IFCC 2001 Internet Fraud Report

January 1, 2001—December 31, 2001

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

Contents

The Internet Fraud Complaint Center
2001 Internet Fraud Report:
January 1, 2001-December 31, 2001

Executive Summary

The Internet Fraud Complaint Center (IFCC) 2001 Internet Fraud Report is the first annual compilation of information on complaints received and referred by the IFCC to law enforcement or regulatory agencies for appropriate action. From January 1, 2001 – December 31, 2001 the IFCC web site received 49,711 complaints. This total includes many different fraud types and non-fraudulent complaints, such as computer intrusions, SPAM/unsolicited email, and child pornography. During this same time period, the IFCC has referred 16,775 complaints of fraud, the majority of which was committed over the Internet or similar online service. The total dollar loss from all referred cases of fraud was $17.8 million, with a median dollar loss of $435 per complaint. Some of the significant findings of this report include:

- Internet auction fraud was by far the most reported offense, comprising 42.8% of referred complaints. Non-deliverable merchandise and payment account for 20.3% of complaints, and Nigerian Letter fraud made up 15.5% of complaints. Credit/debit Card fraud and Confidence fraud (such as home improvement scams and multi-level marketing) round out the top five 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 Nigerian Letter Scam ($5,575), Identity Theft ($3,000), and Investment fraud ($1,000) complainants.

- Nearly 76% of alleged fraud perpetrators tend to be individuals (as opposed to businesses), 81% are male, and half reside in one of the following states: California, Florida, New York, Texas, and Illinois. While most are from the United States, perpetrators have a representation in Canada, Nigeria, Romania and the United Kingdom.

- Over 70% of fraud complainants are male, half are between the ages of 30 and 50 (the average age is 38.6), and over one-third resides in one of the four most populated states: California, Texas, Florida, and New York. While most are from the United States, the IFCC has received a number of complaints from Canada, United Kingdom, Australia, and Japan.

- The amount loss by complainants tends to be related to a number of factors. Business victims tend to lose more than individuals and males tend to lose more than females. This may be a function of both online purchasing differences by gender, and the type of fraud the individual finds themselves involved in. While there isn't a strong relationship between age and loss, proportion of individuals losing at least $5,000 is higher for those 60 years and older than it is for any other age category.

- Electronic mail (E-mail) and web pages are the two primary mechanisms by which the fraudulent contact took place. Nearly 70% of complainants reported they had e-mail contact with the perpetrator.

Overview

The Internet Fraud Complaint Center (IFCC), which began operation on May 8, 2000, is a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI). The IFCC's primary mission is to address fraud committed over the Internet. This is done by facilitating the flow of information between law enforcement agencies and the victims of fraud, information that might otherwise go unreported.

While the primary mission of the IFCC is to address Internet fraud, the IFCC served a critical role for the United States starting on September 11, 2001. On that date, just hours after the terrorist attacks in New York, Pennsylvania and metropolitan Washington, D.C., the IFCC web site served as the mechanism by which people filed online tips with the FBI regarding these attacks. Tens of thousands of tips were received and processed in real-time in the months following the tragedies, and some of the information received proved useful in the subsequent criminal investigation.

The IFCC 2001 Internet Fraud Report is the first annual compilation of information on complaints received and referred by the IFCC to law enforcement or regulatory agencies for appropriate action. The results provide an examination of key characteristics of 1) complaints, 2) perpetrators, 3) complainants, and 4) the interaction between perpetrators and complainants. Overall, the results are intended to enhance our general knowledge about the scope and prevalence of Internet fraud in the United States.

General IFCC Filing Information

From January 1, 2001 – December 31, 2001 the IFCC web site received 17,138,551 "unique" web hits[1]. The number of complaints filed during the year equaled 49,711. During the same time period, 33,940 complaints were referred to enforcement agencies on behalf of the filing individual. This total includes many different fraud types and non-fraudulent complaints, such as computer intrusions, SPAM/unsolicited email, and child pornography[2].

The IFCC averaged 1,428,212 "unique" web hits per month. The number of complaints filed per month averaged 4,142. The IFCC saw a significant increase within the year of complaint filings from the January – March period (total complaints 7,040) to the October – December period (total complaints 15,878). Finally, an average of 2,828 (both fraudulent and non-fraudulent) complaints were referred per month.

The IFCC referred 16,775 complaints of fraud during the 2001 calendar year. Even though the IFCC's primary mission is to address fraud committed over the Internet, those complaints involving only the more traditional methods of contact (e.g., telephone and mail) were also referred on behalf of the individual filing a report. Using information provided by the complainant, it is estimated that just over 90% of all fraud complaints are related to the Internet or online service. Each complaint is

[1] This number is significantly lower than what was report in the *Six-Month Data Trends Report*. The first report included *all* web site hits, meaning that one visitor could have multiple hits from the visitor clicking different links on the web site. This report is identifying "unique" web hits, meaning one visitor is only counted one time per visit, no matter how many times they hit different sections on the web site. This figure also includes web hits related to the IFCC role in collection of terrorist information related to the September 11, 2001 incident.

[2] Although the primary mission of the IFCC is to address Internet fraud, IFCC personnel work also with victims of non-fraudulent offenses (e.g., child pornography, violent crime), and will refer information to law enforcement agencies on their behalf. In fact, of the 33,940 referrals in 2001, 17,165 were non-fraudulent in nature.

