2007 Internet Crime Report

Internet Crime Complaint Center

Prepared by:
The National White Collar Crime Center
Bureau of Justice Assistance
Federal Bureau of Investigation

Contents

1. 2007 Internet Crime Report 1

Executive Summary . . . 1
Overview . . . 1
General IC3 Filing Information . . . 2
Complaint Characteristics . . . 5
Perpetrator Characteristics . . . 7
Complainant Characteristics . . . 10
Complainant - Perpetrator Dynamics . . . 13
Additional Information About IC3 Referrals . . . 14
Scams of 2007 . . . 14
Results of IC3 Referrals . . . 15
Conclusion . . . 17

2. Appendix 18

Appendix 1: Explaination of Complaint Categories . . . 18
Appendix 2: Best Practices to Prevent Internet Fraud . . . 19
Appendix 3: Complainant/Perprtrator Statistics, by State . . . 22

Tables/Charts/Maps

Chart 1 . . . 2
Chart 2 . . . 3
Chart 3 . . . 3
Chart 4 . . . 4
Chart 5 . . . 5
Chart 6 . . . 6
Table 1 . . . 6
Chart 7 . . . 7
Map 1 . . . 8
Table 2 . . . 8
Map 2 . . . 9
Chart 8 . . . 10
Chart 9 . . . 10
Map 3 . . . 11
Table 3 . . . 11
Map 4 . . . 12
Table 4 . . . 12
Table 5 . . . 13
Chart 10 . . . 13
Table 6 . . . 22
Table 7 . . . 23
Table 8 . . . 24
Table 9 . . . 25

1 2007 Internet Crime Report

EXECUTIVE SUMMARY

The 2007 Internet Crime Report is the seventh annual compilation of information on complaints received and referred by the Internet Crime Complaint Center (IC3) to law enforcement or regulatory agencies for appropriate investigative action. From January 1, 2007 to December 31, 2007, the IC3 website received 206,884 complaint submissions. This is a 0.3% decrease when compared to 2006 when 207,492 complaints were received. These filings were composed of fraudulent and non-fraudulent complaints primarily related to the Internet.

In 2007, IC3 processed more than 219,553 complaints that support Internet crime investigations by law enforcement and regulatory agencies nationwide. These complaints were composed of many different fraud types such as auction fraud, non-delivery, and credit/debit card fraud, as well as other illegal behavior, such as computer intrusions, spam/unsolicited e-mail, and child pornography. All of these complaints are accessible to federal, state, and local law enforcement to support active investigations, trend analysis, and public outreach and awareness efforts.

From the submissions, IC3 referred 90,008 complaints of crime to federal, state, and local law enforcement agencies around the country for further consideration. The vast majority of cases referred alleged fraud and involved a financial loss on the part of the complainant. The total dollar loss from all referred cases of fraud was $239.09 million with a median dollar loss of $680.00 per complaint. This was an increase from $198.44 million in total reported losses in 2006. Other significant findings related to an analysis of referrals include:

- Perpetrators were predominantly male (75.8%) and half resided in one of the following states: California, Florida, New York, Texas, Illinois, Pennsylvania and Georgia. The majority of reported perpetrators were from the United States. However, a significant number of perpetrators also were located in United Kingdom, Nigeria, Canada, Romania, and Italy.
- Among complainants, 57.6% were male, nearly half were between the ages of 30 and 50 and one-third resided in one of the four most populated states: California, Florida, Texas, and New York. While most were from the United States, IC3 received a number of complaints from Canada, United Kingdom, Australia, India, and Mexico.
- Males complainants lost more money than females (ratio of $1.67 to every $1.00 lost per female). This may be a function of both online purchasing differences by gender and the type of fraudulent schemes by which the individuals were victimized.
- Electronic mail (e-mail) (73.6%) and web pages (32.7%) were the two primary mechanisms by which the fraudulent contact took place.
- Recent high activity scams commonly reported to the IC3 in 2007 were those involving pets, checks, spam, and online dating sites, all of which have proven effective as criminal devices in the hands of fraudsters.

OVERVIEW

The Internet Crime Complaint Center (IC3), began operation on May 8, 2000 as the Internet Fraud Complaint Center. In December 2003, the Internet Fraud Complaint Center (IFCC) was renamed the Internet Crime Complaint Center (IC3) to better reflect the broad character of such criminal matters having a cyber (Internet) nexus. IC3 established a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI) to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. IC3 was intended and continues to emphasize serving the broader law enforcement community, including federal, state and local agencies, which employ key participants in the growing number of Cyber Crime Task Forces. Since its inception, IC3 has received complaints across a wide variety of cyber crime matters, including online fraud (in its many forms), intellectual property rights (IPR) matters, computer intrusions (hacking), economic espionage (theft of trade secrets), child pornography, international money laundering, identity theft, and a growing list of additional criminal matters.

IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving Internet related crimes. Significant and supplemental to partnering with law enforcement and regulatory agencies, it will remain a priority objective of IC3 to establish effective alliances with industry. Such alliances will enable IC3 to leverage both intelligence and subject matter expert resources, pivotal in identifying and crafting an aggressive, proactive approach to combating cyber crime. In 2007, the IC3 saw an increase in

several additional crimes that were exclusively related to the Internet these included but are not limited to pet scams, check cashing scams, online dating fraud, phishing, spoofing, and spam. Each of these types of complaints has increased in prevalence over the past year.

Overall, the "IC3 2007 Internet Crime Report" is the seventh annual compilation of information on complaints received and referred by IC3 to law enforcement or regulatory agencies for action. This report provides an examination of key characteristics of 1) complaints, 2) perpetrators, 3) complainants, 4) interaction between perpetrators and complainants, 5) common Internet scams observed throughout the year and 6) success stories involving complaints referred by IC3. The results in this report are intended to enhance our general knowledge about the scope and prevalence of Internet crime in the United States. This report does not represent all victims of Internet crime or fraud because it is derived solely from information provided by the people who filed a complaint with IC3.

GENERAL IC3 FILING INFORMATION

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

From January 1, 2007 to December 31, 2007, there were 206,884 complaints filed online with IC3. This is a 0.3% decrease compared to 2006 when 207,492 complaints were received (see Chart 1). The number of complaints filed per month, last year, averaged 17,240 (see Chart 2). Dollar loss of referred complaints was at an all-time high in 2007, at $239.09 million, as compared to previous years (see Chart 3).

