charged with one count of wire fraud. If convicted, they each face a maximum penalty of twenty years in prison and a $250,000 fine. The Court would also order restitution and determine the appropriate sentence to be imposed.

- In March of 2006 IC3 received notification that another perpetrator is behind bars. Thanks to the diligence of a lieutenant in Oconee County GA and the cooperation of the Chicago Police Department, Steven Pruette is facing at least five felony charges. Pruette allegedly sent the scam victim, an Oconee County resident, a fraudulent second chance offer posing as the original seller of an item on EBay. After wiring the money, the victim learned that EBay was in no way involved in the transaction and he promptly filed a complaint with the IC3. The complaint was forwarded to his local sheriff's department. After reviewing the complaint, Lt. David Kilpatrick advised Western Union of the fraud. Pruette, who had been using a Miami, FL address, was nabbed when he entered a Western Union location in Chicago, IL and attempted to pick up the funds. Pruette is a Romanian national and is currently being held by the Immigration and Naturalization Service. He is believed to be part of a multi-state cell which sends funds to Romania and other countries to support terrorist efforts.

- Analysts IC3 were pleased to learn that a lengthy and complex case had finally been closed when Martin Haber, the subject of numerous complaints over a two-year span, pled guilty to federal charges of mail and wire fraud. Haber was the owner and operator of a business named South Dixie Rare Coins in Miami, FL. Haber used the EBay auction site to offer collectibles and rare coins which he never delivered. The initial investigation began after several IC3 complaints against Haber were referred to local and state agencies in Florida. Despite two arrests by local law enforcement for his fraudulent activity, Haber continued to sell on EBay.

  While the IC3 continued to receive complaints about Haber, victims were filing with other consumer reporting agencies and local police departments as well. In January of 2005 FBI joined in the investigation. In all, 188 complaints were received totaling more than $400,000. The FBI investigation revealed that Haber used EBay accounts belonging to friends, family members and business associates to continue his scheme. By assuming the identities of legitimate EBay sellers, Haber was able to hide his true history from potential buyers. While many of the accounts Haber used were suspended by EBay because of buyer complaints, he continued to sell on the site until federal search warrants were executed on his home and business.

  Haber will be sentenced for his crimes in August of 2006. At that time he will face a statutory minimum of twenty years for each of the six counts of wire fraud and one count of mail fraud, fines of up to $250,000, and can be ordered to make full restitution to the victims.

- John Bombard has been charged with hacking into two computer systems, establishing a "bot" network of compromised computers, and launching a distributed denial of service (DDOS) attack against Akamai Technologies. According to the United States Attorney's Office, John Bombard has been charged in federal court with two counts of intentionally accessing a protected computer without authorization. The information alleges that in June of 2004 Bombard launched the DDOS attack causing a significant increase in web traffic to a number of the Cambridge-based company's domain name system (DNS) servers. This attack caused a widespread loss of service to users by consuming the bandwith of the network and overloading its computational resources. Affected Akamai customers had access to their websites slowed or rendered inaccessible for a period of time. Many of these customers filed complaints with the IC3. The information also alleges that the attack against Akamai originated from a "bot" network. A "bot" is a computer program that seeks out and places itself on vulnerable computers and runs silently in the background until it receives instructions from a controlling computer. The information alleges that Bombard compromised the systems using a variant of the GAOBOT worm, a software program capable of reproducing itself and spreading from one computer to the next over a network. If convicted, Bombard faces up the two years imprisonment to be followed by one year of supervised release and a $200,000 fine on each of the charges.

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 207,492 complaints, in 2006, down from 231,493 complaints in 2005 and 207,449 in 2004. This total includes many different fraud types and non-fraudulent complaints. Yet, research indicates that only one in seven incidents of fraud ever make their way to the attention of enforcement or regulatory agencies[1]. The total dollar loss from all referred cases of fraud was $198.44 million up from $183.12 million in 2005.