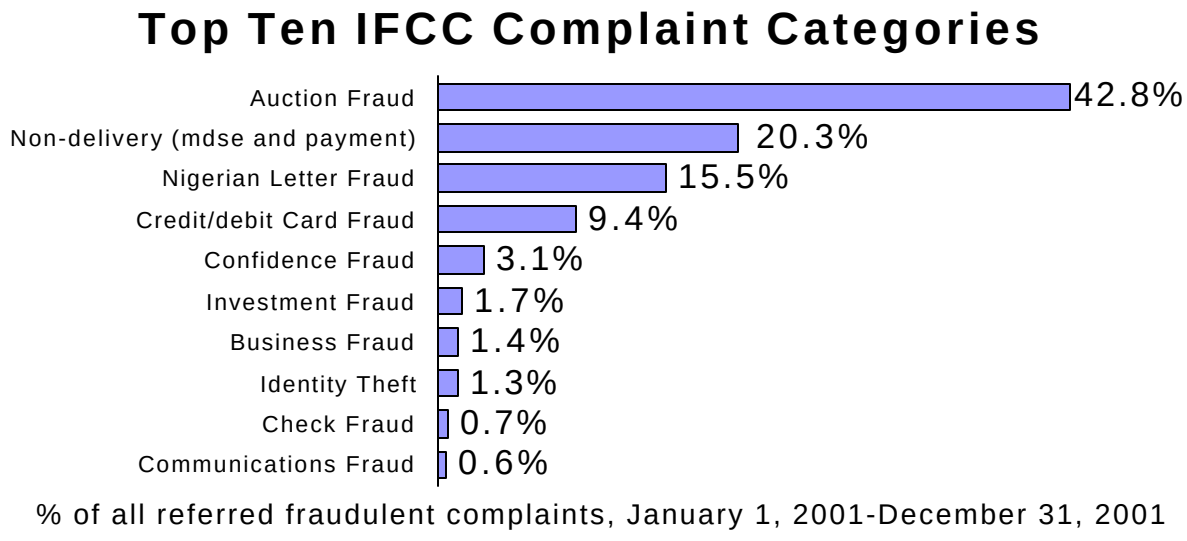
usually referred to multiple agencies, based on where the subject(s) and victims(s) reside(s). During the 2001 year, each referral was sent to an average of three law enforcement and regulatory agencies; overall, 2,711 unique law enforcement and regulatory agencies around the United States received complainant filings.

The results from this report were based on information that was provided to the IFCC on the complaint forms submitted via the Internet by complainants. These complaints were subsequently referred to law enforcement and regulatory agencies. This report may not represent all victims of Internet fraud, or fraud in general, because it is derived solely from the people that reported to the IFCC. Care must also be taken in comparing these results with those from the *IFCC Six-Month Data Trends Report*. On January 11, 2001 a new complaint form was implemented and over the past year the IFCC has automated many of its processes; this has resulted in more relevant, accurate, and complete data. The culmination of these efforts is a report that continues to serve as an awareness tool for the general public and those groups responsible for controlling Internet-related fraud.

Complaint Characteristics

During 2001, Internet auction fraud was by far the most reported offense, comprising 42.8% of referred complaints. This represents a marked decrease from the levels of auction fraud reported in the 6-month report. Part of this decrease is due to increasing reporting levels of other fraudulent activity. Non-deliverable merchandise and payment comprise 20.3% of complaints, and credit and debit card fraud make up 9.4% of complaints. Part of the change may also be explained by the implementation of the new complaint form, which allowed analysts to better decide if the complaint concerned Internet auction fraud.

Due to relationships with enforcement agencies developed over the course of the year, the IFCC is now referring Nigerian Letter fraud complaints to the U.S. Secret Service. This offense represents 15.5% of all referred complaints. Complaints involving confidence fraud confidence (such as home improvement scams and multi-level marketing) comprise 3.1% of referrals. Compared to the 6-month data, there are slightly higher reporting levels of investment fraud, business fraud, and identity theft. For a more detailed explanation on complaint categories used by the IFCC, please refer to Appendix 1 at the end of this report.

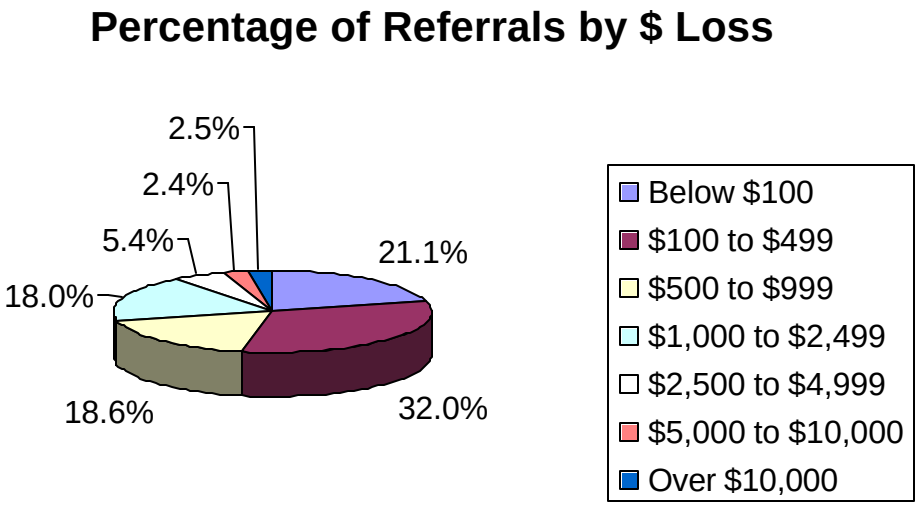


A key area of interest regarding Internet fraud is the average monetary loss incurred by complainants contacting the IFCC. Such information is valuable because it provides a foundation for estimating average Internet fraud losses in the general population. To present information on average losses, two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

Of the 16,775 fraudulent referrals processed by the IFCC during the year, 9,864 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., had just received a fraudulent business investment offer 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 2001 was $17.8 million. With those complaints where a monetary loss was reported, the mean dollar loss was $1804 and the median was $435. Nearly 29% of these referred complaints involved losses of $1000 or more with 71% representing cases of less than $1,000. One-fifth of all cases involving loss had a total value of less than $100, and just over one-half lost under $500. For Internet fraud, the highest dollar loss per incident is found among Nigerian Letter fraud victims (median loss of $5,575); however, only sixteen of the Nigerian Letter fraud complainants actually incurred loss. Identity theft (median loss of $3000) and investment fraud (median loss of $1000) were other high dollar loss categories. The lowest dollar loss was found among communications fraud (median loss of $200) and business fraud (median loss of $160) offenses.

