IFCC 2002 Internet Fraud Report

January 1, 2002—December 31, 2002

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

Contents

The Internet Fraud Complaint Center
2002 Internet Fraud Report:
January 1, 2002-December 31, 2002

Executive Summary

The Internet Fraud Complaint Center (IFCC) 2002 Internet Fraud Report is the second annual compilation of information on complaints received and referred by IFCC to law enforcement or regulatory agencies for appropriate action. From January 1, 2002 to December 31, 2002, the IFCC Web site received 75,063 complaints. This total includes many different fraudulent and non-fraudulent complaints, such as auction fraud, credit/debit card fraud, computer intrusions, unsolicited email (SPAM), and child pornography. During this same time period, IFCC has referred 48,252 complaints of fraud, a three-fold increase from the previous year. The total dollar loss from all referred cases of fraud was $54 million, up from $17 million in 2001, with a median dollar loss of $299 per complaint. Significant findings from the 2002 report include:

- As has been the case since IFCC began operation in 2000, Internet auction fraud was by far the most reported offense, comprising 46% of referred complaints. Non-delivery of merchandise and payment account for 31% of complaints, and credit/debit card fraud made up nearly 12% of complaints. Investment fraud, business fraud, confidence fraud, and identity theft round out the top seven categories of complaints referred to law enforcement during the year (all at 1.0% or more). Among those individuals who reported a dollar loss, the highest median dollar losses were found among Nigerian Letter fraud ($3,864), identity theft ($2,000), and check fraud ($1,100) complainants.

- Among perpetrators, nearly four in five (79%) are male and half reside in one of the following states: California, New York, Florida, Texas, and Illinois. While most are from the United States, perpetrators also have a representation in Nigeria, Canada, South Africa, and Romania.

- Among complainants, 71% are male, half are between the ages of 30 and 50 (the average age is 39.4), and over one-third reside in one of the following four states: California, Florida, Texas, and New York. While most complainants are from the United States, IFCC has received a number of complaints from Canada, Australia, Great Britain, Germany, and Japan.

- The amount lost by complainants tends to be related to a number of factors. 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 himself or herself involved with. While there isn't a strong relationship between age and loss, 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.

- Electronic mail (E-mail) and Web pages are the two primary mechanisms by which the fraudulent contact took place. In all, 66% of complainants reported they had e-mail contact with the perpetrator and 18.7% had contact through a Web page.

- Only one in four complainants had contacted a law enforcement agency about the incident prior to filing a complaint with IFCC. These individuals had a higher median dollar loss ($500) than the total complainant population.

Overview

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

The program 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. In the early part of 2002, IFCC was recognized for their work when the program was honored with the *excellence.gov award* for innovation in Electronic Government.

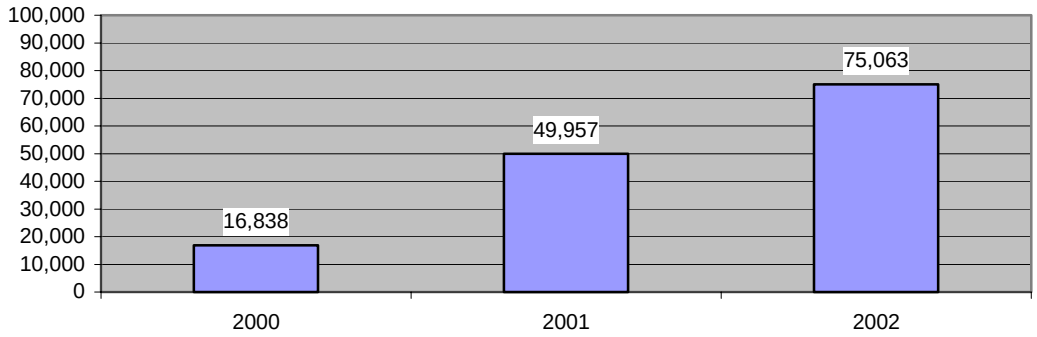
Overall, the IFCC 2002 Internet Fraud Report is the second annual compilation of information on complaints received and referred by IFCC to law enforcement or regulatory agencies for appropriate action. The results provide an examination of key characteristics of 1) complaints, 2) perpetrators, 3) complainants, 4) the interaction between perpetrators and complainants, and 5) success stories involving IFCC. 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, 2002 to December 31, 2002, the IFCC Web site received 11,636,362 "unique" Web hits (down 32% from 2001)[1]. IFCC averaged 969,696 Web hits per month. The number of complaints filed during the year equaled 75,063. This is a 67% increase over 2001, when 49,957 complaints were received. There were 16,838 filings in 2000, although IFCC didn't begin taking complaints until May 8 of that year. The number of complaints filed per month averaged 6,255. There was a steady rise in the number of complaints filed for each quarter of 2002, culminating with 20,325 complaints filed between October and December.

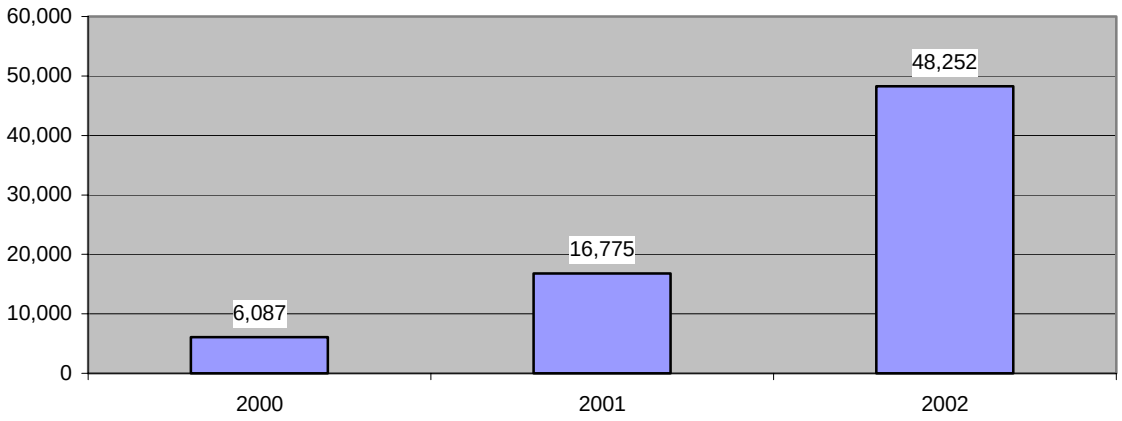
During 2002, 48,252 complaints of fraud were referred to enforcement agencies on behalf of the filing individual[2]. An average of 4,021 complaints were referred per month. This represents a significant increase over IFCC activity in 2001, when 16,775 complaints of fraud were referred. The higher number of filed complaints may represent a combination of increased victimization and a heightened awareness of IFCC as a viable tool to report a complaint.