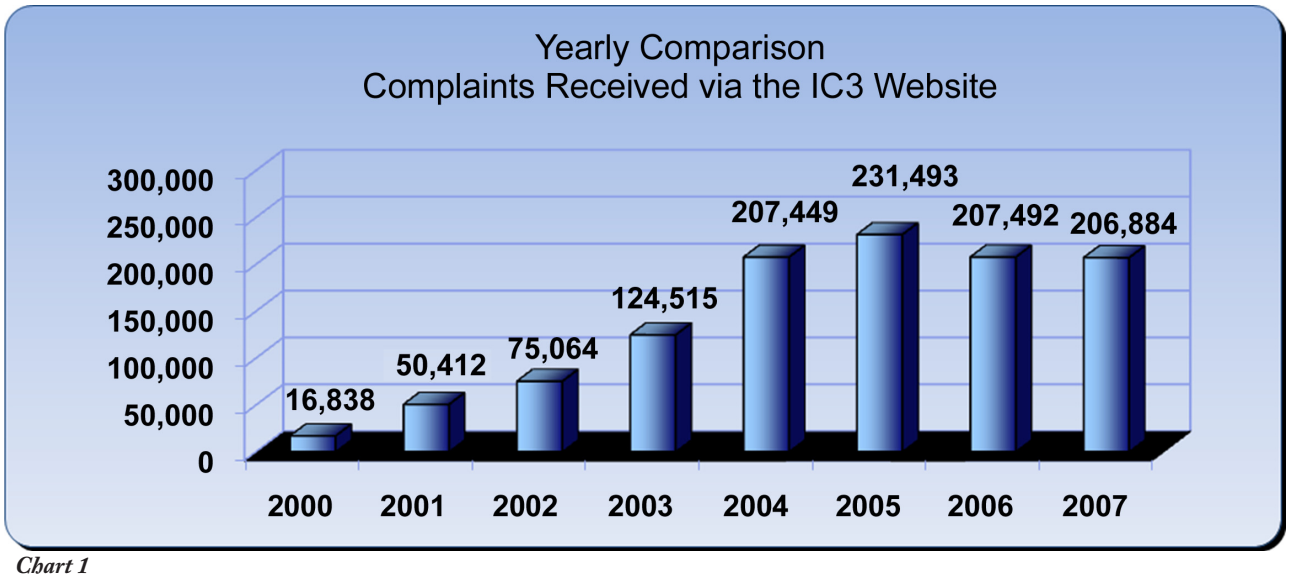


Chart 1

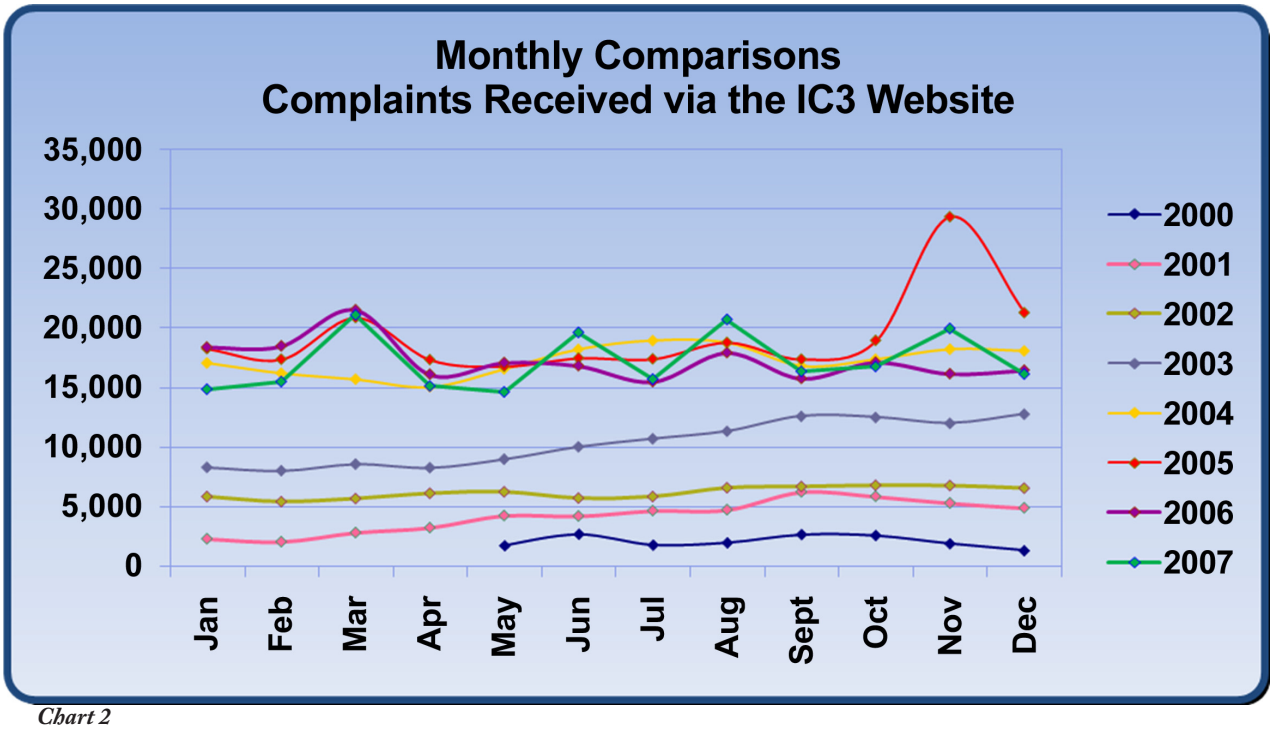


Chart 2

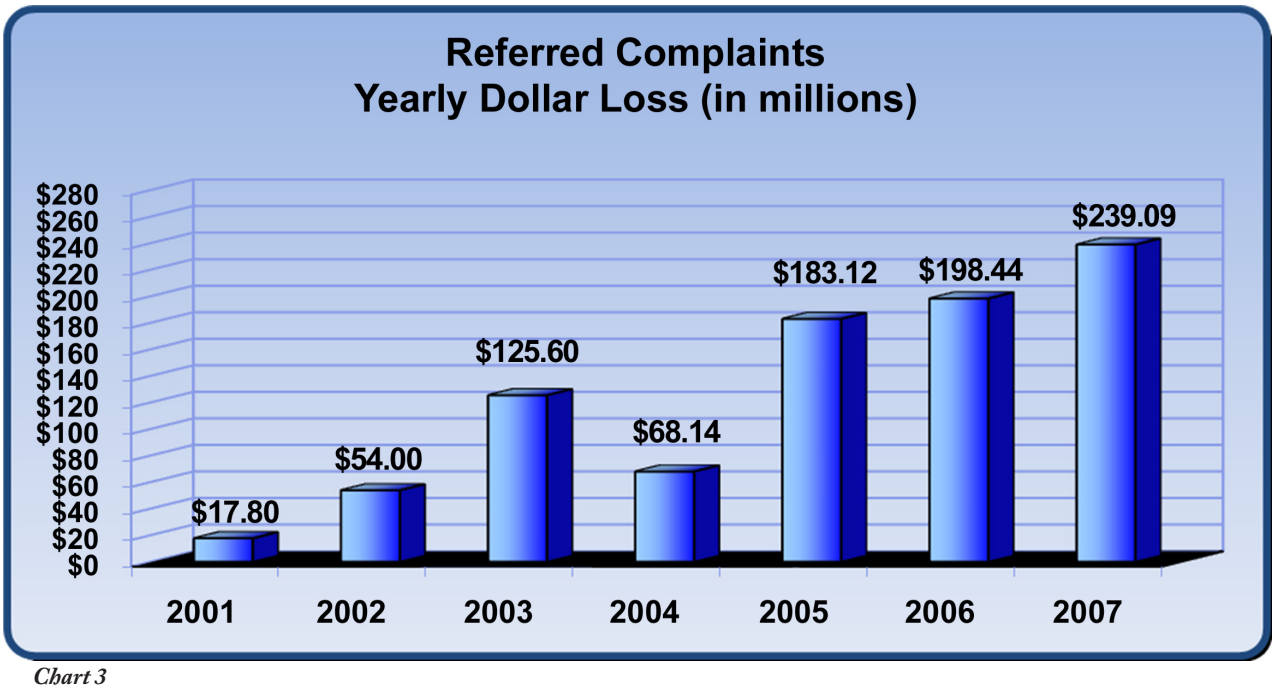


Chart 3

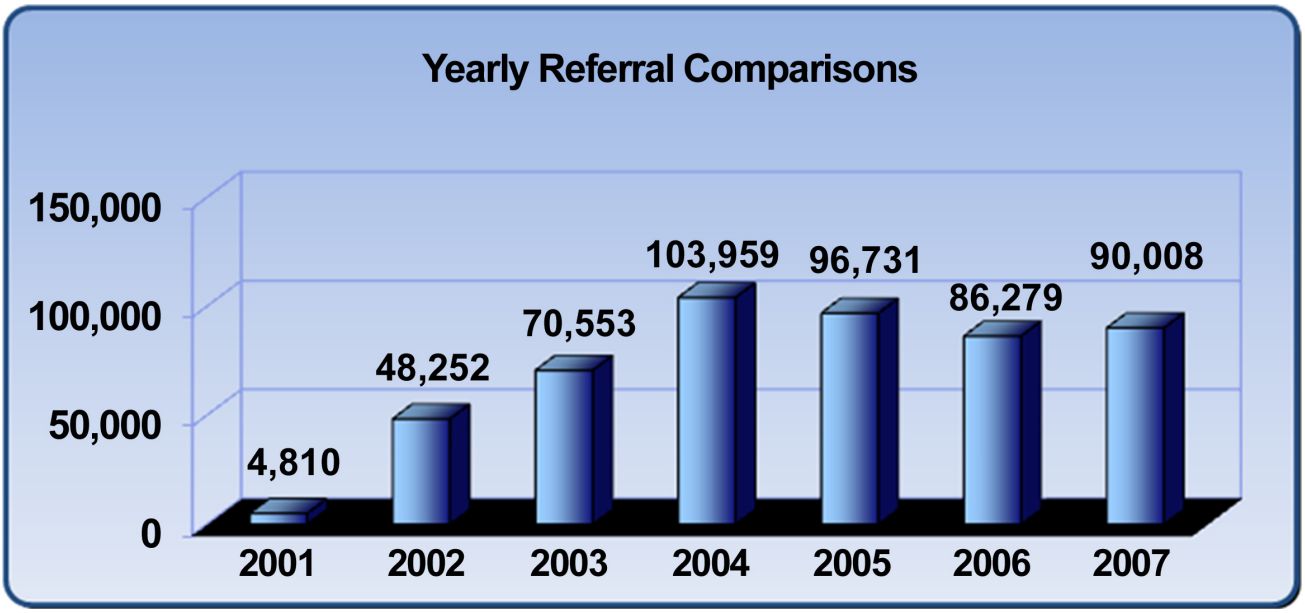


Chart 4

The number of referred complaints has increased slightly from 86,279 in 2006 to 90,008 in 2007 (see Chart 4). The 116,876 complaints that were not directly referred to law enforcement are accessible to law enforcement, used in trend analysis, and also help provide a basis for future outreach events and educational awareness programs. Typically, these complaints do not represent dollar loss but provide a picture of the types of scams that are emerging via the Internet. These complaints in large part are comprised of fraud involving reshipping, counterfeit checks, phishing, etc.

During 2007, there were 219,553 complaints processed on behalf of the complainants. This total includes various crime types, such as auction fraud, non-delivery, and credit/debit card fraud, other criminal complaints as well as non-fraudulent complaints, such as computer intrusions, spam, and child pornography.

The results contained in this report were based on information that was provided to IC3 through the complaint forms submitted online at www.ic3.gov or www.ifccfbi.gov by complainants; however, the data represents a sub-sample comprised of those complaints referred to law enforcement. While IC3's primary mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime, those complaints involving more traditional methods of contact (e.g., telephone and mail) were also referred. Using information provided by the complainants, it is estimated that over 90% of all complaints were related to the Internet or online service. Criminal complaints were referred to law enforcement and/or regulatory agencies based on the residence of the subject(s) and victims(s). In 2007, there were 1 Memorandums of Understanding (MOUs) from non-NW3C member agencies added to the IC3 database system and an additional 12 NW3C member agencies added to the database.

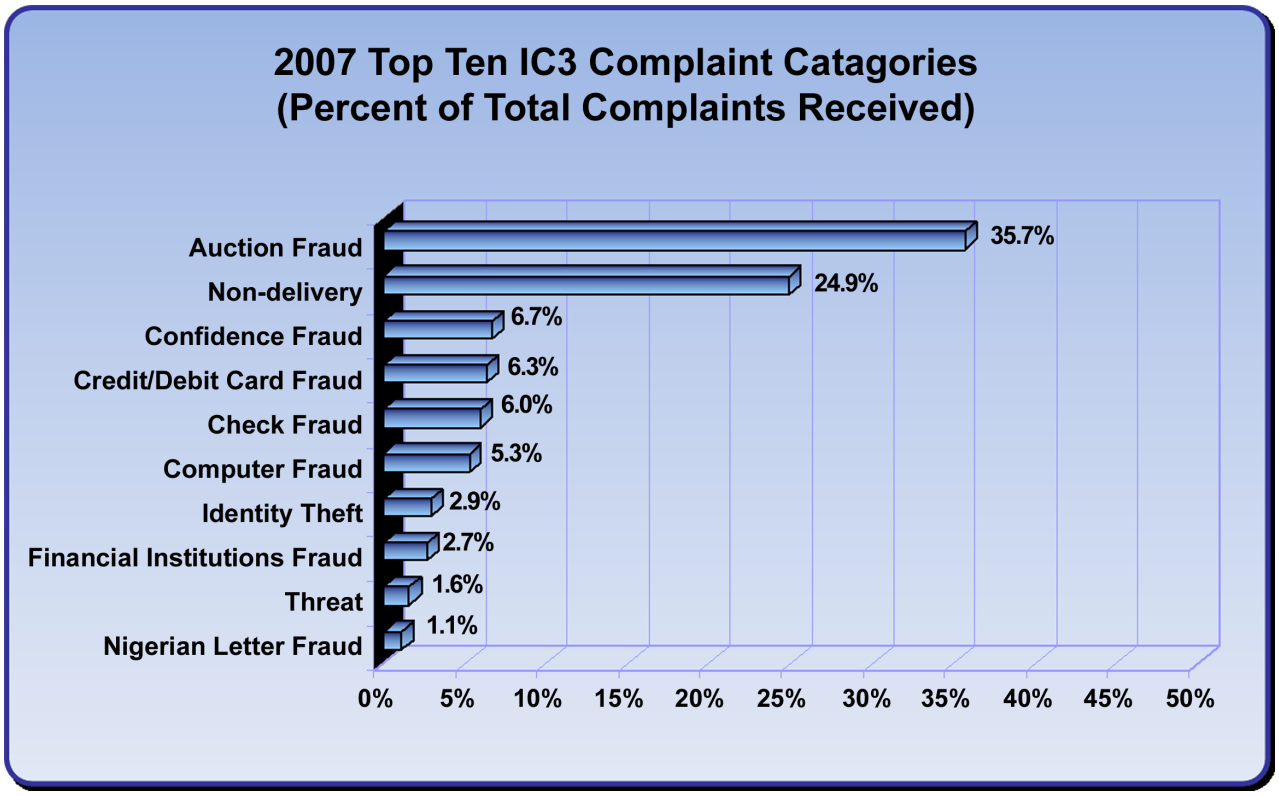


Chart 5

COMPLAINT CHARACTERISTICS

During 2007, Internet auction fraud was by far the most reported offense, comprising 35.7% of referred crime complaints. This represents a 20.5% decrease from the 2006 levels of auction fraud reported to IC3. In addition, during 2007, the non-delivery of merchandise and/or payment represented 24.9% of complaints (up 31.1% from 2006). Confidence fraud made up an additional 6.7% of complaints (see Chart 5). Credit and debit card fraud, check fraud, and computer fraud complaints represented 17.6% of all referred complaints. Other complaint categories such as identity theft, financial institutions fraud, threats, and Nigerian letter fraud complaints together represented less than 8.3% of all complaints.