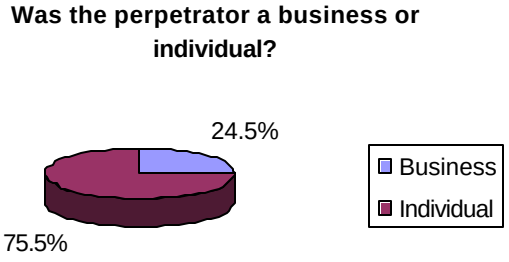
Complaint Type	*% of Complainants Who Reported Dollar Loss*	*Average (median) $ Loss per Typical Complaint*
Auction Fraud	78.2	$395
Non-delivery (mdse and payment)	73.2	$325
Nigerian Letter Fraud	00.6	$5,575
Credit/debit Card Fraud	65.4	$450
Confidence Fraud	53.9	$585
Investment fraud	69.5	$1,000
Business Fraud	42.1	$160
Identity Theft	22.8	$3,000
Check Fraud	67.0	$910
Communications fraud	44.8	$200

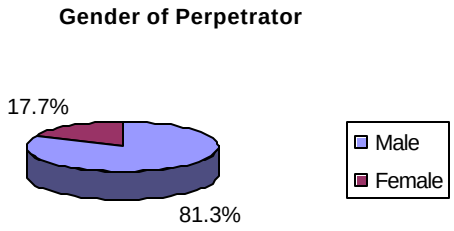


Perpetrator Characteristics

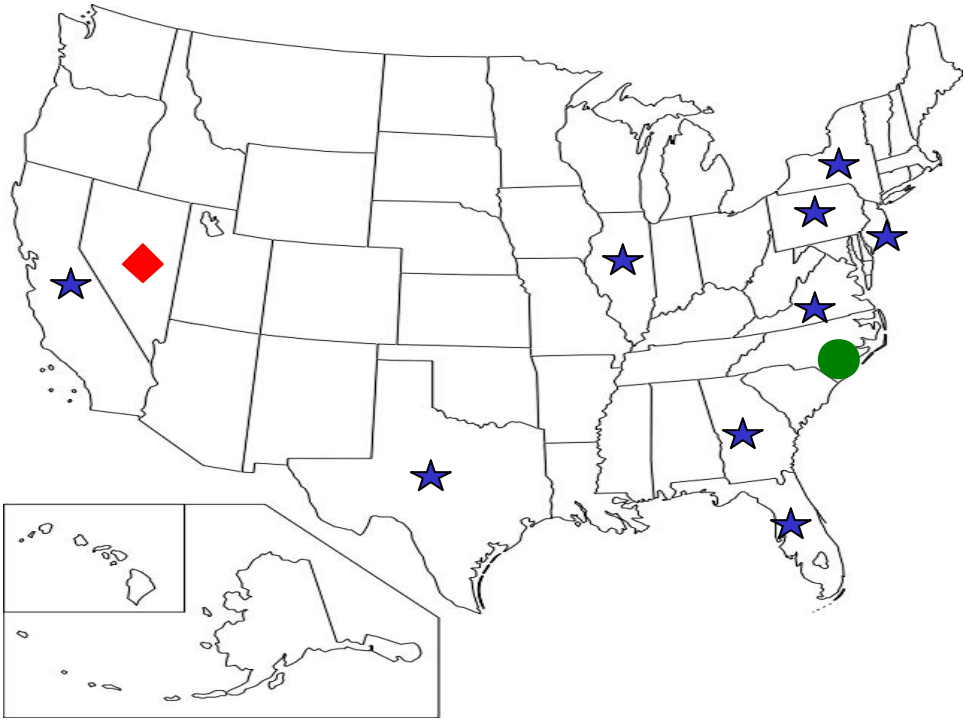
Equally important to presenting the prevalence and monetary impact of Internet fraud is providing insight into the demographics of fraud perpetrators. Nearly 75% of those involved in these types of offenses tend to be individuals (as opposed to businesses), 81% are male, and over half reside in one of the following states: California, Florida, New York, Texas, and Illinois. These locations tend to be among the most populous in the country; controlling for population, Nevada, Florida, New York, California, and the District of Columbia (DC) have the highest per capita rate of perpetrators in the U.S. Perpetrators also come from a varied international background, with significant representation in Canada, Nigeria, Romania and the United Kingdom. Please refer to Appendix III at the end of this report for more information about perpetrator statistics by state.

The statistics also highlight the anonymous nature of the Internet in facilitating fraud. The gender of the perpetrator was reported only 52% of the time, and the state of residence for domestic perpetrators was reported approximately only 77% of the time by complainants.