Chart 1
Yearly Comparison of Complaints Received Via IFCC Web site



[1] The visitor count in 2001 was particularly high, due in large part to the increased volume experienced by the IFCC Web site in response to the terrorist tips initiative.
[2] Although the primary mission of IFCC is to address Internet fraud, IFCC personnel work also with victims of non-fraudulent offenses (e.g., child pornography, computer intrusions), and make that complaint information available to enforcement agencies.

Chart 2
Yearly Comparison of Fraud Complaints Referred By IFCC



Even though 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 usually referred to multiple agencies, based on where the subject(s) and victims reside. During 2002, each referral was sent to an average of three law enforcement and regulatory agencies; overall, 2,875 unique law enforcement and regulatory agencies around the United States received complainant filings for investigation.

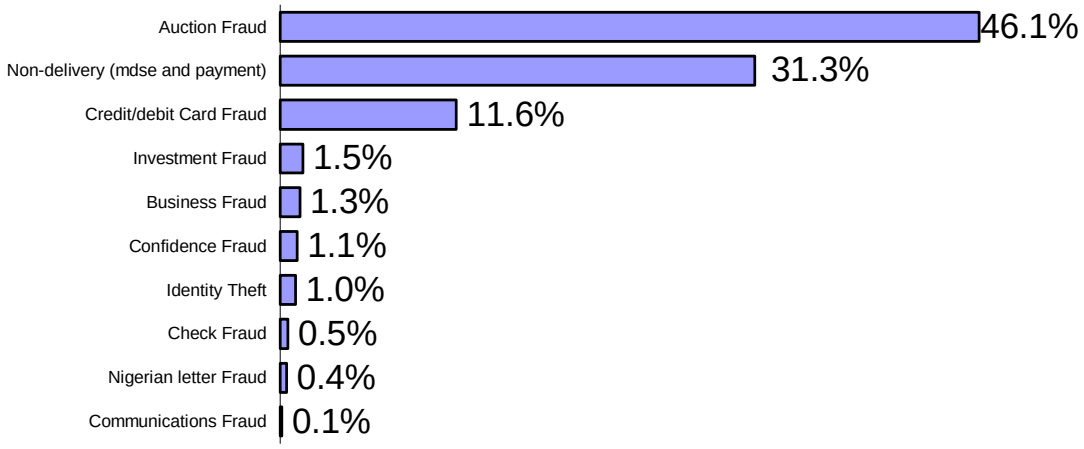
The results from this report are largely based on information related to fraudulent activity that was provided to IFCC on the complaint forms submitted by complainants. These complaints were subsequently referred to law enforcement and regulatory agencies. This report may not represent all victims of Internet fraud, or fraud in general, because it is derived solely from the complaints that were reported to IFCC. Analysts evaluate complaints for validity. However each referral agency makes its own investigative determination. The resulting information contained in this report serves as an awareness tool for both the general public and for groups tasked with controlling Internet fraud.

Complaint Characteristics

During 2002, Internet auction fraud was by far the most reported offense, comprising 46.1% of referred fraud complaints. This represents a 7.7% increase from 2001 (42.8%) levels of reported auction fraud. In addition, during 2002, the non-delivery of merchandise and payment comprise 31.3% of complaints (up 54.2% from 2001), and credit and debit card fraud make up an additional 11.6% of complaints (up 23.4% from 2001). The remainder of the top ten types of activity referred by IFCC (investment fraud, business fraud, confidence fraud, identity theft, check fraud, Nigerian letter fraud and communications fraud) makes up nearly 6% of complaints.

While the actual number of referrals has risen for most categories, the large percentage variations over 2001 results can be explained in part by a change in the way findings are presented. Even though the number of Nigerian letter fraud complaints increased from 2,600 to over 16,000 in 2002, only those cases where either a loss of money or information (e.g., sharing personal identifiers with the perpetrator) occurred are referred to appropriate local, state, or federal agencies. The remainder of the complaints are made available to the U.S. Secret Service for consideration. This is a change from the reporting practices of the 2001 Annual Report. For a more detailed explanation of complaint categories used by IFCC, please refer to Appendix I at the end of this report.

Chart 3
Top Ten IFCC Complaint Categories



% of all referred fraudulent complaints, January 1, 2002 - December 31, 2002

A key area of interest regarding Internet fraud is the average monetary loss incurred by complainants contacting 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 values, 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 48,252 referrals of fraud processed by IFCC during the year, 36,332 involved victims who reported monetary losses. 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 2002 was $54 million. This compares with $17 million in total losses from all referrals in 2001. With those complaints where a monetary loss was reported, the mean dollar loss was $1,482 and the median was $299. Nearly 28% of these referred complaints involved losses of less than $100, while nearly half of all referred complaints (49.2%) had a loss of between $100 and $1,000. One in five complaints (19%) involved a loss between $1,000 and $5,000 dollars and only 3.6% had a loss of greater than $5,000. The highest dollar loss per incident is found among Nigerian letter fraud, (median loss of $3,400), identity theft ($2,000), and check fraud ($1,100) complaints. The lowest dollar loss was found among credit/debit card fraud (median loss of $120) and non-delivery ($176) referrals.

Chart 4
Percentage of Referrals by $ Loss

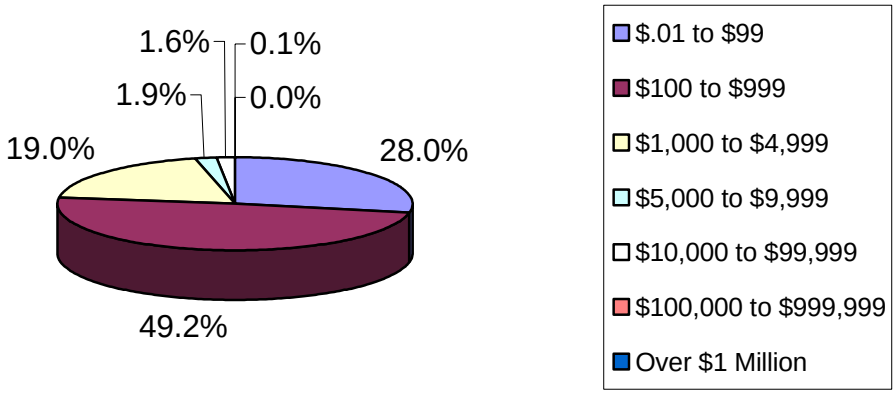


Table 1: Amount Lost by Fraud Type for Individuals Reporting Monetary Loss

Complaint Type	*% of Complainants Who Reported Dollar Loss*	*Average (median) $ Loss per Typical Complaint*
Auction Fraud	87	$320
Non-delivery (mdse and payment)	82	$176
Credit/debit Card Fraud	62	$120
Investment Fraud	75	$570
Business Fraud	75	$220
Confidence Fraud	58	$1,000
Identity Theft	15	$2,000
Check Fraud	56	$1,100
Nigerian letter Fraud*	< 1	$3,864
Communications Fraud	36	$174