Statistics contained within a complaint category must be viewed as a snapshot which may produce a misleading picture due to the perception of consumers and how they characterize their particular victimization within a broad range of complaint categories. It is important to realize IC3 has actively sought support from many key Internet E-Commerce stake holders. As part of these efforts, many of these companies, such as eBay, have provided their customers with links to the IC3 website. As a direct result, an increase in referrals depicted as auction fraud has emerged.

Through its relationships with law enforcement and regulatory agencies, IC3 continues to refer specific fraud types to the agencies with jurisdiction over the matter. Complaints received by IC3 included confidence fraud, investment fraud, business fraud, and other unspecified frauds. Identity theft complaints are referred to the Federal Trade Commission (FTC) and also are being addressed by other agencies. Nigerian letter fraud or 419 scams are referred to the United States Secret Service (USSS) in addition to other agencies.

Compared to 2006, there were slightly higher reporting levels of all complaint types, except for auction fraud and investment fraud, in 2007. For a more detailed explanation of complaint categories used by IC3, refer to Appendix I at the end of this report.

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

Of the 90,008 fraudulent referrals processed by IC3 during 2007, 72,226 involved a victim who reported a monetary loss. Other complainants who did not file a loss may have reported the incident prior to victimization (e.g., received a fraudulent business investment offer online or in the mail), or may have already recovered money from the incident prior to filing (e.g., zero liability in the case of credit/debit card fraud). Other referrals that do not have a dollar loss such as child pornography are sent to the National Center for Missing and Exploited Children, terrorist tips are sent to PACU and threats which are referred to state and local law enforcement.

The total dollar loss from all referred cases of fraud in 2007 was $239.09 million. That loss was greater than 2006 when a total

loss of $198.44 million was reported. Of those complaints with a reported monetary loss, the mean dollar loss was $2,529.90 and the median was $680.00. Nearly sixteen percent (15.5%) of these complaints involved losses of less than $100.00, and forty one and a half percent (41.5%) reported a loss between $100.00 and $1,000.00. In other words, over half of these cases involved a monetary loss of less than $1,000.00. Nearly a third (30.7%) of the complainants reported losses between $1,000.00 and $5,000.00 and only 12.2% indicated a loss greater than $5,000.00 (see Chart 6). The highest dollar loss per incident was reported by Investment Fraud (median loss of $3,547.94). Check fraud victims, with a median loss of $3,000.00 and Nigerian letter fraud (median loss of $1,922.99) were other high dollar loss categories. The lowest dollar loss was associated with credit/debit card fraud (median loss of $298.00).

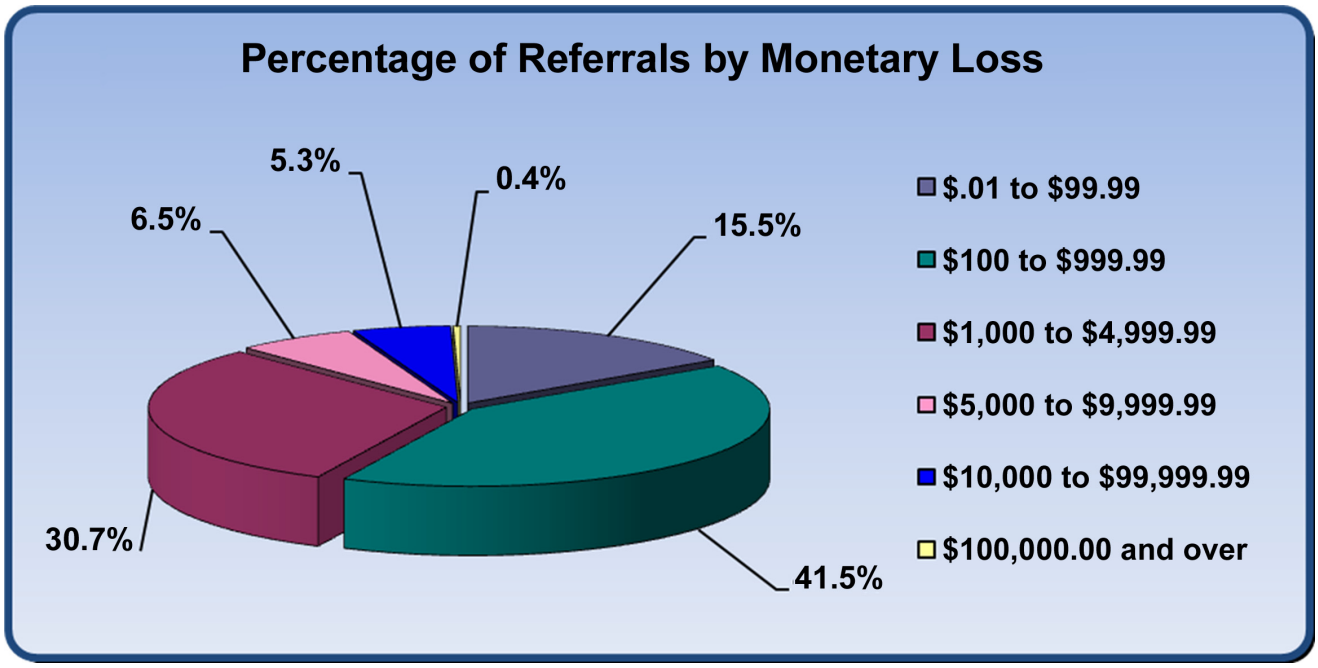


Chart 6

Amount Lost by Selected Fraud Type for Individuals Reporting Monetary Loss

Complaint Type	% of Reported Total Loss	Of those who reported a loss the Average (median) $ Loss per Complaint
Investment Fraud	6.1%	$3,547.94
Check Fraud	9.9%	$3,000.00
Nigerian Letter Fraud	6.4%	$1,922.99
Confidence Fraud	12.6%	$1,200.00
Auction Fraud	22.4%	$483.95
Non-delivery (merchandise and payment)	17.8%	$466.00
Credit/Debit Card Fraud	4.6%	$298.00

Table1

PERPETRATOR CHARACTERISTICS

Equally important to presenting the prevalence and monetary impact of Internet fraud is providing insight into the demographics of fraud perpetrators. In those cases with a reported location, over 75% of the perpetrators were male and over half resided in one of the following states: California, Florida, New York, Texas, Illinois, Pennsylvania, and Georgia (see Chart 7 and Map 1). These locations are among the most populous in the country. Controlling for population, District of Columbia, Nevada, Delaware, Florida, New York, and Utah have the highest per capita rate of perpetrators in the United States. Perpetrators also have been identified as residing in United Kingdom, Nigeria, Canada, Romania, and Italy (see Map 2). Interstate and international boundaries are irrelevant to Internet criminals. Jurisdictional issues can impede investigations due to issues with multiple victims, multiple states/countries, and varying dollar loss thresholds used for initiating investigations.

The vast majority of perpetrators were in contact with the complainant through either e-mail or via the web. (Refer to Appendix III at the end of this report for more information about perpetrator statistics by state). These statistics highlight the anonymous nature of the Internet. The gender of the perpetrator was reported only 42% of the time, and the state of residence for domestic perpetrators was reported only 35.1% of the time.

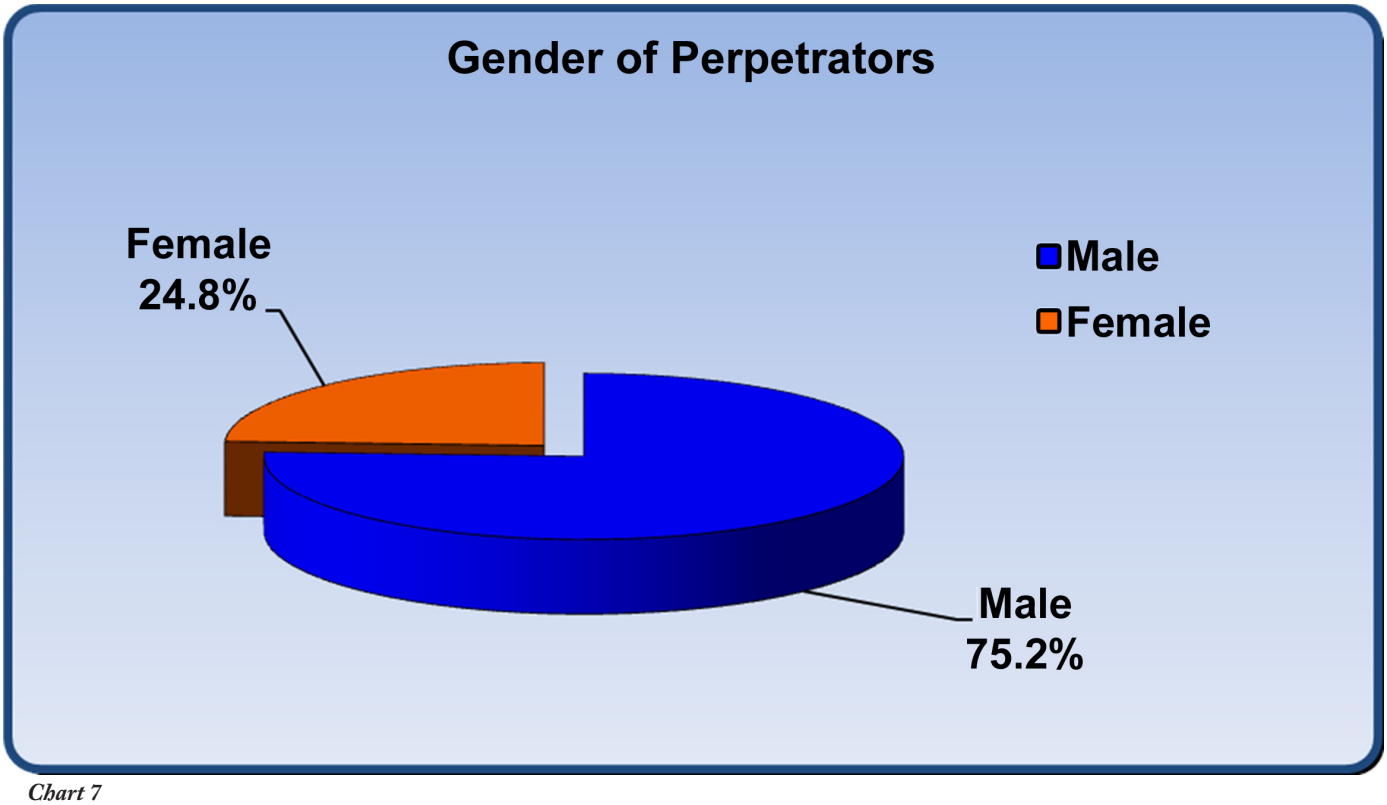
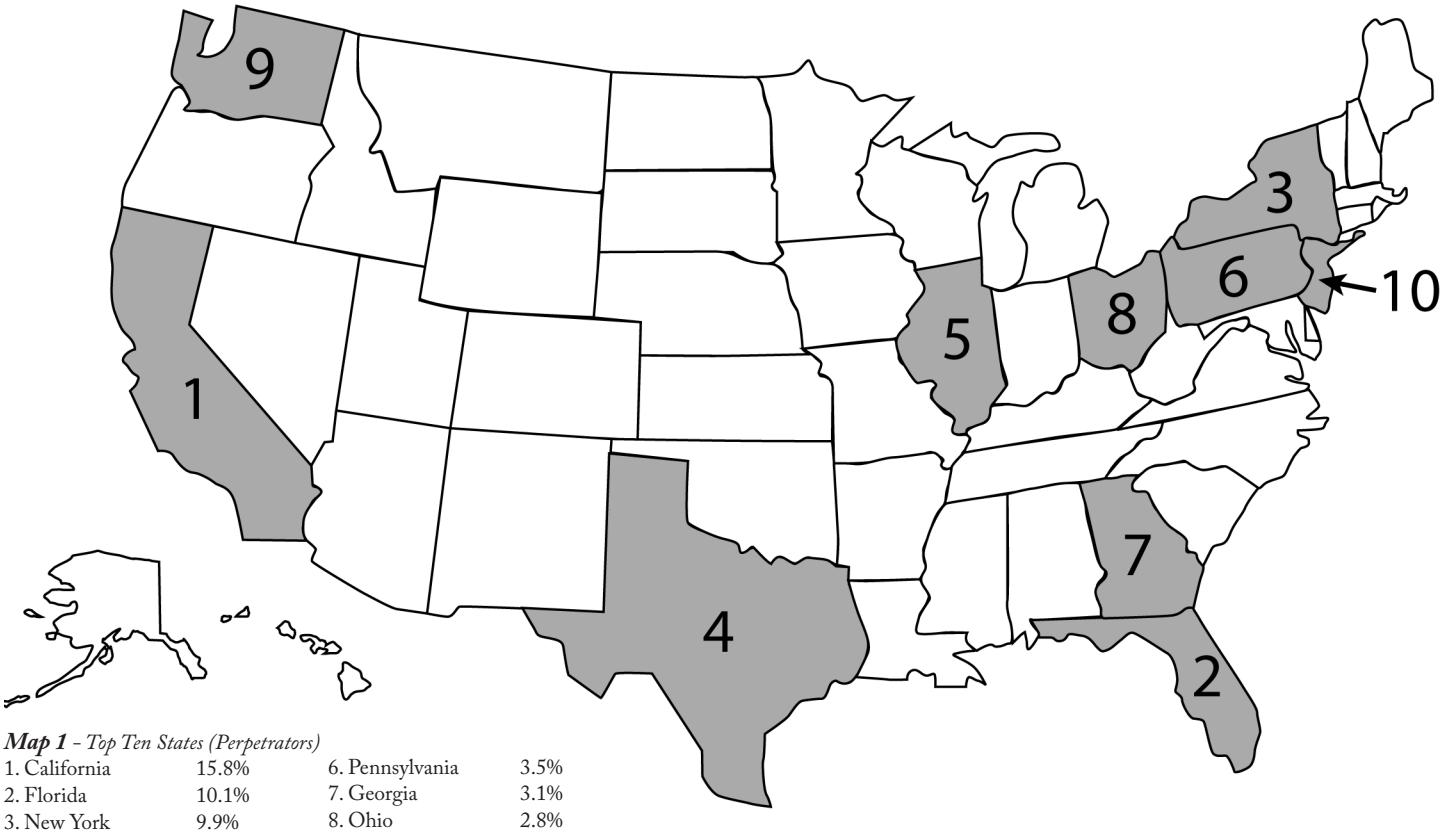