Top Ten States by Count: Business and Individual Perpetrators



Top Ten State: Individual Perpetrators

Top Ten State: Business Perpetrators

Top Ten State: Business & Individual Perpetrators

Represents % of total perpetrators where state is known

Individual Perpetrators	Business Perpetrators
California: 19.3% Florida: 13.5% New York: 12.4% Illinois: 4.1% Texas: 4.1% New Jersey: 3.3% Georgia: 3.1% Virginia: 3.0% North Carolina: 2.5% Pennsylvania: 2.2%	California: 22.5% Florida: 16.9% New York: 12.7% Texas: 5.7% Illinois: 3.8% Virginia: 3.2% Georgia: 3.0% Pennsylvania: 2.7% New Jersey: 2.5% Nevada: 2.2%

Top Ten States per Capita: All Perpetrators

Perpetrators per 100,000 population (based on 1999 Census figures)

Perpetrators

Nevada: 11.9
Florida: 9.4
New York: 6.8
California: 6.0
District of Columbia: 5.7
Nebraska: 5.2
Virginia: 4.3
Arizona: 3.8
Georgia: 3.8
Utah: 3.8

Top Ten Countries by Count: All Perpetrators

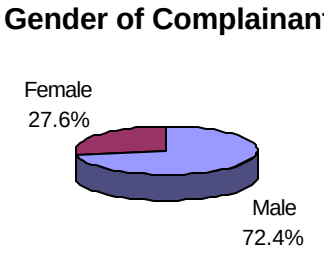
Represents % of total perpetrators where country is known

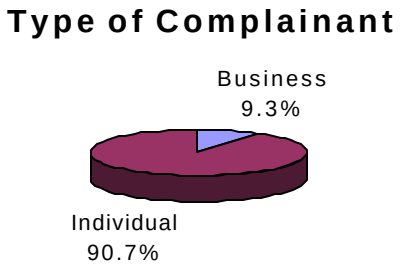
Perpetrators

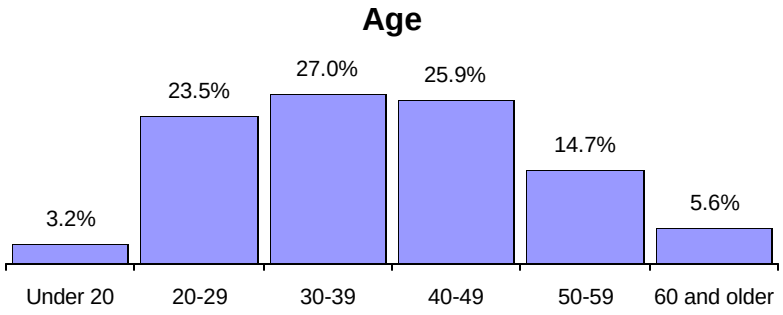
United States: 87.6%
Nigeria: 2.7%
Canada: 2.5%
Romania: 0.9%
United Kingdom: 0.9%
South Africa: 0.5%
Australia: 0.4%
Indonesia: 0.3%
Togo: 0.3%
Russia: 0.2%

Complainant Characteristics

The following graphs offer a detailed description of the individuals who file an Internet fraud complaint through IFCC. Overall, complainants tend to be male, between 30 and 50 (the average age is 38.6), and reside in one of the four most populated states: California, Florida, New York, and Texas. Hawaii and Alaska, while having a relatively small number of complaints (ranked 34th and 44th, respectively), have among the highest per capita rate of complainants in the U.S. While most complainants are from the United States, IFCC has also received a number of filings from Canada, United Kingdom, Australia, and Japan. Though the majority of complainants are individuals, it may be misleading to draw conclusions that only 1 in 10 victims of Internet fraud are businesses. IFCC is not yet fully set up to handle business complaints, and therefore this group is underrepresented in the current analysis. As the IFCC evolves to meet the needs of all victims, it is anticipated that businesses will make up a larger proportion of Internet fraud complainants. Please refer to Appendix III at the end of this report for more information about complainant statistics by state.







Top Ten States by Count: Business and Individual Complainants

Top Ten State: Individual Complainants

Top Ten State: Business Complainants

Top Ten State: Business & Individual Complainants

Represents % of total complainants where state is known

Individual Complainants	Business Complainants
California: 16.7% Florida: 7.7% New York: 6.9% Texas: 5.8% Illinois: 4.2% New Jersey: 3.6% Virginia: 3.4% Pennsylvania: 3.4% Michigan: 3.0% Maryland: 2.9%	California: 18.9% Florida: 7.4% New York: 5.9% Texas: 5.4% Virginia: 4.5% Illinois: 4.2% Pennsylvania: 4.2% New Jersey: 3.4% Washington: 3.0% Michigan: 2.7%

Top Ten States per Capita: All Complainants

Complainants per 100,000 population (based on 1999 Census figures)

Complainants

District of Columbia: 9.4
Hawaii: 8.9
Colorado: 8.2
Alaska: 7.9
Maryland: 7.8
Nevada: 7.7
Virginia: 7.4
California: 7.4
Florida: 7.4
Washington: 6.7

Top Ten Countries by Count: All Complainants

Represents % of total complainants where country is known

Complainants

United States: 93.4%
Canada: 2.2%
United Kingdom: 1.0%
Australia: 0.5%
Japan: 0.2%
Germany: 0.2%
Singapore: 0.2%
Indonesia: 0.1%
New Zealand: 0.1%
South Africa: 0.1%

Table 1 looks at differences between the dollar loss per incident and the various complainant demographics. The amount loss appears to be related to a number of factors. First, businesses lose considerably more per fraud offense than do individuals. Males also tend to lose more than females ($500 to $271). This may be affected by differences in online shopping by gender or by differences in involvement with a particular type of fraud (e.g., men tend to report higher levels of investment fraud). There does not appear to be a strong relationship between age and loss, with those 20-29 having the highest median dollar loss ($478). In addition, the proportion of individuals losing at least $5,000 is higher for those 60 years and older than it is for any other age category (i.e., 6.2% of those in this group incurred losses of $5,000 or more).