* Of 16,164 complaints, 74 individuals lost money totaling $1.6 million

Perpetrator Characteristics

Equally important to presenting the prevalence and monetary impact of Internet fraud is providing insight into the demographics of fraud perpetrators. Of those perpetrators for which information is known, nearly four in five (79%) were male and over half reside in one of the following states: California, Florida, New York, Texas, Illinois, and Pennsylvania (see Map 1). These locations tend to be among the most populous in the country. When controlling for population, Nevada, Arizona, New York, Florida, California, and Washington have the highest per capita rate of perpetrators in the U.S. Please refer to Appendix II at the end of this report for more information about perpetrator statistics by state. Perpetrators also come from a varied international background, with significant representation in Nigeria, Canada, South Africa, Romania, and Spain (see Map 2).

The statistics also highlight the anonymous nature of the Internet in facilitating fraud. The gender of the perpetrator was reported only 65% of the time, and the residence state for perpetrators was reported only 72% of the time.

Chart 5
Gender of Perpetrator

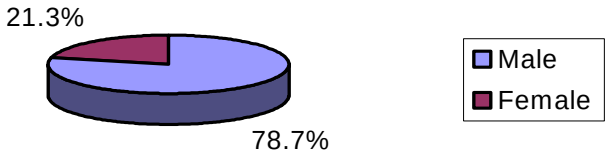
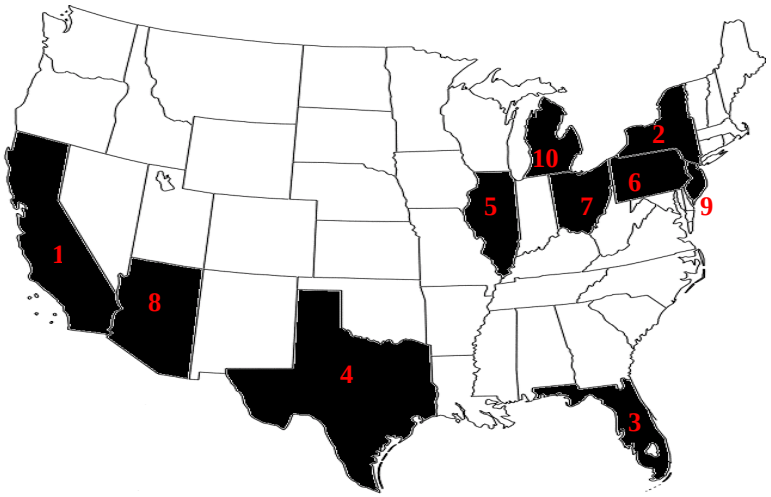


Table 2: Perpetrators per 100,000 population (based on 2002 Census figures)

1. Nevada – 20.75
2. Arizona – 13.93
3. New York – 12.71
4. Florida – 12.61
5. California – 12.08
6. Washington – 11.09
7. Maine – 10.74
8. District of Columbia – 10.51
9. Rhode Island – 10.28
10. Connecticut – 10.23

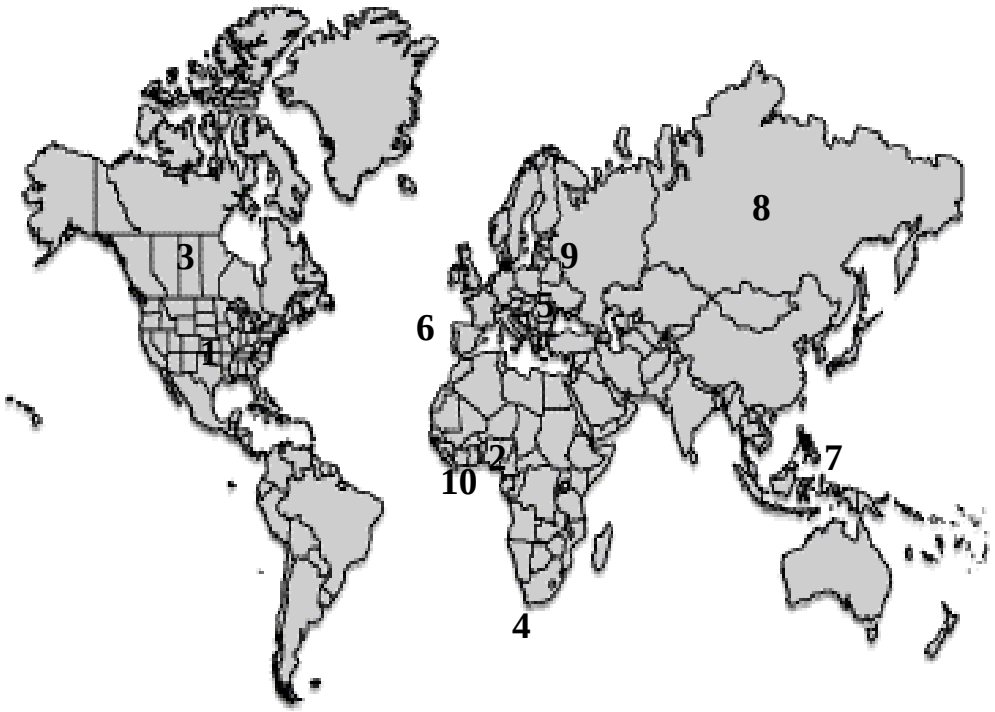
Map 1 - Top Ten States by Count: Individual Perpetrators (Number is Rank)



Top Ten States - Perpetrator

1. California – 17.1%
2. New York – 9.8%
3. Florida – 8.5%
4. Texas – 7.4%
5. Illinois – 3.6%
6. Pennsylvania – 3.6%
7. Ohio – 3.4%
8. Arizona – 3.1%
9. New Jersey – 2.9%
10. Michigan – 2.8%

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



Top Ten Countries - Perpetrator

1. United States – 76.7%
2. Nigeria – 5.1%
3. Canada – 3.5%
4. South Africa – 2.0%
5. Romania – 1.7%
6. Spain – 1.3%
7. Indonesia – .9%
8. Russia – .7%
9. Netherlands – .6%
10. Togo – .5%

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 39.4), and reside in one of the four most populated states: California, Florida, New York, and Texas (see Map 3). 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, Australia, and Japan (see Map 4). Please refer to Appendix II at the end of this report for more information about complainant statistics by state.