Chart 7

Top Ten States by Count: Individual Perpetrators



Map 1 *- Top Ten States (Perpetrators)*

1. California	15.8%	6. Pennsylvania	3.5%
2. Florida	10.1%	7. Georgia	3.1%
3. New York	9.9%	8. Ohio	2.8%
4. Texas	7.0%	9. Washington	2.8%
5. Illinois	3.6%	10. New Jersey	2.8%

Perpetrators per 100,000 people

Rank	State	Per 100,000 People
1	District of Columbia	99.10
2	Nevada	65.45
3	Delaware	41.98
4	Florida	40.73
5	New York	38.06
6	Utah	36.40
7	Washington	31.96
8	California	31.87
9	Alaska	28.53
10	Rhode Island	28.45

Table 2

Top Ten Countries By Count: Perpetrators

Map 2 *- Top Ten Countries By Count (Perpetrators)*

1. United States	63.2%	6. Italy	1.3%
2. United Kingdom	15.3%	7. Spain	0.9%
3. Nigeria	5.7%	8. South Africa	0.9%
4. Canada	5.6%	9. Russia	0.8%
5. Romania	1.5%	10. Ghana	0.7%

COMPLAINANT CHARACTERISTICS

The following graphs offer a detailed description of the individuals who filed an Internet fraud complaint through IC3. The average complainant was male, between 40 and 49 years of age, and a resident of one of the four most populated states: California, Florida, Texas, and New York (see Chart 8 and 9 and Map 3). Alaska, Colorado, and Washington, while having a relatively small number of complaints (ranked 24th, 16th, and 8th respectively), had among the highest per capita rate of complainants in the United States (see Table 3). While most complainants were from the United States, IC3 has also received a number of filings from Canada, the United Kingdom, and Australia (see Map 4).

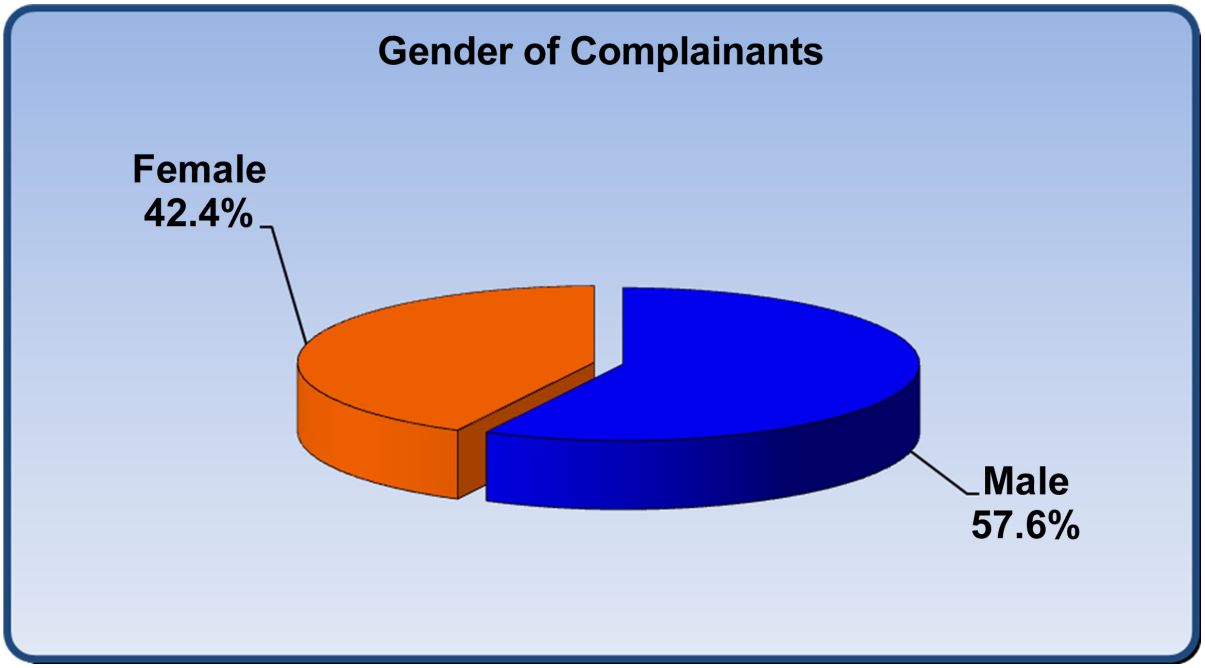


Chart 8

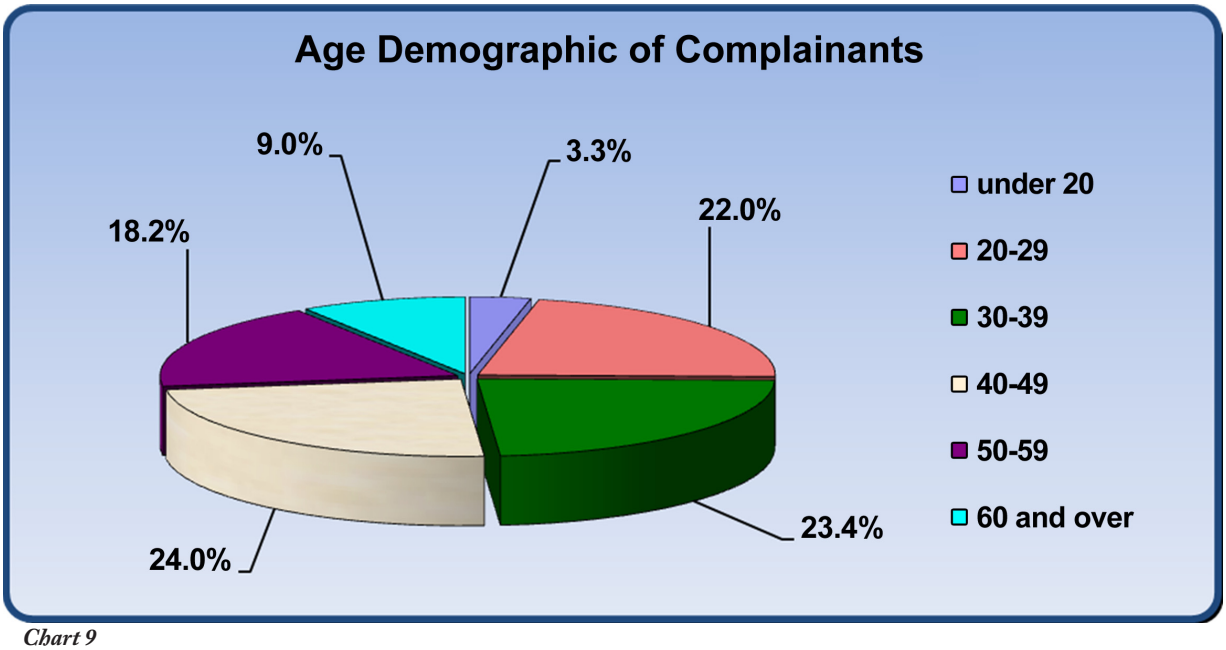
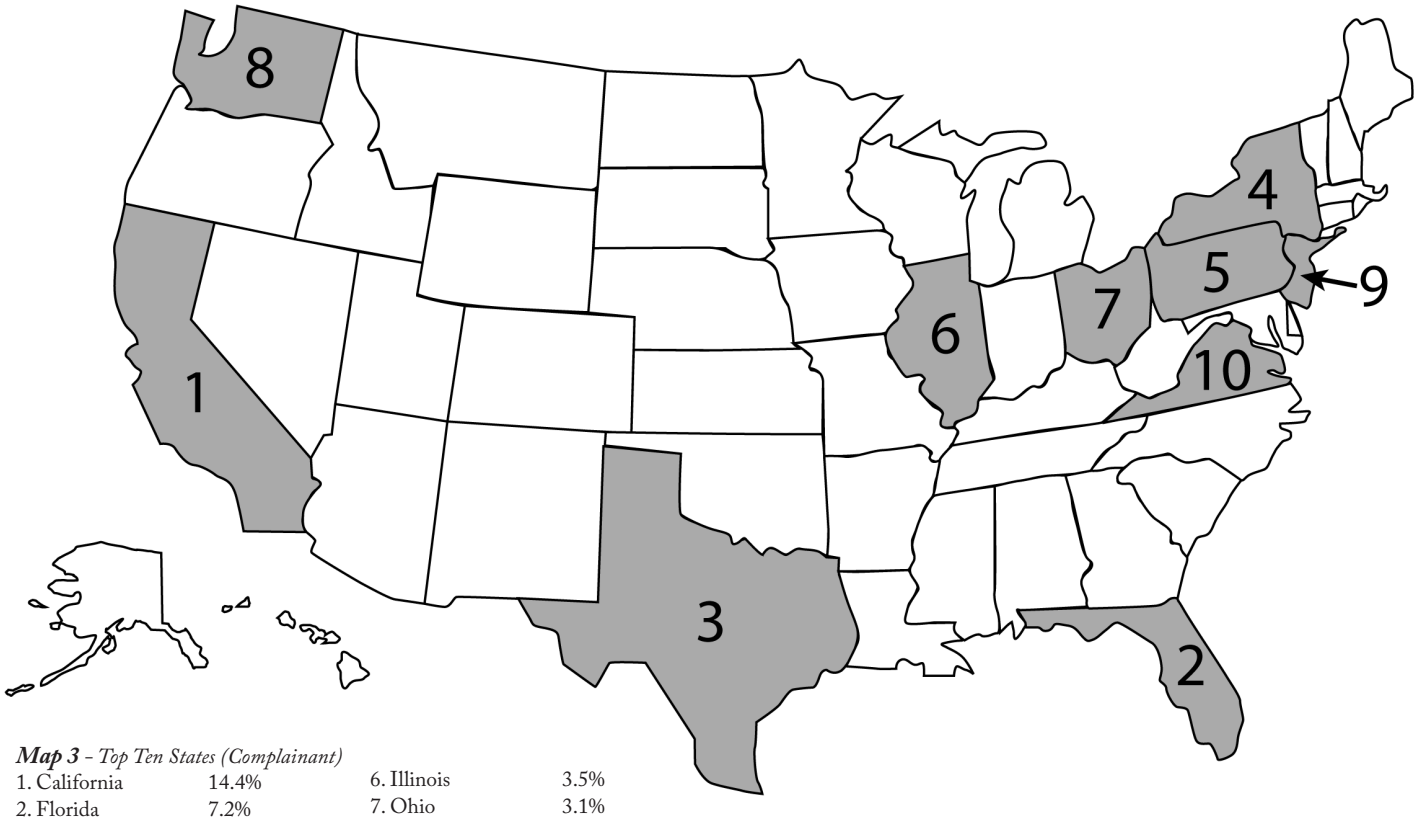