Because the majority of referrals consist of a handful of offense types, there is little variance between the victims and fraud type. For example, auction fraud is the most reported offense regardless of age or gender.

Table 1: Amount Lost Per Referred Complaint By Selected Complainant Demographics

Complainant Demographics	*Average (median) $ Loss per Typical Complaint*
Type	
Individual	$410
Business	$789
Gender	
Male	$500
Female	$271
Age	
Under 20	$329
20-29	$478
30-39	$418
40-49	$443
50-59	$455
60 and older	$385

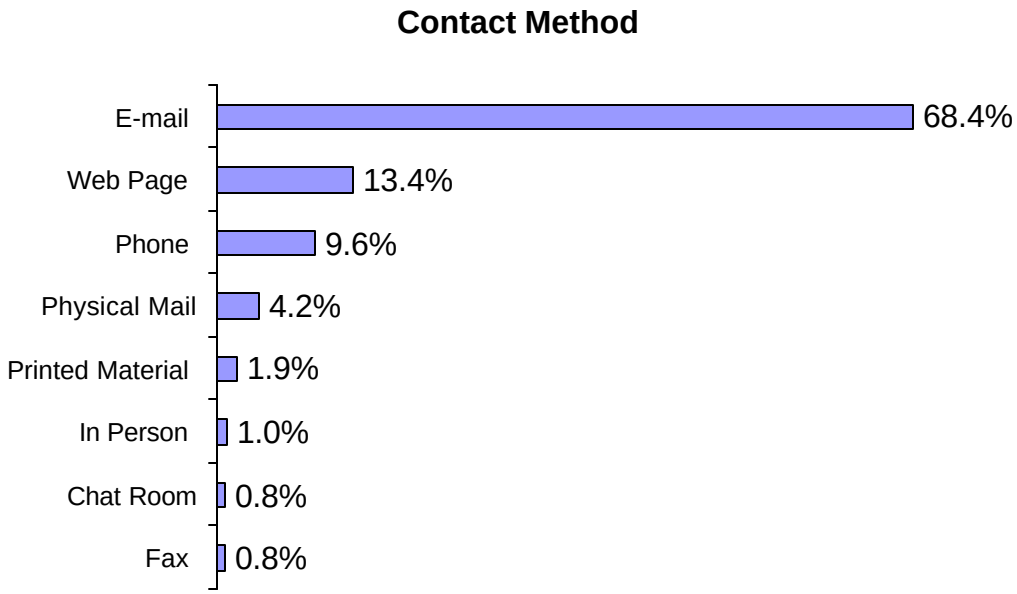
Complainant-Perpetrator Dynamics

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 thousands of miles apart. 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 2 highlights this truly 'borderless' phenomenon. Even in California, where most fraud seems to originate, only 25.1% of referred cases involve 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 seem to not only indicate 'hot spots' of perpetrators (California for example) that can target potential victims from around the world, but it appears that most complaints probably involve complainants and perpetrators that did not have a relationship prior to the incident.

Table 2: % of Perpetrators From Same State (Other top locations in parentheses)

Complainant's State	
California	25.1 (14.8 from Florida, 13.5 from New York, 4.0 from Texas, 2.8 from New Jersey)
Florida	21.1 (18.4 from California, 9.9 from New York, 4.6 from Texas, 4.5 from Illinois)
New York	14.9 (22.4 from California, 14.1 from Florida, 4.4 fro m Texas, 3.7 from Illinois)
Texas	7.8 (18.3 from California. 13.3 from Florida, 12.5 from New York, 4.5 from Illinois)
Illinois	7.6 (20.5 from California, 13.2 from Florida, 10.5 from New York, 5.3 from Texas)
New Jersey	4.8 (19.7 from California, 15.0 from Florida, 10.2 from New York, 6.1 from Illinois)
Virginia	6.7 (15.9 from California, 15.9 from Florida, 14.2 from New York, 3.8 from Pennsylvania)
Pennsylvania	5.5 (17.3 from California, 14.4 from Florida, 12.0 from New York, 4.7 from Virginia)
Michigan	4.0 (17.4 from California, 13.1 from Florida, 11.1 from New York, 6.4 from Illinois)
Maryland	4.0 (17.8 from New York, 17.3 from California, 15.3 from Florida, 5.0 from Illinois)

The following chart provides further information on complainant-perpetrator dynamics. Electronic mail (E-mail) and web pages are the two primary mechanisms by which the alleged fraudulent contact took place. Nearly 70% of complainants reported they had e-mail contact with the perpetrator. Also of interest is the fact that 'traditional' means of communication (e.g., phys ical mail and the phone) are sometimes used along with the Internet, in the form of e-mail and web pages, to facilitate fraud.



Additional Information About IFCC Referrals

Although the IFCC is dedicated to specifically addressing complaints about fraud, specifically Internet fraud, it occasionally receives complaints about other crimes. These have included violent crimes, robberies, burglaries, threats, and many other violations of law. The people submitting these complaints to the IFCC 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 IFCC personnel may make contact with local law enforcement authorities on behalf of the complainant. The IFCC also receives a substantial number of computer-related offenses that are

not fraudulent in nature. It is estimated that 3.9% of all complaints received are computer intrusion/hacking, 5.8% are related to SPAM/unsolicited e-mail, and .8% involve child pornography.