Chart 6
Gender of Complainant

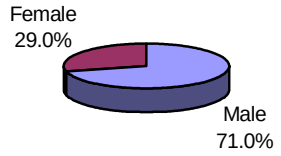


Chart 7
Age

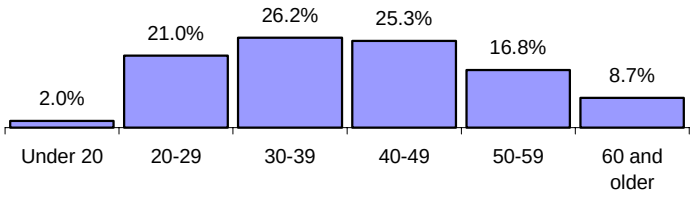


Table 3: Complainants per 100,000 population (based on 2002 Census figures)

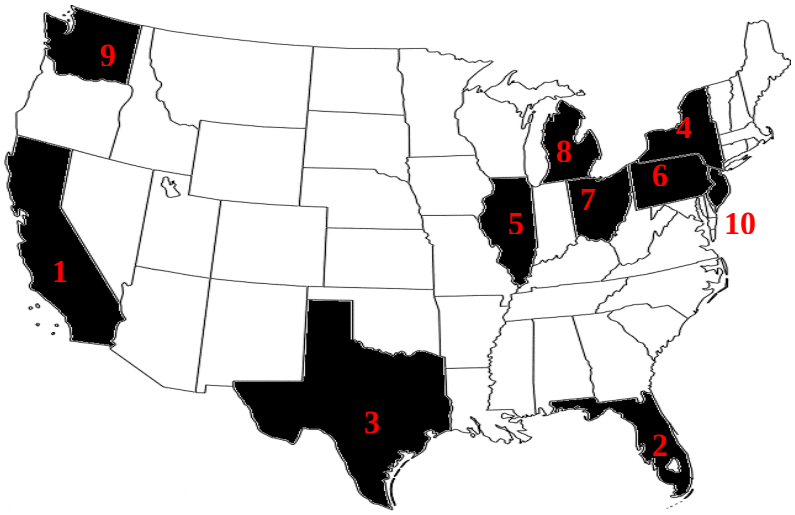
1. District of Columbia – 39.59
2. Hawaii – 33.10
3. Alaska – 31.22
4. Colorado – 30.27
5. Washington – 29.97
6. Oregon – 28.74
7. Arizona – 28.30
8. California – 25.24
9. Florida – 24.79
10. Maryland – 24.46

Table 4 looks at differences between the dollar loss per incident and the various complainant demographics. The amount lost appears to be related to a number of factors. First, males tend to lose more than females (ratio of over $2.00 to $1.00). Second, there are loss variations by age, with those 20-29 having the highest median dollar loss ($350). However, 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% of those in this group incurred losses of $5,000 or more).

Table 4: Amount Lost Per Referred Complaint By Gender and Age

Complainant Demographics		*Average (median) $ Loss per Typical Complaint*
Gender:	***Male***	$388
	Female	$168
Age:	***Under 20***	$270
	20-29	$350
	30-39	$285
	40-49	$260
	50-59	$295
	60 and older	$323

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



Top Ten States - Complainant

1. California – 15%
2. Florida – 7.0%
3. Texas – 6.9%
4. New York – 6.0%
5. Illinois – 3.9%
6. Pennsylvania – 3.8%
7. Ohio – 3.3%
8. Michigan – 3.3%
9. Washington – 3.1%
10. New Jersey – 3.0%

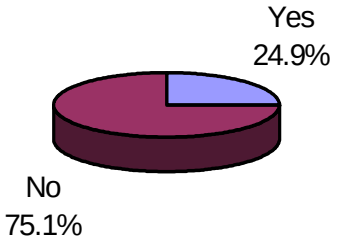
Map 4 - Top Ten Countries by Count: Individual Complainants (Number is Rank)

Top Ten Countries - Complainant

1. United States – 92.9%
2. Canada – 2.5%
3. Australia – .6%
4. Great Britain – .4%
5. Germany – .3%
6. Japan – .2%
7. Netherlands – .1%
8. Italy – .1%
9. India – .1%
10. France – .1%

Only one in four complainants were found to have previously sought assistance from a law enforcement agency prior to filing with IFCC. This trend is consistent with other data sets that track reporting practices among victims of fraud. The decision to initially reach out to a state or local enforcement agency is influenced by the monetary loss of the incident; victims who previously sought assistance had median financial losses of $500 (compared to a population average of $299).

Chart 8
Contacted Law Enforcement?



Complainant-Perpetrator Dynamics

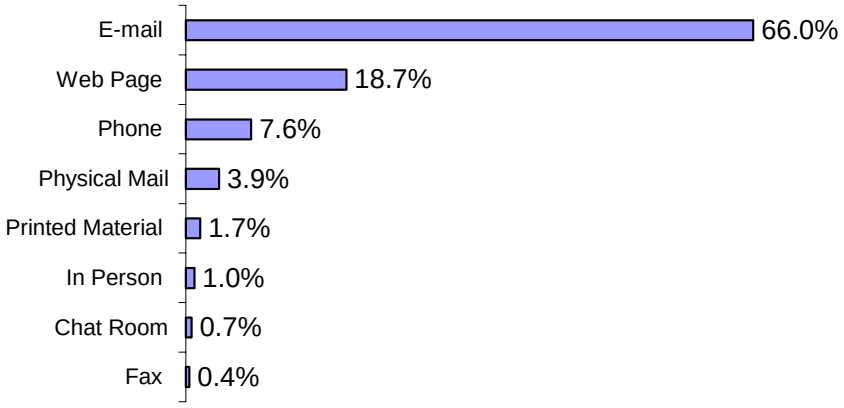
One of the components of fraud committed via the Internet that makes investigation and prosecution difficult is that the offender and victim may be located hundreds or thousands of miles apart. This is a unique characteristic not found with many other types of 'traditional' crime. These jurisdictional issues often require the cooperation of multiple agencies to resolve a given case. Table 5 highlights this truly 'borderless' phenomenon. Even in California, where IFCC statistics seem to indicate that most fraud originates, only 20.3% 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 5: Complainant-Perpetrator Locations, By State