Chart 9

Top Ten States By Count: Individual Complainants



Map 3 *- Top Ten States (Complainant)*

1. California	14.4%	6. Illinois	3.5%
2. Florida	7.2%	7. Ohio	3.1%
3. Texas	7.2%	8. Washington	3.1%
4. New York	5.7%	9. New Jersey	3.1%
5. Pennsylvania	3.6%	10. Virginia	2.9%

Complainants per 100,000 people

Rank	State	Per 100,000 People
1	Alaska	356.41
2	Colorado	90.65
3	Washington	86.76
4	Maryland	83.39
5	Nevada	81.90
6	Oregon	79.41
7	Arizona	78.58
8	District of Columbia	78.19
9	Florida	71.18
10	California	70.87

Table 3 *- based on 2007 Census figures*

Map 4 *- Top Ten Countries (Complainant)*

1. United States	91.9%	6. Mexico	0.18%
2. Canada	2.10%	7. South Africa	0.16%
3. United Kingdom	1.1%	8. Germany	0.14%
4. Austrailia	0.60%	9. France	0.14%
5. India	0.36%	10. Philippines	0.11%

Table 4 compares differences between the dollar loss per incident and the various complainant demographics. Males reported greater dollar losses than females (ratio of $1.67 to every $1.00). Individuals over 60 years of age reported higher or equal amounts of loss than did other age groups.

Amount Lost per Referred Complaint by Selected Complainant Demographics Complainant Demographics	Average (Median) Loss Per Typical Complaint
Male	$765.00
Female	$552.00
Under 20	$384.99
20-29	$610.00
30-39	$699.99
40-49	$760.00
50-59	$750.40
60 and older	$760.00

Table 4

COMPLAINANT-PERPETRATOR DYNAMICS

One of the components of fraud committed via the Internet that makes investigation and prosecution difficult is that the offender and victim may be located anywhere in the world. This is a unique characteristic not found with other types of "traditional" crime. This jurisdictional issue often requires the cooperation of multiple agencies to resolve a given case. Table 5 highlights this truly "borderless" phenomenon. Even in California, where most of the reported fraud cases originated, only 18.3% of all cases involved both a complainant and perpetrator residing in the same state. Other states have an even smaller percentage of complainant-perpetrator proximity in residence. These patterns not only indicate "hot spots" of perpetrators (California for example) that target potential victims from around the world, but also indicate that complainants and perpetrators may not have had a relationship prior to the incident.

Another factor that impedes the investigation and prosecution of Internet crime is the anonymity afforded by the Internet. Although complainants in these cases may report multiple contact methods, few reported interacting face-to-face with the vast majority of perpetrators. Contact with complainants predominantly stemmed from e-mail (73.6%) or a webpage (32.7%) communication. Others reportedly had phone contact (18.0%) with the perpetrator or corresponded through physical mail (10.1%). Interaction through chat rooms (2.3%) and in-person (1.7%) meetings rarely were reported. The anonymous nature of an e-mail address or a website allows perpetrators to solicit a large number of victims with a keystroke (see Chart 10).

Perpetrators from Same State as Complainant

State	Percent	1	2	3
1. California	18.3	(New York 9.1%)	(Florida 8.0%)	(Texas 5.7%)
2. Florida	13.6	(California 13.4%)	(New York 8.1%)	(Texas 5.7%)
3. New York	12.6	(California 12.9%)	(Florida 9.1%)	(Texas 5.9%)
4. Nevada	10.9	(California 14.4%)	(Florida 9.5%)	(New York 9.5%)
5. Texas	10.9	(California 11.7%)	(Florida 9.5%)	(New York 8.9%)
6. Arizona	10.6	(California 12.9%)	(Florida 8.8%)	(New York 8.4%)
7. Illnois	9.2	(California 12.9%)	(Florida 8.9%)	(New York 8.9%)
8. New Mexico	8.8	(California 11.3%)	(Florida 8.3%)	(New York 8.0%)
9. Washington	8.8	(California 13.6%)	(New York 9.3%)	(Florida 8.8%)
10. Tennessee	8.7	(California 12.2%)	(Florida 10.3%)	(New York 9.5%)

Table 5 *- Other top three locations in parentheses*

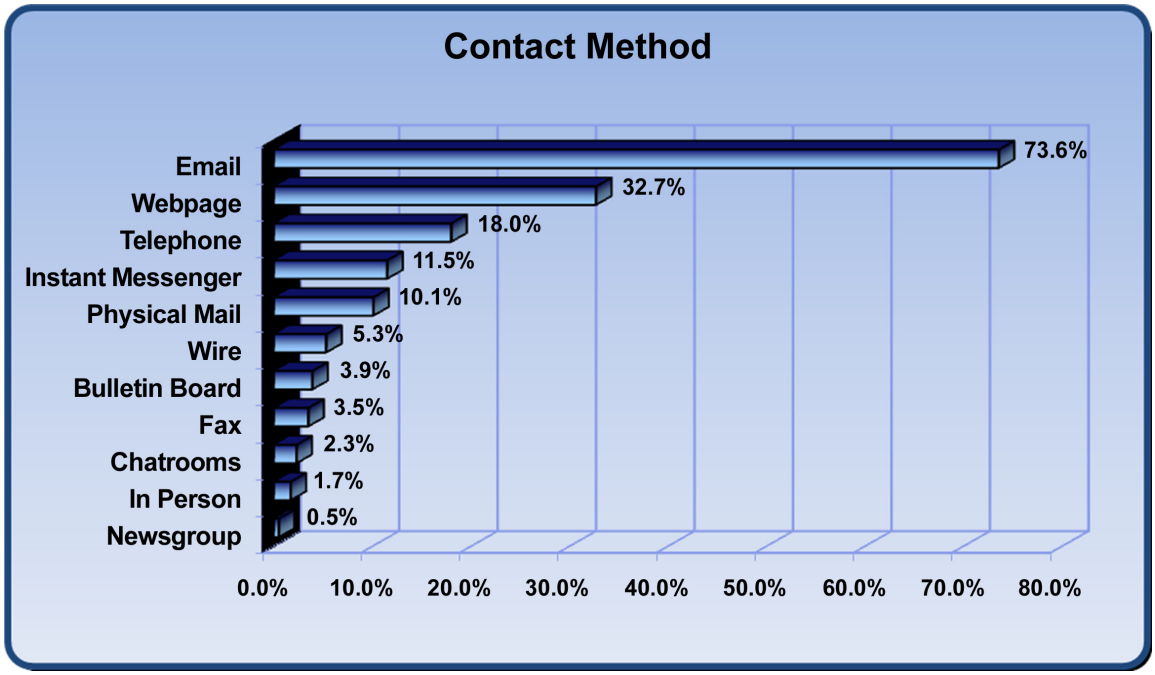


Chart 10

ADDITIONAL INFORMATION ABOUT IC3 REFERRALS

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

For those complaints that are computer-related but not considered Internet fraud, IC3 routinely refers these to agencies and organizations that handle those particular violations. For example, if IC3 receives information related to a threat on the President of the United States, the complaint information is immediately forwarded to PACU (FBI tips) who forwards them to the United States Secret Service. Spam (USSS) complaints and cases of identity theft are forwarded to the Federal Trade Commission (FTC) and referred to other government agencies with jurisdiction. The FTC also receives all other complaints on a monthly basis as well.

SCAMS OF 2007

Among the Internet-facilitated scams commonly reported to the IC3 in 2007 were those involving pets, checks, spam, and online dating sites, all of which have proven effective as criminal devices in the hands of fraudsters. In an effort to raise public awareness, this section describes the basic characteristics of these scams, while highlighting their variations and the ways they often overlap.

Pet Scams

Pet scams can target either buyers or sellers. In pet scams targeting buyers, fraudsters advertise pets for sale in online (or hard copy) publications and agree to sell to buyers. Buyers, in turn, send payment to the fraudsters, often covering delivery costs as well. Then, having parted with their money, the buyers wait for their pets to be delivered; but the pets never arrive.

When pet scams target sellers, the fraudster agrees to buy the pet and sends the seller a bad check (or some other illicit payment instrument) for an amount that exceeds the asking price. When asked about the overpayment, the fraudster explains that the extra money is intended for another person who will be receiving and temporarily caring for the pet. The fraudster then instructs the seller to deposit the check and wire the difference immediately to this other person. If the scam is successful, the seller wires money to the fraudster, and the fraudster makes off with the cash before the bank returns the initial payment as invalid, at which point the seller absorbs the financial loss.