Internet auction fraud was again the most reported offense followed by non-delivered merchandise/payment, and Check fraud. Among those individuals who reported a dollar loss from the fraud, the highest median dollar losses were found among Nigerian Letter fraud victims ($5,100), check fraud victims ($3,744), and investment fraud victims ($2,695). 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 2005 and the 2006 reports, e-mail and webpages were the two primary mechanisms by which the fraudulent contact took place.

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 have been implemented, with those changes taking effect as of January, 2006. Along with these changes the IC3 and its partners have launched a public website, www.lookstoogoodtobetrue.com , which will educate consumers to various consumer alerts, tips and fraud trends.

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

[1] National White Collar Crime Center, *The National Public Survey on White Collar Crime*, August 2005.

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.

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 2005 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. [2] 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 complainant's 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.[3] 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.[4]

- 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.[5]

- Government Fraud - A knowing misrepresentation of the truth, or concealment of a material fact to induce the government to act to its own detriment.[6] 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.[7] 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.[8] 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.[9] 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.

---

[2] Black's Law Dictionary, Seventh Ed., 1999.
[3] Ibid.
[4] Ibid.
[5] Fraud Examiners Manual, Third Ed., Volume 1, 1998.
[6] Black's Law Dictionary, Seventh Ed., 1999. The Merriam Webster Dictionary, Home and Office Ed., 1995.
[7] Barron's Dictionary of Finance and Investment Terms, Fifth Ed., 1998.
[8] Black's Law Dictionary, Seventh Ed., 1999.
[9] 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 90 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, UPS, Fed-Ex, etc.
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 websites regarding this person/company.
- Do not judge a person/company by their fancy website; 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 website 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 websites 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. Send an e-mail requesting additional information before you process the order asking for: a non-free e-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 website 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 websites 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	13.5	27	Louisiana	1.1
2	Texas	7.2	28	Connecticut	1.1
3	Florida	7.1	29	Alabama	1.1
4	New York	5.5	30	Kentucky	1.1
5	Pennsylvania	4.0	31	Alaska	1.1
6	New Jersey	3.6	32	Oklahoma	1.0
7	Illinois	3.5	33	Kansas	.9
8	Ohio	3.3	34	Iowa	.7
9	Virginia	3.0	35	New Mexico	.7
10	Michigan	2.9	36	Arkansas	.7
11	Georgia	2.9	37	Idaho	.6
12	North Carolina	2.8	38	Mississippi	.6
13	Washington	2.7	39	West Virginia	.6
14	Arizona	2.5	40	New Hampshire	.5
15	Colorado	2.3	41	Nebraska	.5
16	Maryland	2.2	42	Hawaii	.5
17	Indiana	2.0	43	Maine	.4
18	Massachusetts	1.9	44	Rhode Island	.3
19	Missouri	1.8	45	Montana	.3
20	Tennessee	1.8	46	District of Columbia	.3
21	Wisconsin	1.6	47	Delaware	.3
22	Oregon	1.6	48	Vermont	.2
23	Minnesota	1.4	49	Wyoming	.2
24	Utah	1.4	50	South Dakota	.2
25	South Carolina	1.2	51	North Dakota	.1
26	Nevada	1.2			