State of Complainants	*% of Perpetrators from Same State*	*Other Location of Perpetrators, By %*	*Other Location of Perpetrators, By %*	*Other Location of Perpetrators, By %*
1. California	20.3%	New York (6.9%)	Texas (5.7%)	Florida (5.4%)
2. Arizona	20.3%	California (10.8%)	Florida (6.4%)	New York (5.6%)
3. Colorado	13.2%	California (17.9%)	Texas (7.7%)	New York (4.7%)
4. Texas	11.8%	California (16.0%)	Florida (6.3%)	New York (6.0%)
5. Illinois	10.5%	California (14.8%)	Texas (7.7%)	Florida (5.8%)
6. Michigan	10.4%	California (14.8%)	New York (6.2%)	Florida (6.0%)
7. Florida	9.8%	California (13.3%)	New York (6.4%)	Texas (5.5%)
8. New York	9.3%	California (16.1%)	Massachusetts (5.8%)	Florida (5.7%)
9. Washington	8.3%	California (17.0%)	Florida (6.9%)	Texas (6.4%)
10. Pennsylvania	8.0%	California (13.4%)	New York (7.0%)	Texas (5.5%)

The following chart provides further information on complainant-perpetrator dynamics. The majority of perpetrators were in contact with the complainant through either email (66%) or via the Web (18.7%). Less than one in ten (7.6%) had phone contact with the complainant and 3.9% had corresponded through the physical mail. Chat rooms (.7%) and in-person meetings (1.0%) appeared to take place very rarely.

Chart 9
Contact Method



Additional Information About IFCC Complaints

IFCC is dedicated to addressing complaints about fraud, specifically Internet fraud, although it regularly receives complaints about other crimes. IFCC processed 85,172 fraud and non-fraud complaints in 2002. This figure, which is higher than the 75,063 complaints received by IFCC during the same time period, represents a number of filings that were received in the fourth quarter of 2001. This backlog was caused in part by a shifting of IFCC resources following the September 11th incident, and has subsequently been eliminated. Overall, in addition to the 48,252 fraud referrals accepted during 2002, IFCC processed 36,920 non-fraudulent complaints. These non-fraud complaints include high-tech crimes, violent crimes, robberies, burglaries, threats, and many other violations of law. The people submitting these complaints to 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. Even though some of the complaints fall outside 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. If warranted, IFCC personnel may make contact with local law enforcement authorities on behalf of the complainant. IFCC receives a substantial number of computer-related complaints that are not fraudulent in nature. It is estimated that 4.3% of all complaints received at IFCC are computer intrusion/hacking, 11.6% are related to SPAM/unsolicited e-mail, and 1.5% involve child pornography.

For those filings that are computer-related but not considered Internet fraud, IFCC routinely refers these to agencies and organizations that handle those particular complaints and has aggressively developed partnerships with agencies to enhance the ability to serve victims of fraud. For example, if 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/). Unsolicited e-mail ("SPAM") and identity theft complaints are forwarded to the Federal Trade Commission (http://www.ftc.gov/) and IFCC has reached an arrangement with the U.S. Secret Service (http://www.treas.gov/usss/) for the purpose of referring complaints regarding credit card fraud and Nigerian Letter Fraud (419 scam).

One complaint that IFCC continues to receive in high volume is the well-known Nigerian letter fraud. The Nigerian letter fraud is defined as a correspondence outlining an opportunity to receive non-existent government funds from alleged dignitaries and is designed to collect advance fees from the victims. This is sometimes represented as payoff money required 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. It is sometimes referred to as "advance fee fraud." IFCC received 16,164 complaints of the Nigerian letter fraud in 2002. This is a five hundred percent increase over 2001 volume. In 2002, 74 individuals lost money totaling $1.6 million. Because of the scam, the country of Nigeria ranks second for total perpetrators.

During 2002, IFCC identified a variant of the traditional "419 Fraud" that has been commonly reported by complainants. The process of the scam is that the victim sells an item to the subject. The subject then tells the victim that he will be overpaying for the item and the victim is to send the remainder of the money somewhere else. The check presented by the subject is deposited by the victim's bank. However, the check is fraudulent and the victim is left paying the bill. In most cases the sum is large and can devastate a person's bank account or credit.

An example of this scam would be a situation where an individual sells a car for $8,000 dollars to a buyer. The buyer then sends the seller a check for $15,000 and tells the seller to take out the $8,000 and send the rest to a contact somewhere else. There can be a variety of reasons offered by the buyer as to the circumstances of this unusual transaction. The seller goes to the bank and cashes the check and forwards the $7,000 difference to the specified third party. Later, the seller is contacted by the bank, told that the check was fraudulent, and is asked to return the entire $15,000.

Results of IFCC Referrals

IFCC 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, IFCC can only gather this data from those agencies that voluntarily return enforcement results; it has no authority to require agencies to submit or return status forms. IFCC has assisted law enforcement with many successful case resolutions. A number of recent cases include:

United States v. Teresa Smith, No. 02CR40029-NMG (D. Mass.)

This case has been stated as one of the largest Internet scam investigations on record. Over 300 victims were involved, totaling more that $800,000 in losses. The first IFCC complaint on Teresa Smith came in February 2002 and was sent to the Massachusetts State Police. At that time no one was aware that over 300 more complaints on the same subject would be filed through IFCC, helping to unveil one of the largest Internet scams to date.

From April 2001 through October 2002, Ms. Smith was selling hundreds of computers to individual buyers through Internet auction Web sites. At the time, Ms. Smith was living in Worchester, Massachusetts, and operating from an office in West Boylston, Massachusetts.[3] Her scheme was simple: she would defraud her victims by selling a computer, requiring them to pay up front, and then not sending any of the merchandise and refusing any type of refund requested. When unsatisfied customers started questioning Ms. Smith's business ethics, they were given a number of false explanations. During the investigation it was discovered that Ms. Smith had spent most of the victims' money on living expenses, a new vehicle, and on an advertising business.[4] It was also discovered that Ms. Smith was using a number of different identities through eBay to perpetrate her fraud.[5] Each time eBay would receive complaints regarding Ms. Smith they would suspend her actions on their site. However, Ms. Smith would then simply change to another identity and the process would start all over again.

Complaints on Ms. Smith received by IFCC were initially sent to the Massachusetts State Police and, after dollar thresholds were met, to the Massachusetts Attorney General's Office for investigation. From there, the Massachusetts Attorney General sent copies of the complaints to the West Boylston Police department and the U.S. Postal Inspection Service in Boston. The initial arrest resulted from a warrant when Ms. Smith tried to pass a bad check. This led investigators to allegations that Ms. Smith had defrauded a large number of individuals.[6] After learning more about the fraud, the U.S. Attorney's Office, the Massachusetts Attorney General, the U.S. Postal Inspection Service, the FBI and the Worchester District Attorney's Office all launched investigations.[7]

---

[3] U.S. Department of Justice (Michael J. Sullivan United States Attorney District of Massachusetts)."Connecticut Women charged with Running $800,000 eBay Auction Fraud Scheme.
http://www.usdoj.gov/usao/ma/presspage/Dec2002/Smith-Teresa-plea.htm

[4] CNN "Scam Artists prowl online auction sites" January 10, 2003.
http://www.cnn.com/2003/TECH/internet/01/10/auction.scams.reut/

[5] IBID

[6] Boder, Jim Worcester Telegram and Gazette Staff April 23, 2002 "Money Disappeared into Web Addresses"
http://www.geocities.com/imad_scam/money.html

[7] IBID

In December 2002, the United States Attorney Michael Sullivan and Kenneth Jones, Inspector in Charge of the U.S. Postal Inspection Service's Northeast Region, announced that Ms. Smith pleaded guilty before U.S. District Judge Nathaniel M. Gorton to five counts of mail fraud and five counts of wire fraud.[8] Judge Gorton scheduled sentencing for March 18, 2003. If convicted, Smith faces a maximum of five years in prison on each count and a $250,000 fine.