For those complaints that *are* computer-related but not considered Internet fraud, the IFCC routinely refers these to agencies and organizations that handle those particular subjects. For example, if the IFCC receives an allegation of the distribution of child pornography via the Internet, the complaint information would immediately be forwarded to the National Center for Missing and Exploited Children (http://www.ncmec.org/), and to the Baltimore, Md., FBI office, which coordinates all child pornography investigations nationwide through the Innocent Images initiative. Likewise, allegations of computer intrusion would be passed on to the National Infrastructure Protection Center (http://www.nipc.gov/). E-mail "spam" complaints are forwarded to the Federal Trade Commission (http://www.ftc.gov/).

The IFCC has also been aggressively developing partnerships to enhance the ability to serve victims of fraud. The IFCC has reached an arrangement with the U.S. Secret Service (http://www.treas.gov/usss/) for the purpose of referring complaints to them regarding credit card fraud. Cases of identity theft are also forwarded to the Federal Trade Commission. Even though some of the above-mentioned complaints fall outside the IFCC's area of focus, all complaints are handled with importance and every effort is made to direct the complainant's information to the appropriate responding agency.

One complaint that the IFCC continues to receive in high volume, and thus merits special consideration, is the well-known Nigerian Letter Scam. The Nigerian Letter Scam is defined as a correspondence outlining an opportunity to receive non-existent government funds from alleged dignitaries that is designed to collect advance fees from the victims. This sometimes requires payoff money to bribe government officials. While other countries may be mentioned, the correspondence typically indicates "The Government of Nigeria" as the nation of origin. This scam has run since the early 1980's and is also referred to as "419 Fraud" after the relevant section of the Criminal Code of Nigeria, as well as "Advance Fee Fraud." Because of the scam, the country of Nigeria ranks 2nd for total complaints reported at the IFCC on businesses by country. The IFCC will be forwarding all Nigerian Letter Scam complaints to the U.S. Secret Service.

The scam works as follows:

1. A letter, e-mail, or fax is sent from an alleged official representing a foreign government or agency.
2. The letter presents a business proposal to transfer millions of dollars in over- invoiced contract funds into your personal bank account. You are offered a certain percentage of the funds for your help.
3. The letter encourages you to travel overseas to complete the details.
4. The letter also asks you to provide blank company letterhead forms, banking account information, and telephone numbers.
5. Next, you receive various documents with official looking stamps, seals and logos testifying to the authenticity of the proposal.
6. Finally, they ask for up-front or advance fees for various taxes, processing fees, license fees, registration fees, attorney fees, etc.

Results of IFCC Referrals

In 2001, the IFCC-sponsored initiative called "Operation Cyber Loss," a nationwide series of investigations into Internet fraud that resulted in criminal charges being brought against approximately 90 individuals. The fraud schemes exposed by this May, 2001 initiative represent over 56,000 victims who suffered cumulative losses in excess of $117 million.

The Internet Fraud Complaint Center 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, the IFCC 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.

Agencies that voluntarily offered information reported 1867 investigations initiated from complaints in 2001. There were 3 reported arrests derived from complaints. Agencies reported $51,427.63 in documented restitution to the victims. Also, there were 26 victims who had their complaints handled through refunds, receipt of ordered merchandise, or resolved through other agreed upon arrangements. It is important to note that information voluntarily furnished by the referral agencies are in addition to the statistics from "Operation Cyber Loss" mentioned above.

Conclusion

It is well known that a certain level of crime in society, particularly property crime, is never reported to police. In fact, recent research indicates that only one in ten incidents of fraud ever make their way to the attention of enforcement or regulatory agencies[3]. When deciding whether to report a crime, individuals need to remember that their decisions may impact much more than their own particular case. Not only does the information serve the public through the identification of current fraud patterns and trends, it may also provide assistance to agencies working with other victims of the same offender.

While 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 of these types of crimes. Anyone who utilizes the Internet is susceptible, and the IFCC 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 from fraud. Despite a small online population of disreputable users, the Internet is a safe, fast, and effective tool for communication; following some basic prevention strategies (see Appendix II) can make it even safer.

Despite the best proactive efforts, some individuals may find themselves the victims of computer-related criminal activity. Whether falling prey to a bogus investment offer, a dishonest auction seller, or a host of other fraudulent and non-fraudulent offenses, the Internet Fraud Complaint Center is in the position to offer assistance. Through the online complaint and referral process, victims of Internet crime are provided with an easy way to alert authorities, at many different jurisdictional levels, of a suspected criminal or civil violation.

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

Appendix I: Types of Internet Fraud

Analysts at the IFCC determine a fraud type for each Internet fraud complaint received. IFCC analysts sort 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. [4] Credit/debit card fraud is an example of financial institution fraud that ranks among the most commonly reported offenses to the IFCC. 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.[5] 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.[6]

- 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.[7]

- Government Fraud- A knowing misrepresentation of the truth, or concealment of a material fact to induce the government to act to its own detriment.[8] 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.[9] 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.[10] Examples of business fraud include bankruptcy fraud and copyright infringement.

---

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

- 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.[11] Auction fraud and non-delivery of payment or merchandise are both types of confidence fraud and are the most reported offenses to the IFCC. Nigerian Letter Scam is another offense classified under confidence fraud.

Appendix II: Best Practices to Prevent Internet Fraud

Internet Auction Fraud

- Understand as much as possible about how Internet auctions works, what your obligations are as a buyer, and what the seller's obligations are before you bid.
- Find out what actions the web site/company 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 PO Box #.
- Be aware of the difference in laws governing auctions between the US 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 costs.
- 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.

Non-Delivery of Merchandise

- Make sure you are purchasing merchandise from a reputable source. As with auction fraud, check the reputation of the seller whenever possible.
- 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.
- Check with the Better Business Bureau from the seller's home area to see if there have been any problems with the seller before.
- 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.