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

1	California	15.2	27	Oregon	1.0
2	New York	9.5	28	South Carolina	.9
3	Florida	9.3	29	Kentucky	.8
4	Texas	6.5	30	Oklahoma	.8
5	Illinois	4.5	31	Maine	.7
6	Pennsylvania	3.3	32	Louisiana	.6
7	Tennessee	3.2	33	District of Columbia	.6
8	North Carolina	3.1	34	Kansas	.5
9	Ohio	3.1	35	Iowa	.5
10	New Jersey	3.0	36	Nebraska	.5
11	Georgia	2.9	37	Arkansas	.4
12	Michigan	2.8	38	Idaho	.4
13	Washington	2.7	39	Delaware	.4
14	Nevada	2.4	40	West Virginia	.4
15	Arizona	2.3	41	New Mexico	.3
16	Virginia	1.7	42	Mississippi	.3
17	Colorado	1.7	43	New Hampshire	.3
18	Maryland	1.5	44	Montana	.3
19	Massachusetts	1.5	45	Rhode Island	.3
20	Indiana	1.5	46	Hawaii	.2
21	Missouri	1.3	47	Alaska	.2
22	Alabama	1.2	48	Wyoming	.2
23	Wisconsin	1.1	49	Vermont	.2
24	Connecticut	1.1	50	South Dakota	.1
25	Utah	1.1	51	North Dakota	.1
26	Minnesota	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 the District of Columbia. The table above does not represent statistics from other U.S. territories or Canada.)

Complainants per 100,000 people (based on 2006 Census figures)

1	Alaska	276.55	27	North Carolina	54.94
2	Utah	98.55	28	Georgia	54.91
3	Colorado	84.36	29	Rhode Island	54.42
4	Nevada	82.11	30	Texas	54.02
5	District of Columbia	78.59	31	West Virginia	54.00
6	Oregon	74.96	32	Massachusetts	53.28
7	Washington	74.92	33	Tennessee	53.01
8	Arizona	72.60	34	Wisconsin	52.14
9	New Jersey	72.59	35	Delaware	51.67
10	Idaho	70.92	36	Michigan	50.95
11	Maryland	69.57	37	Ohio	50.66
12	Florida	69.20	38	South Carolina	50.01
13	Virginia	68.91	39	New York	49.88
14	New Hampshire	65.63	40	Minnesota	49.35
15	California	65.21	41	Oklahoma	48.95
16	Wyoming	64.66	42	Illinois	48.30
17	New Mexico	64.62	43	Nebraska	47.56
18	Hawaii	63.71	44	Louisiana	47.13
19	Vermont	58.02	45	Kentucky	44.60
20	Connecticut	57.26	46	Alabama	43.05
21	Montana	56.74	47	Iowa	42.76
22	Maine	56.67	48	Arkansas	42.58
23	Pennsylvania	56.62	49	North Dakota	41.52
24	Indiana	56.50	50	Mississippi	34.80
25	Kansas	55.93	51	South Dakota	33.89
26	Missouri	55.61			

Perpetrators per 100,000 people (based on 2006 Census figures)

1	District of Columbia	74.57	27	Pennsylvania	20.46
2	Nevada	73.05	28	Idaho	20.39
3	Tennessee	40.49	29	Oregon	20.32
4	Maine	40.33	30	Rhode Island	19.39
5	Florida	39.06	31	Alabama	19.13
6	New York	37.76	32	New Hampshire	18.94
7	Utah	32.86	33	Indiana	18.29
8	Delaware	32.57	34	Massachusetts	18.19
9	Washington	31.96	35	Missouri	17.58
10	California	31.92	36	Virginia	17.38
11	Wyoming	29.51	37	Oklahoma	16.79
12	Arizona	28.51	38	South Carolina	16.68
13	Colorado	27.62	39	Minnesota	16.08
14	North Carolina	26.71	40	Kansas	15.38
15	Illinois	26.66	41	Wisconsin	15.28
16	New Jersey	26.51	42	Kentucky	15.14
17	Connecticut	24.00	43	West Virginia	14.90
18	Georgia	23.99	44	Hawaii	13.54
19	Alaska	23.58	45	New Mexico	13.20
20	Montana	22.44	46	Iowa	12.88
21	Vermont	21.80	47	South Dakota	12.66
22	Nebraska	21.55	48	Arkansas	11.95
23	Michigan	21.22	49	Louisiana	11.24
24	Texas	21.20	50	North Dakota	10.38
25	Maryland	21.07	51	Mississippi	8.66
26	Ohio	20.60			