People of the State of California v. Chris Chong Kim, No. DA239496 (Los Angeles Superior Court)

Chris Chong Kim of Los Angeles was arrested and charged with four counts of grand theft and 26 counts of holding a mock auction for allegedly failing to deliver computers and computer parts he sold through his e-Bay business site called Calvin Auctions.[9] Mr. Kim is being held on $400,000 bond and is currently awaiting trial.[10]

The first complaint against Mr. Kim was received by IFCC on July 15, 2002. The loss involved was over $2,000. From that date until the present IFCC has received 183 consumer complaints totaling more than $407,000. The Los Angeles County prosecutor's office reports that Kim had been selling computers and equipment through his Web site for at least two years. It was reported that in April 2002 Mr. Kim stopped sending the merchandise, prompting consumers to file reports with their local police department as well as with IFCC. Victim losses ranged anywhere from $1,900 to $6,000 each.[11] If convicted of all counts Mr. Kim could face up to 24 years in prison.[12]

Commonwealth of Virginia v. Mattehw William Tynan, Case No's. CR02000105-00-CR02000118-00 (Montgomery County Circuit Court, Criminal Division

IFCC contacted the Blacksburg, Va., Police Department, regarding a complaint filed on its Web site on August 15, 2001. The Las Vegas, Nev., victim filed a complaint for non-delivery of goods associated with an Internet auction. The victim responded to an advertisement on July 30, 2001, from a Web page advertising used wheels being offered for sale by an individual identifying his/herself as Colleen McGee of Christianburg, Va. The victim agreed to pay $425 for the wheels and processed payment through PayPal who verified that the seller was a verified customer.

On July 31, 2001, the victim received confirmation via e-mail from the seller that the wheels had been shipped. Subsequent e-mail contacts with the seller failed to ensure delivery of the wheels, and when the seller refused to provide a tracking number for the wheels, the victim began to think that the sale was a fraud. When the wheels had not arrived by August 5, 2001, the victim began tracking down the seller over the Internet by obtaining the IP address of the original ad placed by the seller with the Internet auction site. From this IP address the victim was able to find the Internet service provider used by the seller to place the ad. The origin of the advertisement was Blacksburg, Va. The victim also made contact with the Internet auction site to advise them of the seller's fraudulent activities, and was able to garner the names of additional victims of the same seller. This information was alluded to in the IFCC complaint with the victim stating that further information would be provided to the police agency that investigated the fraud.

The complaint received by IFCC on August 15, 2001, was referred to the IFCC member agency in Blacksburg, Va., where it was assigned to Patrol Officer II William Cullen for investigation. Officer Cullen was able to take the information provided by the victim and use that as the initial contact form for his investigation. After contact with the first victim, Officer Cullen was able to obtain the names and contact information for the additional victims. The resulting investigation by Officer Cullen resulted in 14 counts of theft by false pretenses against one Matthew Tynan, a.k.a. Colleen McGee. The case was presented to the Montgomery County Circuit Court where a guilty plea was entered, with all criminal charges being amended to misdemeanors. At sentencing, the defendant was ordered to make full restitution on over $9,000 of undelivered goods, and was required to serve thirty days in the county jail.

---

[8] U.S. Department of Justice (Michael J. Sullivan United States Attorney District of Massachusetts)."Connecticut Women charged with Running $800,000 eBay Auction Fraud Scheme".
http://www.usdoj.gov/usao/ma/presspage/Dec2002/Smith-Teresa-plea.htm

[9] Cnn.com http://www.cnn.com/2002/TECH/internet/12/05/crime.ebay.reut/ Dec 5, 2002

[10] Itworld.com:// http://www.itworld.com/Man/2681/021206ebayfraud/ Dec 6, 2002

[11] http://www.traderlist.com/ScamBusters.html

[12] Cnn.com http://www.cnn.com/2002/TECH/internet/12/05/crime.ebay.reut/ Dec 5, 2002

People of the State of California v. Raj Bindesh Trivedi, Case No. SD164405 (San Diego Superior Court)

The CATCH Task Force operating out of San Diego, Calif., has successfully prosecuted Raj Trivedi for victimizing more than 700 individuals throughout the world with his Internet fraud scheme of advertising high-tech products, accepting payment, and then failing to deliver the merchandise advertised. Losses resulting from Trivedi's frauds exceeded $992,000. Deputy Attorney General Tawnya Boulan of the California Attorney General's Office successfully prosecuted Trivedi. "His scheme was fairly complicated considering the number of victims he was able to scam over a relatively short period of time while working alone," Boulan said. "He showed a high level of sophistication in the execution of his fraud."

Trivedi victimized consumers who went to his Web site to purchase electronic equipment, such as computers and camcorders, or bid for similar products that Trivedi advertised on the auction Web sites eBay, uBid, and Yahoo!. Average losses for victims were about $1,200.

In September 2001, Trivedi moved from California to Fort Bend County, Tex., where he continued his fraudulent activities. On December 12, 2001, the Fort Bend County Sheriff's Department together with officials from the San Diego CATCH Task Force conducted a search warrant at Trivedi's home in Katy, Tex. Trivedi was arrested on a felony and theft warrant issued in California. Trivedi was returned to California where he entered a guilty plea to five felony counts from a 96-count indictment, including fraud, mock auction, grand theft, and accessing a computer to defraud. On March 22, 2002, he was sentenced to three years in prison and was ordered to pay restitution to the victims of his fraudulent activity.

The Internet not only provided the impetus for this case by having IFCC complaints filed and referred to the San Diego CATCH Task Force, but it also provided the California Attorney General's Office with the means of contacting victims about the ongoing investigation and the outcome of sentencing. Additionally, the California AG's Office encouraged people who felt they might have been victims of Trivedi's fraud scheme to file on-line complaints at the IFCC Web site located at www.ifccfbi.gov.