[11] Ibid.

- The safest way to purchase items via the Internet is by credit card because you can often dispute the charges if something is wrong. Also, consider utilizing an escrow or alternate payment service.
- Make sure the web site is secure when you electronically send your credit card numbers.

Credit Card Fraud

- Don't give out your credit card number(s) online unless the site is both secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but may provide you some assurance.
- Before using the site, check out the security/encryption software it uses make sure your information will be protected.
- Make sure you are purchasing merchandise from a reputable/legitimate source. Once again investigate the person or company before purchasing any products.
- Try to obtain a physical address rather than merely a post office box and a phone number, call the seller to see if the number is correct and working.
- Send them e-mail to see if they have an active e-mail address and be wary of sellers who use free e-mail services where a credit card wasn't required to open the account.
- Do not purchase from sellers who won't provide you with this type of information.
- Check with the Better Business Bureau from the seller's area 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) you should contact the card issuer immediately.

Investment Fraud

- Don't invest in anything based on appearances. Just because an individual or company has a flashy web site doesn't mean it is legitimate. Web sites can be created in just a few days. After a short period of taking money, a site can vanish without a trace.
- Don't invest in anything you are not absolutely sure about. Do your homework on the investment to ensure that it is legitimate.
- Thoroughly investigate the individual or company to ensure that they are legitimate.
- Check out other web sites regarding this person/company.
- Be cautious when responding to special investment offers (especially through unsolicited e-mail) by fast talking telemarketers. Know whom you are dealing with!
- Inquire about all the terms and conditions dealing with the investors and the investment.
- Rule of Thumb: If it sounds too good to be true it probably is!!

Nigerian Letter Scam

- 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

- 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.

Appendix Three: Complainant/Perpetrator Statistics, by State

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

1	California	16.7	**27**	Kentucky	1.0
2	Florida	7.7	**28**	Nevada	1.0
3	New York	6.9	**29**	Utah	1.0
4	Texas	5.8	**30**	Oklahoma	.9
5	Illinois	4.2	**31**	Kansas	.8
6	New Jersey	3.6	**32**	Alabama	.8
7	Virginia	3.4	**33**	Hawaii	.7
8	Pennsylvania	3.4	**34**	Iowa	.7
9	Michigan	3.0	**35**	Arkansas	.6
10	Maryland	2.9	**36**	New Hampshire	.5
11	Ohio	2.8	**37**	Nebraska	.5
12	Washington	2.6	**38**	West Virginia	.5
13	Georgia	2.4	**39**	Idaho	.4
14	North Carolina	2.4	**40**	New Mexico	.4
15	Colorado	2.3	**41**	Maine	.4
16	Massachusetts	2.3	**42**	Mississippi	.4
17	Missouri	2.0	**43**	District of Columbia	.3
18	Arizona	1.9	**44**	Alaska	.3
19	Wisconsin	1.7	**45**	Montana	.3
20	Oregon	1.5	**46**	Rhode Island	.3
21	Indiana	1.4	**47**	Delaware	.2
22	Minnesota	1.4	**48**	Vermont	.2
23	Tennessee	1.2	**49**	South Dakota	.2
24	Louisiana	1.1	**50**	North Dakota	.1
25	South Carolina	1.1	**51**	Wyoming	.1
26	Connecticut	1.1			

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

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

1	California	18.9	**27**	Nevada	1.0
2	Florida	7.4	**28**	Iowa	.9
3	New York	5.9	**29**	Oklahoma	.9
4	Texas	5.4	**30**	Utah	.7
5	Virginia	4.5	**31**	West Virginia	.7
6	Illinois	4.2	**32**	Alabama	.7
7	Pennsylvania	4.2	**33**	Hawaii	.7
8	New Jersey	3.4	**34**	Idaho	.7
9	Washington	3.0	**35**	Kansas	.7
10	Michigan	2.7	**36**	Arkansas	.6
11	Georgia	2.4	**37**	Nebraska	.6
12	Ohio	2.4	**38**	Kentucky	.5
13	Arizona	2.2	**39**	Alaska	.4
14	Colorado	2.2	**40**	District of Columbia	.4
15	Massachusetts	2.2	**41**	New Hampshire	.4
16	Maryland	2.1	**42**	Delaware	.3
17	Tennessee	1.9	**43**	Mississippi	.3
18	North Carolina	1.8	**44**	Rhode Island	.3
19	Louisiana	1.6	**45**	Maine	.2
20	Missouri	1.6	**46**	North Dakota	.2
21	Wisconsin	1.6	**47**	New Mexico	.2
22	Indiana	1.4	**48**	South Dakota	.2
23	Connecticut	1.3	**49**	Vermont	.1
24	Oregon	1.3	**50**	Wyoming	.1
25	South Carolina	1.3	**51**	Montana	-
26	Minnesota	1.0			

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

Individual Perpetrators By State
Represents % of total individual perpetrators where state is known