Secret Shopper and Funds Transfer Scams

Another kind of scam involving the use of bad checks is the secret shopper scam. In this scam, victims are led to believe that they have been hired to shop or dine out and to submit evaluations of their consumer experiences. A sequence of financial transactions, similar to the one characterizing seller-targeted pet scams, then follows: Victims receive bad checks, are instructed to deposit them, and then are asked to wire a percentage of the money to a third party, while using the rest of the money to complete their assignments. As in the seller-targeted pet scams, this scam is successful when the fraudster is able to convert the victim's wire transfer into cash before the bank realizes that the initial payment is counterfeit.

In order to give the secret shopper scam the appearance of a legitimate employment opportunity, many fraudsters commit another crime: they misappropriate brand logos and place them on letters or in e-mails containing instructions for "new hires," thus violating U.S. copyright law. For instance, the logos of Wal-Mart, FedEx, Target, McDonalds, Gap, Pepsi, Kmart, and Money Gram all have appeared on such letters. The use of these logos gives the document an official appearance and often is effective in deceiving recipients.

Several variations of this overpayment scam have surfaced in the past year, including one in which people advertise rental properties—particularly apartments and other kinds of residential units In these scams, the fraudster sends the renter an amount of money that exceeds the amount of rent due and instructs the renter to wire the difference to a third party. In a slightly different version of this scam, victims are led to believe that they have been hired by a company to receive payments on the company's behalf and to redistribute funds via wire transfers to other people affiliated with the company (e.g., employees, clients, contact persons, etc.). Here, the same sequence of financial transactions is present, only the hook is not an overpayment; it is the job description itself that requires victims to receive and redistribute money.

Adoption Fraud (Charity Fraud)

Another prevalent scam reported to the IC3 involves the use of unsolicited e-mails, or spam. The specific form taken by this scam varies, but essentially the scam includes e-mails that appeal to the more compassionate and charitable among us, often announcing in the subject field, "URGENT ASSISTANCE IS NEEDED." Such scams are commonly known as "charity frauds."

A charity fraud that came to the IC3's attention in 2007 involved spam where senders claimed to be representatives of the British Association for Adoption and Fostering (BAAF), a legitimate UK-registered charity; however, according to the BAAF, the spammers were not collecting money on the organization's behalf; they were out to defraud people. The content of the spam was generally devoted to explaining the predicament of an orphan or abandoned child and to convince the recipient to file for adoption. The spam then solicited the recipient for money to cover application fees.

Another version of this scam involves a slightly different approach. It casts a much wider net by adding a financial lure. In this version, the spam contains a poignant account of a child whose only parent is about to die due to some incurable illness. Moreover, the dying parent is rich and has promised to leave a small fortune to whoever adopts the child. Here, again, the BAAF is invoked to give the solicitation an air of legitimacy and the recipient is asked to send money for the adoption papers.

Spam, of course, is the preferred instrument in a wide variety of other scams. Perhaps foremost among these scams is the "phishing" expedition that can lead to identity theft. Phishing refers to the practice of eliciting identity information from victims under false pretenses. For instance, the intended victim receives an e-mail that purports to collect personal information on behalf of a financial institution in order to update personal files. Here, again, the misappropriation of a brand logo often is used to give the communication a legitimate appearance. If the phishing is successful, the victim discloses his or her identity information to the fraudster, who, in turn, can sell this information or assume the person's identity while taking out bank loans or applying for credit cards.

Romance Fraud

Online dating and social networking sites also have figured prominently in scams reported to the IC3. Fraudsters use these sites as springboards for meeting people and committing what is commonly known as "romance fraud." Here's how it works: After meeting someone at one of these sites, the fraudster tries to gain a person's trust through false displays of affection. In most cases, the fraudster lives far away, usually in another country. The fraudster expresses an ardent desire to visit the person, but the fraudster cannot afford to make the trip. The scam is successful when the two agree to meet and the fraudster convinces the victim to send money to cover his travel expenses. Then, invariably, an unforeseen event (often an accident of some sort) prevents the fraudster from making the trip (or, at least, so goes the fraudster's lie). The fraudster lands in the hospital, and now the victim's money has to be used to cover medical expenses. The fraudster's brother has been kidnapped, and now the money has to be used to set him free. The fraudster was mugged on her way to the airport, and now she has no money at all. In any event, the fraudster always needs more money; and, if the fraudster's success continues, he is able to obtain more money from the victim while making more promises to visit. The fraudster, however, always has an excuse for missing the plane, and the rounds of false promises and excuses continue until the victim loses patience and stops sending money.

Scam Synopsis

The scams detailed above are just a sample of scams that were frequently reported to the IC3 in 2007. Although in this report we have focused on pets, checks, spam, and online dating sites, we would be remiss to leave the impression that the Internet fraudster's toolbox is limited to these devices. The Internet presents fraudsters with myriad opportunities to multiply the devices at their disposal. Some fraudsters, as we have seen, have even used the reputations of charitable organizations to exploit the most benevolent of human impulses.

Perhaps the best way to guard against Internet-facilitated scams is to simply stay informed. Keeping informed of the latest scams on the Internet may enable Internet users to recognize and report these scams instead of losing money in one of them. To learn about the new scams, we recommend periodically checking the FBI, and IC3 and lookstoogoodtobetrue.com websites for the latest updates.

RESULTS OF IC3 REFERRALS

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

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

- The Colorado Attorney General's Office announced they have reached a $40,000 out-of-court settlement with Uzed Enterprises and their company president, Steve Bonneau. The company, which has been the subject of more than a hundred complaints filed with the IC3 in the past two years, operated the Uzed.com website. The site solicited consumers to send their used CDs, DVDs, video games and electronics to the Broomfield-based business in exchange for an advertised payment. The Colorado Attorney General's Office received more than 200 complaints from the Better Business Bureau and the IC3 when the company failed to pay consumers in a timely fashion. Some consumers stated they had not been paid at all.
- Prior to the settlement, Consumer Protection Intake Manager Nancy Bullis, contacted the IC3 and requested a search of the complaint database to identify as many victims as possible. This search uncovered 127 consumers who had filed against the site with the IC3. The settlement requires Uzed and Bonneau to pay back nearly $40,000 to more than 400 consumers across the country. In addition, the company and Bonneau are barred from operating any business in Colorado in which they are responsible for paying consumers, unless a bond is in place.
- Two Houston, TX men have been found guilty of setting up a bogus Salvation Army website that collected more than $48,000 in the name of Hurricane Katrina relief. Brothers Steven and Bartholomew Stephens set up the site in September 2005, which collected money via PayPal, in September 2005, but it had no affiliation with the Salvation Army. According to testimony from FBI Analyst Tony Yurkovich (assigned to IC3), the site featured icons associated with the Christian organization including the red shield and kettle. The brothers used other people's identities to set up the PayPal accounts, but had the money sent to their bank accounts. The brothers had a dozen bank accounts, six of which received hurricane relief donations. The accounts were frozen after fraud reports were made.

The brothers were found guilty on nine counts of conspiracy, wire fraud, and aggravated identity theft. They face up to twenty years in prison and fines up to $250,000.

- The New Jersey Attorney General reports that John G. Messina was sentenced to three years in state prison and restitution of $35,500 for perpetrating an online fraud and check kiting scheme. Messina advertised online at vFinance.com, claiming that he could obtain investors and investment capital for businesses. He subsequently took $14,900 from victims while promising to either secure money from investors for the client or to release funds that he had already raised for the client; he never obtained investors or raised money for the victims. Messina also was ordered to pay $20,600 to Bank of America for check kiting wherein he deposited this amount into his mother's Bank of America account using fraudulent checks, withdrawing the money before the check had time to bounce.
- Four defendants have been arraigned in Atlanta, Georgia on Internet fraud charges. Jonathan Rembert, Dwayne Barrow, Clarence Shelton, and Andwele Butler, along with three others, face federal wire fraud and conspiracy to commit wire fraud charges related to an eBay fraud ring. The charges state that the defendants used eBay auctions to sell custom car tires and rims as well as vehicles. Interested customers negotiated a price with the defendants and payment was made via wire transfer or Western Union; it is alleged that the merchandise was never sent to the victims. From July 2003 to October 2006, 215 individuals paid the defendants approximately $539,000 for non-existent merchandise. This case is currently being investigated by the FBI and is being prosecuted by the United State's Attorneys Office for the Northern District of Georgia.
- In February of 2007, the United States Attorney's Office for the Southern District of Florida announced that three defendants, Steven Michael May, Jr., Christopher William Cook, and Joseph John Vaquera, pled guilty to mail fraud charges in a $2 million scheme to defraud retail businesses throughout the United States. The defendants used false and fraudulent financial information to establish business-to-business lines of credit with over 30 businesses. This credit then was used to obtain assorted high-end merchandise (including computer monitors, flat-screen televisions, DVD camcorders, electronic equipment and cameras). The merchandise was shipped to various commercial mailboxes or virtual business offices (set up by the defendants) across the United States. Once merchandise was received at the mailbox or virtual office, the defendants would have the merchandise re-shipped to a different commercial mailbox, virtual office, or storage facility located in Palm Beach County. The defendants subsequently sold the high-end merchandise through eBay auctions for a profit.
- Terrance J. Holmes of Vermillion, Ohio was sentenced to 37 months in prison and three years of supervised release for wire fraud charges. Holmes owned and operated GPS Computer Services from January 2001 to February 2002. The company offered various laptop and notebook computers for sale via an Internet website for the company and through eBay auctions. The computers, retailing for $1,100 to $1,600 each, were sold for $400 to $700. Orders were accepted from at least 1,187 customers via Internet, phone, and in-person, with sales totaling approximately $964,560. The merchandise, however, was not delivered. In addition to prison time, Holmes has also been ordered to pay restitution to the victims in the amount of $867,340.09.

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

CONCLUSION

The IC3 report has outlined many of the current trends and patterns in Internet crime. The data indicates that fraud is increasing; however, reported complaints remained relatively level with 206,884 complaints in 2007, down from 207,492 complaints in 2006, 231,493 complaints in 2005, and 207,449 complaints in 2004. This total includes many different fraud types, non-fraudulent complaints, as well as complaints of other types of crime. Yet, research indicates that only one in seven incidents of fraud ever make their way to the attention of enforcement or regulatory agencies. [1] The total dollar loss from all referred cases of fraud was $239.09 million in 2007 up from $198.44 million in 2006.

Internet auction fraud again was the most reported offense followed by non-delivered merchandise/payment and confidence fraud. Among those individuals who reported a dollar loss from the fraud, the highest median dollar losses were found among investment fraud victims ($3,547), check fraud victims ($3,000), and Nigerian letter fraud victims ($1,922). Male complainants reported greater losses than female complainants, which may be a function of both online purchasing differences by gender and the type of fraud. Comparing data from the 2006 and the 2007 reports, e-mail and web pages were still the two primary mechanisms by which the fraudulent contact took place.