Conclusion

Since May 2000, IFCC has determined Internet fraud trends based on complaints filed by individuals from around the world. While these trends, reflected in the annual reports, can provide a picture 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 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. Despite the best proactive efforts, it appears victimization is on the rise. While the number of referrals at IFCC has tripled over the last year, these statistics represent only the tip of the proverbial iceberg; most of these crimes still fail to reach the attention of those agencies, such as IFCC, who are in a position to offer assistance. As online usage continues to climb, education must focus not only on preventive strategies (see Appendix III), but also on where an individual can turn for help should a crime occur.

Another important pattern that has emerged from IFCC data is the increasing prevalence of non-fraudulent activity that is being reported. The adoption of technology as an invaluable tool, for both commerce and communication, has resulted in a proliferation of problems that range from online harassment to computer intrusions. Outreach efforts must focus on keeping all online users safe from harm, whether that harm is fraudulent or non-fraudulent in nature.

Whether a victim has fallen prey to a bogus investment offer, a dishonest auction seller, or a host of other problems, 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.

Appendix I: Explanation of Complaint Categories

The Internet Fraud Complaint Center's Internet Fraud analysts sort each Internet fraud complaint received 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. [13] 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 identity theft 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.[14] Sports tampering and claiming false bets are two examples of gaming fraud.

- Communications Fraud- A fraudulent act or process involving systems 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.[15]

- 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.[16]

- Government Fraud- A knowing misrepresentation of the truth, or concealment of a material fact to induce the government to act to its own detriment.[17] 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.[18] 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.[19] 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.[20] Auction fraud and non-delivery of payment or merchandise are both types of

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

confidence fraud and are the most reported offenses to the IFCC. Nigerian Letter Scam is another offense classified under confidence fraud.

Appendix II: Complainant/Perpetrator Statistics, by State

Complainants By State

Represents % of total individual complainants where state is known.

1	California	15.0	**27**	Kansas	1.0
2	Florida	7.0	**28**	South Carolina	1.0
3	Texas	6.9	**29**	Louisiana	1.0
4	New York	6.0	**30**	Kentucky	1.0
5	Illinois	3.9	**31**	Utah	.9
6	Pennsylvania	3.8	**32**	Nevada	.8
7	Ohio	3.3	**33**	Iowa	.8
8	Michigan	3.3	**34**	Hawaii	.7
9	Washington	3.1	**35**	West Virginia	.6
10	New Jersey	3.0	**36**	Nebraska	.6
11	Virginia	2.9	**37**	Arkansas	.6
12	Massachusetts	2.6	**38**	New Hampshire	.5
13	Arizona	2.6	**39**	Mississippi	.5
14	Colorado	2.3	**40**	New Mexico	.5
15	Georgia	2.3	**41**	Idaho	.4
16	Maryland	2.3	**42**	District of Columbia	.4
17	North Carolina	2.2	**43**	Maine	.4
18	Indiana	1.8	**44**	Alaska	.3
19	Missouri	1.8	**45**	Rhode Island	.3
20	Tennessee	1.8	**46**	Montana	.3
21	Oregon	1.7	**47**	Delaware	.3
22	Wisconsin	1.7	**48**	Vermont	.2
23	Minnesota	1.5	**49**	North Dakota	.2
24	Connecticut	1.4	**50**	South Dakota	.2
25	Alabama	1.1	**51**	Wyoming	.1
26	Oklahoma	1.1			

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

Perpetrators By State

Represents % of total individual perpetrators where state is known.

1	California	17.1	**27**	Louisiana	1.0
2	New York	9.8	**28**	Oklahoma	1.0
3	Florida	8.5	**29**	Wisconsin	.8
4	Texas	7.4	**30**	Utah	.7
5	Illinois	3.6	**31**	Kentucky	.7
6	Pennsylvania	3.6	**32**	Kansas	.6
7	Ohio	3.4	**33**	Arizona	.6
8	Arizona	3.1	**34**	Maine	.6
9	New Jersey	2.9	**35**	West Virginia	.5
10	Michigan	2.8	**36**	Iowa	.5
11	Washington	2.7	**37**	Rhode Island	.4
12	Georgia	2.6	**38**	Nebraska	.4
13	Tennessee	2.3	**39**	Mississippi	.4
14	Massachusetts	2.2	**40**	Hawaii	.3
15	Virginia	2.0	**41**	Delaware	.3
16	Nevada	1.9	**42**	New Hampshire	.3
17	Maryland	1.8	**43**	New Mexico	.3
18	North Carolina	1.6	**44**	District of Columbia	.2
19	Indiana	1.6	**45**	Idaho	.2
20	Connecticut	1.4	**46**	Montana	.2
21	Missouri	1.4	**47**	Alaska	.2
22	Oregon	1.3	**48**	Wyoming	.1
23	Alabama	1.3	**49**	Vermont	.1
24	Colorado	1.1	**50**	South Dakota	.1
25	Minnesota	1.0	**51**	North Dakota	.1
26	South Carolina	1.0			

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

Complainants per 100,000 population (based on 2002 Census figures)

1	District of Columbia	39.59	**27**	Missouri	18.83
2	Hawaii	33.10	**28**	Texas	18.74
3	Alaska	31.22	**29**	New York	18.62
4	Colorado	30.27	**30**	Oklahoma	18.43
5	Washington	29.97	**31**	Illinois	18.34
6	Oregon	28.74	**32**	Wisconsin	18.18
7	Arizona	28.30	**33**	Pennsylvania	18.18
8	California	25.24	**34**	Minnesota	18.13
9	Florida	24.79	**35**	Tennessee	17.94
10	Maryland	24.46	**36**	Indiana	17.60
11	Connecticut	24.22	**37**	Wyoming	17.45
12	Massachusetts	24.04	**38**	Rhode Island	17.20
13	Virginia	23.76	**39**	Maine	17.15
14	New Hampshire	23.14	**40**	Ohio	17.09
15	Nevada	22.91	**41**	Iowa	16.51
16	Utah	22.28	**42**	North Carolina	15.81
17	Kansas	21.83	**43**	Georgia	15.72
18	Vermont	21.41	**44**	Alabama	14.98
19	New Jersey	20.72	**45**	New Mexico	14.82
20	Nebraska	20.53	**46**	South Carolina	14.39
21	West Virginia	20.20	**47**	South Dakota	14.06
22	Montana	20.12	**48**	Kentucky	14.05
23	Delaware	19.57	**49**	Louisiana	12.96
24	Idaho	19.39	**50**	Arkansas	12.95
25	Michigan	19.21	**51**	Mississippi	10.24
26	North Dakota	19.08			

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

Perpetrators per 100,000 population (based on 2002 Census figures)