1	California	19.3	**27**	Oregon	.9
2	Florida	13.5	**28**	Alabama	.9
3	New York	12.4	**29**	Oklahoma	.7
4	Illinois	4.1	**30**	Minnesota	.7
5	Texas	4.1	**31**	Utah	.7
6	New Jersey	3.3	**32**	Kansas	.7
7	Georgia	3.1	**33**	Nebraska	.7
8	Virginia	3.0	**34**	Iowa	.6
9	North Carolina	2.5	**35**	Rhode Island	.4
10	Pennsylvania	2.5	**36**	Hawaii	.4
11	Nevada	2.2	**37**	New Hampshire	.3
12	Arizona	1.9	**38**	Arkansas	.3
13	Maryland	1.9	**39**	District of Columbia	.3
14	Ohio	1.9	**40**	Maine	.3
15	Michigan	1.7	**41**	Mississippi	.3
16	Colorado	1.6	**42**	West Virginia	.2
17	Washington	1.6	**43**	Delaware	.2
18	Missouri	1.3	**44**	Idaho	.2
19	Wisconsin	1.2	**45**	New Mexico	.2
20	Louisiana	1.2	**46**	Alaska	.1
21	South Carolina	1.2	**47**	Montana	.1
22	Kentucky	1.1	**48**	Vermont	.1
23	Indiana	1.0	**49**	South Dakota	.1
24	Tennessee	1.0	**50**	North Dakota	.0
25	Connecticut	1.0	**51**	Wyoming	.1
26	Massachusetts	1.0			

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

Business Perpetrators By State
Represents % of total business perpetrators where state is known

1	California	22.5	**27**	Oregon	.7
2	Florida	16.9	**28**	Kansas	.5
3	New York	12.7	**29**	Minnesota	.4
4	Texas	5.7	**30**	Iowa	.4
5	Illinois	3.8	**31**	Louisiana	.4
6	Virginia	3.2	**32**	Hawaii	.3
7	Georgia	3.0	**33**	New Hampshire	.3
8	Pennsylvania	2.7	**34**	Alabama	.3
9	New Jersey	2.5	**35**	District of Columbia	.3
10	Nevada	2.2	**36**	Indiana	.3
11	North Carolina	1.9	**37**	Arkansas	.2
12	Arizona	1.8	**38**	Mississippi	.2
13	Missouri	1.5	**39**	Oklahoma	.2
14	Nebraska	1.4	**40**	West Virginia	.2
15	Massachusetts	1.4	**41**	Delaware	.2
16	Maryland	1.3	**42**	Montana	.2
17	Ohio	1.3	**43**	Wyoming	.2
18	Washington	1.2	**44**	Maine	.1
19	Colorado	1.2	**45**	Rhode Island	.1
20	Michigan	1.2	**46**	Alaska	.1
21	Utah	1.1	**47**	Idaho	.1
22	South Carolina	.8	**48**	New Mexico	.1
23	Kentucky	.8	**49**	South Dakota	.1
24	Tennessee	.7	**50**	North Dakota	.0
25	Connecticut	.7	**51**	Vermont	.0
26	Wisconsin	..7			

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

Complainants per 100,000 population (based on 1999 Census figures)

1	District of Columbia	9.44	**27**	Maine	4.47
2	Hawaii	8.94	**28**	Georgia	4.47
3	Colorado	8.28	**29**	North Carolina	4.42
4	Alaska	7.91	**30**	Michigan	4.41
5	Maryland	7.89	**31**	Montana	4.30
6	Nevada	7.74	**32**	Pennsylvania	4.25
7	Virginia	7.49	**33**	South Carolina	4.22
8	California	7.45	**34**	Texas	4.21
9	Florida	7.42	**35**	Minnesota	4.19
10	Washington	6.67	**36**	Rhode Island	4.14
11	New Jersey	6.45	**37**	West Virginia	4.10
12	Oregon	6.42	**38**	Oklahoma	3.87
13	New Hampshire	6.41	**39**	Louisiana	3.87
14	Utah	6.39	**40**	Iowa	3.80
15	Arizona	5.92	**41**	Wyoming	3.75
16	New York	5.47	**42**	Ohio	3.62
17	Idaho	5.43	**43**	Kentucky	3.56
18	Massachusetts	5.42	**44**	Indiana	3.47
19	Missouri	5.30	**45**	Tennessee	3.46
20	Vermont	5.05	**46**	North Dakota	3.31
21	Illinois	5.00	**47**	Arkansas	3.29
22	Connecticut	4.94	**48**	New Mexico	3.28
23	Delaware	4.78	**49**	South Dakota	3.14
24	Wisconsin	4.57	**50**	Alabama	2.70
25	Nebraska	4.56	**51**	Mississippi	2.02
26	Kansas	4.52			

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

Perpetrators per 100,000 population (based on 1999 Census figures)

1	Nevada	11.94	**27**	Kansas	2.30
2	Florida	9.49	**28**	Texas	2.25
3	New York	6.80	**29**	Louisiana	2.20
4	California	6.06	**30**	Pennsylvania	2.13
5	District of Columbia	5.78	**31**	Wisconsin	2.04
6	Nebraska	5.28	**32**	Maine	2.00
7	Virginia	4.36	**33**	Iowa	1.85
8	Arizona	3.89	**34**	Alaska	1.78
9	Georgia	3.86	**35**	Massachusetts	1.77
10	Utah	3.85	**36**	Oklahoma	1.73
11	New Jersey	3.76	**37**	Tennessee	1.66
12	Colorado	3.65	**38**	Alabama	1.56
13	Illinois	3.27	**39**	Michigan	1.52
14	Maryland	3.27	**40**	Ohio	1.50
15	Rhode Island	3.03	**41**	Montana	1.36
16	North Carolina	3.02	**42**	Vermont	1.35
17	Hawaii	2.82	**43**	Indiana	1.33
18	South Carolina	2.75	**44**	Minnesota	1.30
19	New Hampshire	2.75	**45**	Idaho	1.28
20	Connecticut	2.71	**46**	West Virginia	1.16
21	Kentucky	2.60	**47**	Arkansas	1.14
22	Washington	2.59	**48**	Mississippi	.98
23	Wyoming	2.50	**49**	New Mexico	.92
24	Oregon	2.44	**50**	South Dakota	.82
25	Missouri	2.40	**51**	North Dakota	.47
26	Delaware	2.39			

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