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

Over the two years, the IC3 has begun to update/change its method of gathering data regarding complaints, in recognition of the constantly changing nature of cybercrime and to more accurately reflect meaningful trends. With this in mind, changes to the IC3 website and complaint form have been implemented, with many of those changes taking effect as of January, 2006. Along with these changes, the IC3 and its partners continue to host a public website, ***www.lookstoogoodtobetrue.com***, which educates consumers with various consumer alerts, tips, and description of fraud trends.

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

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

Whether a consumer has become a victim of a bogus investment offer, a dishonest auction seller, or a host of other Internet crimes, the IC3 is in the position to offer assistance. Through the online complaint and referral process, victims of Internet crime are provided with an easy way to alert authorities, at many different jurisdictional levels, of a suspected criminal or civil violation.

2 Appendix - 1

Explanation of Complaint Terms

IC3 Internet Fraud Analysts determined a fraud type for each Internet fraud complaint received and sorted complaints into fraud and crime categories. Below are the definitions for the categories and terms used within this report:

- Financial Institution Fraud - Knowing misrepresentation of the truth or concealment of a material fact by a person to induce a business, organization, or other entity that manages money, credit, or capital to perform a fraudulent activity.[2] Credit/debit card fraud is an example that ranks among the most commonly reported offenses to IC3. Identity theft also falls into this category; cases classified under this heading tend to be those where the perpetrator possesses the complainant's true name identification (in the form of a social security card, driver's license, or birth certificate), but there has not been a credit or debit card fraud committed.
- Gaming Fraud - To risk something of value, especially money, for a chance to win a prize when there is a misrepresentation of the odds or events.[3] Sports tampering and claiming false bets are two examples of gaming fraud.
- Communications Fraud - A fraudulent act or process in which information is exchanged using different forms of media. Thefts of wireless, satellite, or landline services are examples of communications fraud.
- Utility Fraud - When an individual or company misrepresents or knowingly intends to harm by defrauding a government regulated entity that performs an essential public service, such as the supply of water or electrical services.[4]
- Insurance Fraud - A misrepresentation by the provider or the insured in the indemnity against loss. Insurance fraud includes the "padding" or inflating of actual claims, misrepresenting facts on an insurance application, submitting claims for injuries or damage that never occurred, and "staging" accidents.[5]
- Government Fraud - A knowing misrepresentation of the truth, or concealment of a material fact to induce the government to act to its own detriment. Examples of government fraud include tax evasion, welfare fraud, and counterfeit currency.
- Investment Fraud - Deceptive practices involving the use of capital to create more money, either through income-producing vehicles or through more risk-oriented ventures designed to result in capital gains.[7] Ponzi/Pyramid schemes and market manipulation are two types of investment fraud.
- Business Fraud - When a corporation or business knowingly misrepresents the truth or conceals a material fact.[8] Examples of business fraud include bankruptcy fraud and copyright infringement.
- Confidence Fraud - The reliance on another's discretion and/or a breach in a relationship of trust resulting in financial loss. A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.[9] Auction fraud and non-delivery of payment or merchandise are both types of confidence fraud and are the most reported offenses to IC3. The Nigerian letter scam is another offense classified under confidence fraud.
- Credit/Debit Card Fraud – Any t unauthorized use of a credit card with the purpose of obtaining anything of value with the intent to defraud.
- Check Fraud - The forgery, alteration, counterfeiting, or knowing issuance of a check on an account that has been closed or has insufficient funds to cover the amount for which the check was written.
- Computer Fraud - In the broadest sense, computer crime is a violation of law involving a computer. As defined by the U.S. General Accounting Office, Office of Special Investigations, computers can be "used as tools to commit traditional offenses." This means that the functions specific to computers, such as software programs and Internet capabilities, can be manipulated to conduct criminal activity. This broad category of crime is often discussed in terms of two subcategories: "true" computer crime and computer-related crime. "True" computer crime refers to those crimes that target the content of computer operating systems, programs, or networks.
- Identity Theft -Simply put, identity theft is the illegal use of another person's identifying information (such as a name, birth date, social security and/or credit card number), and it is one of the fastest growing crimes in the United States.

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

- Nigerian Letter Fraud – Any scam that involves an unsolicited email message, purportedly from Nigeria or another African nation, in which the sender promises a large sum of money to the recipient. In return the recipient is asked to pay an advance fee or provide identity, credit card or bank account information. Subsequently, the recipient loses all monies they have entrusted to the sender of the message and they get nothing in return.

2 Appendix - 2

Best Practices to Prevent Internet Crime

Internet Auction Fraud Prevention tips:

- Understand as much as possible about how Internet auctions work, what your obligations are as a buyer, and what the seller's obligations are before you bid.
- Find out what actions the website takes if a problem occurs and consider insuring the transaction and shipment.
- Do not allow the seller or buyer to convince you to ignore the rules of a legitimate Internet auction website or exit the auction website to complete a transaction.
- Be cautious of second chance offers especially unsolicited email offers where you are contacted after an auction is listed as closed, or the item is listed as sold, with an offer to purchase the listed item allegedly because the original buyer backed out of a sale. Many times these second chance offers are fraudulent.
- Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.
- Examine the feedback on the seller and use common sense. If the seller has a history of negative feedback, then do not deal with that particular seller.
- Determine what method of payment the seller is asking for and where he/she is asking to send payment. Use caution when the mailing address is a post office box number.
- Be aware of the difference in laws governing auctions between the U.S. and other countries. If a problem occurs with the auction transaction that has the seller in one country and a buyer in another, it might result in a dubious outcome leaving you empty handed.
- Be sure to ask the seller about when delivery can be expected and warranty/exchange information for merchandise that you might want to return.
- To avoid unexpected costs, find out if shipping and delivery are included in the auction price or are additional.
- Avoid giving out your social security number or driver's license number to the seller, as the sellers have no need for this information.
- Finally, practice an attitude of healthy skepticism. If something sounds too good to be true, it usually is.

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 90 days after the listing end-date at (***http://crs.ebay.com/aw-cgi/ebayisapi.dll?crsstartpage***).
2. File a complaint with the Internet Crime Complaint Center (***http://www.ic3.gov***).
3. Contact law enforcement officials at the local and state level (your local and state police departments).
4. Also contact law enforcement officials in the perpetrator's town and state.
5. File a complaint with the shipper USPS, UPS, Fed-Ex, etc.
6. File a complaint with the National Fraud Information Center (***http://www.fraud.org/info/contactnfic.htm***).
7. File a complaint with the Better Business Bureau (***http://www.bbb.org***).

Non-Delivery of Merchandise

Prevention tips:

- Make sure you are purchasing merchandise from a reputable source. As with auction fraud, check the reputation of the seller whenever possible, including the Better Business Bureau.
- Try to obtain a physical address rather than merely a post office box and a phone number. Also, call the seller to see if the number is correct and working.
- Send them e-mail to see if they have an active e-mail address. Be cautious of sellers who use free e-mail services where a credit card was not required to open the account.
- Investigate other websites regarding this person/company.
- Do not judge a person/company by their fancy website; thoroughly check out the person/company out.
- Be cautious when responding to special offers (especially through unsolicited e-mail).
- Be cautious when dealing with individuals/companies from outside your own country. Remember the laws of different countries might pose issues if a problem arises with your transaction.
- Inquire about returns and warranties on all items.
- The safest way to purchase items via the Internet is by credit card because you can often dispute the charges if something is wrong. Also, consider utilizing an escrow

or alternate payment service, after conducting thorough research on the escrow service. Many times fraudsters want victims to pay using wire transfers because they can collect and move the victim's money before the victim learns of the fraud.

- Make sure the website is secure when you electronically send your credit card numbers.

Credit Card Fraud

Prevention tips:

- Don't give out your credit card number(s) online unless the website is both secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but may provide you some assurance.
- Before using a site, check out the security software it uses to make sure that your information will be protected.
- Make sure you are purchasing merchandise from a reputable/legitimate source. Once again investigate the person or company before purchasing any products.
- Try to obtain a physical address rather than merely a post office box and a phone number. Call the seller to see if the number is correct and working.
- Send them e-mail to see if they have an active e-mail address and be wary of sellers who use free e-mail services where a credit card was not required to open the account.
- Do not purchase from sellers who refuse to provide you with verifiable contact information.
- Check with the Better Business Bureau to see if there have been any prior complaints against the seller.
- Check out other websites regarding this person/company.
- Be cautious when responding to special offers (especially through unsolicited e-mail).
- Be cautious when dealing with individuals/companies from outside your own country.
- If you are going to purchase an item via the Internet, use a credit card since you can often dispute the charges if something does go wrong.
- Make sure the transaction is secure when you electronically send your credit card numbers.
- You should also keep a list of all your credit cards and account information along with the card issuer's contact information. If anything looks suspicious or you lose your credit card(s), contact the card issuer immediately.

Prevention tips for Businesses:

- Do not accept orders unless complete information is provided (including full address and phone number). Require address verification for all of your credit card orders. Require anyone who uses a different shipping address than their billing address to send a fax with their signature and credit card number authorizing the transaction.
- Be especially careful with orders that come from free e-mail services— there is a much higher incidence of fraud from these services. Many businesses won't even accept orders that come through these free e-mail accounts anymore. Send an e-mail requesting additional information before you process the order asking for: a non-free e-mail address, the name and phone number of the bank that issued the credit card, the exact name on credit card, and the exact billing address.
- Be wary of orders that are larger than your typical order amount and orders with next day delivery.
- Be cautious of buyers who use numerous credit cards to pay for a single order, especially if the order is unusual in nature or size. Check all the credit cards to verify that they all belong to the same person or business.
- Pay extra attention to international orders. Validate the order before you ship your product to a different country.
- If you are suspicious, pick up the phone and call the customer to confirm the order.
- Consider using software or services to fight credit card fraud online.
- If defrauded by a credit card thief, you should contact your bank and the authorities.

Investment Fraud

Prevention tips:

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

Nigerian Letter Scam/419 Scam

Prevention tips:

- Be skeptical of individuals representing themselves as Nigerian or other foreign government officials asking for your help in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- Do not give out any personal identifying information regarding your savings, checking, credit, or other financial accounts.
- If you are solicited, do not respond and quickly notify the appropriate authorities.

Business Fraud

Prevention tips:

- Purchase merchandise from reputable dealers or establishments.
- Try to obtain a physical address rather than merely a post office box and a phone number, and call the seller to see if the number is correct and working.
- Send them e-mail to see if they have an active e-mail address and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Do not purchase from sellers who won't provide you with this type of information.
- Purchase merchandise directly from the individual/company that holds the trademark, copyright, or patent. Be aware of counterfeit and look-alike items.
- Beware when responding to e-mail that may not have been sent by a reputable company. Always investigate before purchasing any products.

Identity Theft

Prevention tips:

- Check your credit reports once a year from all three of the credit reporting agencies (Experian, Transunion, and Equifax).
- Guard your Social Security number. When possible, don't carry your Social Security card with you.
- Don't put your Social Security Number or driver's license number on your checks.
- Guard your personal information. You should never give your Social Security number to anyone unless you can verify that they are required to collect it.
- Carefully destroy papers you discard, especially those with sensitive or identifying information such as bank account and credit card statements.
- Be suspicious of telephone solicitors. Never provide information unless you have initiated the call.
- Delete any suspicious e-mail requests without replying. Remember: If your bank or credit card company needs you to contact them, they have telephone numbers and website information on your statement. You do not have to click on unsolicited emails to contact them.