1	Nevada	20.75	**27**	Hawaii	6.75
2	Arizona	13.93	**28**	Virginia	6.66
3	New York	12.71	**29**	Wyoming	6.62
4	Florida	12.61	**30**	Montana	6.27
5	California	12.08	**31**	Indiana	6.27
6	Washington	11.09	**32**	Nebraska	6.25
7	Maine	10.74	**33**	Colorado	6.21
8	District of Columbia	10.51	**34**	South Carolina	6.09
9	Rhode Island	10.28	**35**	New Hampshire	6.04
10	Connecticut	10.23	**36**	Missouri	5.96
11	Tennessee	9.97	**37**	Kansas	5.93
12	Delaware	9.78	**38**	Alaska	5.90
13	Oregon	9.26	**39**	Louisiana	5.42
14	Massachusetts	8.40	**40**	Arkansas	5.24
15	Texas	8.40	**41**	Minnesota	5.08
16	New Jersey	8.37	**42**	Vermont	4.87
17	Maryland	8.10	**43**	North Carolina	4.70
18	Utah	7.77	**44**	Idaho	4.47
19	Georgia	7.53	**45**	Iowa	4.36
20	Ohio	7.33	**46**	Kentucky	4.25
21	West Virginia	7.33	**47**	Wisconsin	3.82
22	Pennsylvania	7.19	**48**	New Mexico	3.77
23	Illinois	7.17	**49**	Mississippi	3.34
24	Alabama	7.07	**50**	South Dakota	3.02
25	Michigan	6.86	**51**	North Dakota	3.00
26	Oklahoma	6.81			

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

Appendix III: Best Practices to Prevent Internet Fraud

This section outlines best practices to avoid being the victim of fraud. Should a fraudulent offense occur, individuals are encouraged to first file a complaint with the Internet Fraud Complaint Center at http://www.ifccfbi.gov. Though this action will get information into the hands of appropriate enforcement agencies, victims are encouraged to follow additional steps (as outlined below) to ensure a successful resolution to their particular problem.

Internet Auction Fraud

Steps to take if victimized

1. File a complaint with the online auction company. In order to be considered for eBay's Fraud Protection Program, you should submit an Online Fraud Complaint at http://crs.ebay.com/aw-cgi/ebayisapi.dll?crsstartpage 30 days after the listing end-date.
2. Notify your local and state law enforcement officials.
3. Notify law enforcement officials in the perpetrator's town and state.
4. File a complaint with the shipper (e.g., USPS can be reached at http://www.usps.com/websites/depart/inspect.)
5. File a complaint with the Better Business Bureau http://www.bbb.org.

Steps to take to avoid being victimized

- 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 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, 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 U.S. and other countries. If a problem occurs with an auction transaction that involves 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.
- 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, 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.
- Do not judge a person/company by their fancy web site; thoroughly check the person/company out.
- Be cautious when responding to special offers (especially through unsolicited e-mail).
- Be cautious when dealing with individuals/companies from outside your own country. Remember the laws of different countries might pose issues if a problem arises with your transaction.
- Inquire about returns and warranties on all items.
- The safest way to purchase items via the Internet is by credit card because you can often dispute the charges if something is wrong. Also, consider utilizing an escrow or alternate payment service.
- Make sure the web site is secure when you electronically send your credit card numbers.

Credit Card Fraud

- Don't give out your credit card number(s) online unless the site is both secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but may provide you some assurance.
- Before using the site, check out the security software it uses to 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 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 sellers who use free e-mail services where a credit card wasn't required to open the account.
- Check with the Better Business Bureau to see if there have been any complaints against the seller.
- 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.
- 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.

<u>Tips to minimize the risk of credit card fraud for businesses:</u>

- Don't accept orders unless complete information is provided (including full address and phone number). Require address verification for all of your credit card orders. Require anyone who uses a different shipping address than their billing address to send a fax with their signature and credit card number authorizing the transaction.
- Be especially careful with orders that come from free email services -- there is a much higher incidence of fraud from these services. Many businesses will no longer accept orders that come through these free email accounts. Send an email requesting additional information before you process the order asking for: an email address other than a free service, the name and phone number of the bank that issued the credit card, the exact name on the credit card, and the exact billing address.
- Be wary of orders that are larger than your typical order amount, and of orders with next-day delivery
- Pay extra attention to international orders. Validate the order before you ship your product to a different country.
- If you're suspicious, pick up the phone and call the customer to confirm the order.
- Consider using software or services to fight credit card fraud online.
- If defrauded by a credit card thief, you should contact your bank and law enforcement authorities.

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.
- Inquire about all the terms and conditions regarding the investors and the investment.
- Rule of Thumb: If it sounds too good to be true, it probably is.

Nigerian Letter Fraud

Steps to take if you receive a Nigerian Scam Letter

1. If you are a United States citizen or resident and have suffered No Financial Loss, write "No Financial Loss – For Your Database" on the documents you received and fax them to the U.S. Secret Service Task Force handling scam matters at 202-406-6930 or 202-406-5031. Actual hardcopy of the scam document(s) is required to add your scam information to the Task Force Database.
2. If you are a United States citizen or resident and have suffered a financial loss, write "Financial Loss - Contact Me ASAP" on the documents you have received and fax them to the Task Force at 202-406-6930 or 202-406-5031 and give your telephone number. A U.S.Secret Service Agent will call you back to discuss the matter with you.

Additional Steps for International Citizens and Residents

1. Fax hardcopy of the scam correspondence you received, especially any banking data, to the US Task Force at 202-406-6930 or 202-406-5031, , so that it can be included in the Task Force Database. State what country you are sending from and state whether there has been a loss or there is no loss.
2. Notify your own nation's national law enforcement agency and your own nation's foreign office.

- 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.

Identity Theft

Steps to take if victimized

1. Contact the fraud departments of each of the three major credit bureaus and report that your identity has been stolen.
2. Get a "fraud alert" placed on your file so that no new credit will be granted without your approval.
3. Contact the security departments of the appropriate creditors and/or financial institutions for any accounts that may have been fraudulently accessed. Close these accounts. Create new passwords on any new accounts you open.
4. File a report with your local police and/or the police where the identity theft took place.
5. Retain a copy of the police report because it may be needed by the bank, credit card company, or other businesses to prove your innocence.

Steps to take to avoid being victimized

- Check your credit reports from all three of the credit reporting agencies once a year.
- Guard your Social Security number. When possible, don't carry your Social Security card with you.
- Don't have your SSN or driver's license number printed on your checks.
- Guard your personal information. You should never give your Social Security number to anyone unless they have a good reason for needing it.
- Carefully destroy papers you throw out, especially those with sensitive or identifying information.
- Be suspicious of telephone solicitors. Never provide information unless you have initiated the call.
- Delete without replying to any suspicious email requests.