Steps to take if victimized:

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

Cyberstalking

Prevention tips (from W.H.O.A – Working to Halt Online Abuse at ***www.haltabuse.org***):

- Use a gender-neutral user name/e-mail address.
- Use a free e-mail account such as Hotmail (***www.hotmail.com***) or YAHOO! (***www.yahoo.com***) for newsgroups/mailing lists, chat rooms, Instant messages (IMs), e-mails from strangers, message boards, filling out forms, and other online activities.
- Don't give your primary e-mail address to anyone you do not know or trust.
- Instruct children to never give out their real name, age, address, or phone number over the Internet without your permission.
- Don't provide your credit card number or other information as proof of age to access or subscribe to a website with which you are not familiar with.
- Monitor/observe newsgroups, mailing lists, and chat rooms before "speaking" or posting messages.
- When you do participate online, be careful – only type what you would say to someone's face.
- Don't be so trusting online – don't reveal personal things about yourself until you really and truly know the other person.
- Your first instinct may be to defend yourself – Don't – this is how most online harassment situations begin.
- If it looks too good to be true – it is.

2 Appendix - 3

Complainant/Perpetrator Statistics, by State

Complainants by State

Rank	State	Percent	Rank	State	Percent
1	California	14.4	27	South Carolina	1.2
2	Florida	7.2	28	Louisiana	1.1
3	Texas	7.2	29	Connecticut	1.0
4	New York	5.7	30	Kentucky	1.0
5	Pennsylvania	3.6	31	Utah	1.0
6	Illinois	3.5	32	Oklahoma	0.9
7	Ohio	3.1	33	Kansas	0.8
8	Washington	3.1	34	Arkansas	0.8
9	New Jersey	3.1	35	Iowa	0.7
10	Virginia	2.9	36	New Mexico	0.6
11	Michigan	2.8	37	Idaho	0.5
12	Arizona	2.8	38	Mississippi	0.5
13	Georgia	2.6	39	West Virginia	0.5
14	Maryland	2.6	40	New Hampshire	0.5
15	North Carolina	2.6	41	Hawaii	0.5
16	Colorado	2.5	42	Nebraska	0.4
17	Indiana	2.0	43	Maine	0.4
18	Massachusetts	2.0	44	Montana	0.3
19	Missouri	1.9	45	Rhode Island	0.3
20	Tennessee	1.8	46	District of Columbia	0.3
21	Oregon	1.7	47	Delaware	0.3
22	Wisconsin	1.6	48	Vermont	0.2
23	Minnesota	1.6	49	Wyoming	0.2
24	Alaska	1.4	50	South Dakota	0.2
25	Alabama	1.2	51	North Dakota	0.1
26	Nevada	1.2			

Table 6 *- Represents Percentage of total individual complainants within the United States where state is known*

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

Complainant/Perpetrator Statistics, by State (Continued)

Perpetrators by State

Rank	State	Percent	Rank	State	Percent
1	California	15.8	27	Connecticut	1.0
2	Florida	10.1	28	Kentucky	1.0
3	New York	9.9	29	South Carolina	0.9
4	Texas	7.0	30	Oklahoma	0.8
5	Illinois	3.6	31	District of Columbia	0.8
6	Pennsylvania	3.5	32	Louisiana	0.7
7	Georgia	3.1	33	Kansas	0.7
8	Ohio	2.8	34	Maine	0.5
9	Washington	2.8	35	Iowa	0.5
10	New Jersey	2.8	36	Nebraska	0.5
11	Michigan	2.5	37	Arkansas	0.5
12	Arizona	2.4	38	Delaware	0.5
13	Nevada	2.3	39	New Hampshire	0.4
14	North Carolina	2.0	40	Rhode Island	0.4
15	Virginia	1.9	41	New Mexico	0.4
16	Indiana	1.7	42	Mississippi	0.4
17	Colorado	1.7	43	Idaho	0.3
18	Maryland	1.7	44	West Virginia	0.3
19	Massachusetts	1.6	45	Montana	0.3
20	Missouri	1.5	46	Hawaii	0.3
21	Tennessee	1.4	47	Alaska	0.3
22	Utah	1.3	48	Wyoming	0.2
23	Wisconsin	1.2	49	Vermont	0.2
24	Minnesota	1.2	50	South Dakota	0.2
25	Alabama	1.2	51	North Dakota	0.1
26	Oregon	1.1			

Table 7 *- Represents percentage of total individual perpetrators within the United States (where state is known)*

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

Complainant/Perpetrator Statistics, by State (Continued)

Complainants per 100,000 people

Rank	State	Per 1,000	Rank	State	Per 1,000
1	Alaska	356.41	27	Connecticut	53.48
2	Colorado	90.65	28	Minnesota	53.35
3	Washington	86.76	29	New York	52.74
4	Maryland	83.39	30	Pennsylvania	52.23
5	Nevada	81.90	31	Tennessee	51.11
6	Oregon	79.41	32	Kansas	51.08
7	Arizona	78.58	33	North Carolina	51.04
8	District of Columbia	78.19	34	Delaware	50.88
9	Florida	71.18	35	Rhode Island	50.58
10	California	70.87	36	West Virginia	50.39
11	Virginia	68.33	37	Wisconsin	49.81
12	Utah	66.46	38	Michigan	49.71
13	New Hampshire	65.66	39	Georgia	49.36
14	Wyoming	65.03	40	Illinois	48.35
15	New Jersey	63.94	41	Arkansas	47.76
16	Idaho	63.23	42	South Carolina	47.55
17	Hawaii	63.11	43	Alabama	46.50
18	Ohio	62.24	44	Louisiana	45.91
19	Montana	59.51	45	Nebraska	44.01
20	Vermont	58.02	46	Oklahoma	43.04
21	Missouri	57.60	47	Kentucky	42.86
22	Maine	56.10	48	Iowa	42.76
23	Indiana	55.33	49	South Dakota	37.30
24	Massachusetts	54.25	50	North Dakota	35.17
25	Texas	54.04	51	Mississippi	32.10
26	New Mexico	53.56			

Table 8 *- based on 2007 Census figures*

Complainant/Perpetrator Statistics, by State (Continued)

Perpetrators per 100,000 people

Rank	State	Per 1,000	Rank	State	Per 1,000
1	District of Columbia	99.10	27	Massachusetts	19.66
2	Nevada	65.45	28	Missouri	19.24
3	Delaware	41.98	29	Indiana	19.05
4	Florida	40.73	30	Alabama	18.99
5	New York	38.06	31	Hawaii	18.86
6	Utah	36.40	32	Virginia	18.45
7	Washington	31.96	33	Kansas	18.19
8	California	31.87	34	Michigan	18.12
9	Alaska	28.53	35	Ohio	18.09
10	Rhode Island	28.45	36	Tennessee	17.25
11	Arizona	27.99	37	Kentucky	17.23
12	Maine	27.63	38	Minnesota	16.95
13	Colorado	25.84	39	North Carolina	16.54
14	Montana	25.16	40	South Carolina	15.79
15	Georgia	24.25	41	Oklahoma	15.79
16	New Jersey	23.44	42	Idaho	15.67
17	Vermont	22.86	43	Wisconsin	15.37
18	Maryland	21.64	44	North Dakota	15.16
19	Texas	21.53	45	New Mexico	14.67
20	Oregon	21.43	46	South Dakota	13.56
21	Pennsylvania	20.94	47	Arkansas	11.92
22	New Hampshire	20.90	48	West Virginia	11.92
23	Wyoming	20.85	49	Louisiana	11.67
24	Illinois	20.70	50	Iowa	11.58
25	Connecticut	20.39	51	Mississippi	8.77
26	Nebraska	20.17			

Table 9 *- based on 2007 Census figures*

1. *Electronic Law Enforcement: Introduction to Investigations in an Electronic Environment. (2001). Washington, DC: U.S. General Accounting Office, Office of Special Investigations.*

NW3C
NATIONAL WHITE COLLAR CRIME CENTER
INTEGRITY QUALITY SERVICE

BJA Bureau of Justice Assistance

THIS PROJECT WAS SUPPORTED BY GRANT NO. 2007-WC-CX-K001 AWARDED BY THE BUREAU OF JUSTICE ASSISTANCE. THE BUREAU OF JUSTICE ASSISTANCE IS A COMPONENT OF THE OFFICE OF JUSTICE PROGRAMS, WHICH ALSO INCLUDES THE BUREAU OF JUSTICE STATISTICS, THE NATIONAL INSTITUTE OF JUSTICE, THE OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION, AND THE OFFICE FOR VICTIMS OF CRIME. POINTS OF VIEW OR OPINIONS IN THIS DOCUMENT ARE THOSE OF THE AUTHOR AND DO NOT REPRESENT THE OFFICIAL POSITION OR POLICIES OF THE UNITED STATES DEPARTMENT OF JUSTICE.THIS PROJECT WAS SUPPORTED BY GRANT NO. 2007-WC-CX-K001 AWARDED BY THE BUREAU OF JUSTICE ASSISTANCE. THE BUREAU OF JUSTICE ASSISTANCE IS A COMPONENT OF THE OFFICE OF JUSTICE PROGRAMS, WHICH ALSO INCLUDES THE BUREAU OF JUSTICE STATISTICS, THE NATIONAL INSTITUTE OF JUSTICE, THE OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION, AND THE OFFICE FOR VICTIMS OF CRIME. POINTS OF VIEW OR OPINIONS IN THIS DOCUMENT ARE THOSE OF THE AUTHOR AND DO NOT REPRESENT THE OFFICIAL POSITION OR POLICIES OF THE UNITED STATES DEPARTMENT OF JUSTICE.THIS PROJECT WAS SUPPORTED BY GRANT NO. 2007-WC-CX-K001 AWARDED BY THE BUREAU OF JUSTICE ASSISTANCE. THE BUREAU OF JUSTICE ASSISTANCE IS A COMPONENT OF THE OFFICE OF JUSTICE PROGRAMS, WHICH ALSO INCLUDES THE BUREAU OF JUSTICE STATISTICS, THE NATIONAL INSTITUTE OF JUSTICE, THE OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION, AND THE OFFICE FOR VICTIMS OF CRIME. POINTS OF VIEW OR OPINIONS IN THIS DOCUMENT ARE THOSE OF THE AUTHOR AND DO NOT REPRESENT THE OFFICIAL POSITION OR POLICIES OF THE UNITED STATES DEPARTMENT OF JUSTICE.PROJECT WAS SUPPORTED BY GRANT NO. 2007-WC-CX-K001 AWARDED BY THE BUREAU OF JUSTICE ASSISTANCE. THE BUREAU OF JUSTICE ASSISTANCE IS A COMPONENT OF THE OFFICE OF JUSTICE PROGRAMS, WHICH ALSO INCLUDES THE BUREAU OF JUSTICE STATISTICS, THE NATIONAL INSTITUTE OF JUSTICE, THE OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION, AND THE OFFICE FOR VICTIMS OF CRIME. POINTS OF VIEW OR OPINIONS IN THIS DOCUMENT ARE THOSE OF THE AUTHOR AND DO NOT REPRESENT THE OFFICIAL POSITION OR POLICIES OF THE UNITED STATES DEPARTMENT OF JUSTICE.