2008 Internet Crime Report

INTERNET CRIME COMPLAINT CENTER

NW3C
NATIONAL WHITE COLLAR CRIME CENTER
INTEGRITY QUALITY SERVICE

BJA Bureau of Justice Assistance

Table of Contents

2008 Internet Crime Report	1
Executive Summary	1
Overview	2
General IC3 Filing Information	2
Complaint Characteristics	4
Perpetrator Characteristics	6
Complainant Characteristics	8
Complainant - Perpetrator Dynamics	10
Additional Information About IC3 Referrals	11
Scams of 2008	11
Scam Synopsis	12
Results of IC3 Referrals	12
IC3 Capabilities	14
Conclusion	14
Appendix 1: Explanation of Complaint Categories	16
Appendix 2: Best Practices to Prevent Internet Fraud	17
Appendix 3: References	21
Appendix 4: Complainant/Perpetrator Statistics, by State	22

Tables/Charts/Maps

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

This project was supported by Grant No. 2008-CE-CX-0001 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 publication are those of the author and do not represent the official position or policies of the United States Department of Justice. This publication is also available for download in PDF format at ***www.nw3c.org***.

2008 Internet Crime Report

Executive Summary

In December 2003, the Internet Fraud Complaint Center (IFCC) was renamed the Internet Crime Complaint Center (IC3) to better reflect the broad character of such criminal matters having a cyber (Internet) nexus. The 2008 Internet Crime Report is the eighth annual compilation of information on complaints received and referred by the IC3 to law enforcement or regulatory agencies for appropriate action. From January 1, 2008 – December 31, 2008, the IC3 website received 275,284 complaint submissions. This is a (33.1%) increase when compared to 2007 when 206,884 complaints were received. These filings were composed of complaints primarily related to fraudulent and non-fraudulent issues on the Internet.

These complaints were composed of many different fraud types such as auction fraud, non-delivery, and credit/debit card fraud as well as non-fraudulent complaints such as computer intrusions, spam/unsolicited e-mail, and child pornography. All of these complaints are accessible to federal, state, and local law enforcement to support active investigations, trend analysis, and public outreach and awareness efforts.

From the submissions, IC3 referred 72,940 complaints of crime to federal, state, and local law enforcement agencies around the country for further consideration. The vast majority of cases were fraudulent in nature and involved a financial loss on the part of the complainant. The total dollar loss from all referred cases of fraud was $264.6 million with a median dollar loss of $931.00 per complaint. This is up from $239.1 million in total reported losses in 2007. Other significant findings related to an analysis of referrals include:

- Non-delivered merchandise and/or payment was, by far, the most reported offense, comprising 32.9% of referred complaints. Internet auction fraud accounted for 25.5% of referred complaints. Credit/debit card fraud made up 9.0% of referred complaints. Confidence fraud, computer fraud, check fraud, and Nigerian letter fraud round out the top seven categories of complaints referred to law enforcement during the year.
- Of those complaints reporting a dollar loss, the highest median losses were found among check fraud ($3,000), confidence fraud ($2,000), Nigerian (west African, 419, Advance Fee) letter fraud ($1,650).
- Among perpetrators, 77.4% were male and half resided in one of the following states: California, New York, Florida, Texas, District of Columbia, and Washington. The majority of reported perpetrators (66.1%) were from the United States; however, a significant number of perpetrators where also located in the United Kingdom , Nigeria , Canada , China, and South Africa.
- Among complainants, 55.4% 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 (92.4%), IC3 received a number of complaints from Canada, United Kingdom, Australia, India, and France.
- Males lost more money than females (ratio of $1.69 dollars lost per male to every $1.00 dollar lost per female). This may be a function of both online purchasing differences by gender and the type of fraudulent schemes by which the individuals were victimized.
- E-mail (74.0%) and webpages (28.9%) were the two primary mechanisms by which the fraudulent contact took place.

This report provides 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. 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); however, 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.

Overview

The Internet Crime Complaint Center (IC3), which began operation on May 8, 2000, as the Internet Fraud Complaint Center was established as a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI) to serve as a vehicle to receive, process, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. IC3 was intended for and continues to serve 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 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 levels, 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 2008 the IC3 saw an increase in several additional crimes that are exclusively related to the Internet, which include phishing, spoofing, and spam complaints, and have increased over the past year.

Overall, the "IC3 2008 Internet Crime Report" is the eighth annual compilation of information on complaints received and referred by IC3 to law enforcement or regulatory agencies for appropriate action. The results provide an examination of key characteristics of 1) complaints, 2) perpetrators, 3) complainants, 4) interaction between perpetrators and complainants, and 5) success stories involving complaints referred by IC3. The results in this report are intended to enhance our general knowledge about the scope and prevalence of Internet crime in the United States. This report does not represent all victims of Internet crime, or fraud in general, because it is derived solely from the people who filed a report with IC3.

General IC3 Filing Information

Internet crime complaints are primarily submitted to IC3 online at www.ic3.gov. 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, 2008 – December 31, 2008, there were 275,284 complaints filed online with IC3. This is a 33.1% increase compared to 2007 when 206,884 complaints were received (See Chart 1). The number of complaints filed per month, last year, averaged 22,940 (See Chart 2). Dollar loss of referred complaints was at an all time high in 2008, $264.59 million, compared to previous years (See Chart 3).

The number of referred complaints has decreased from 90,008 in 2007 to 72,940 in 2008 (See Chart 4). The 129,349 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.

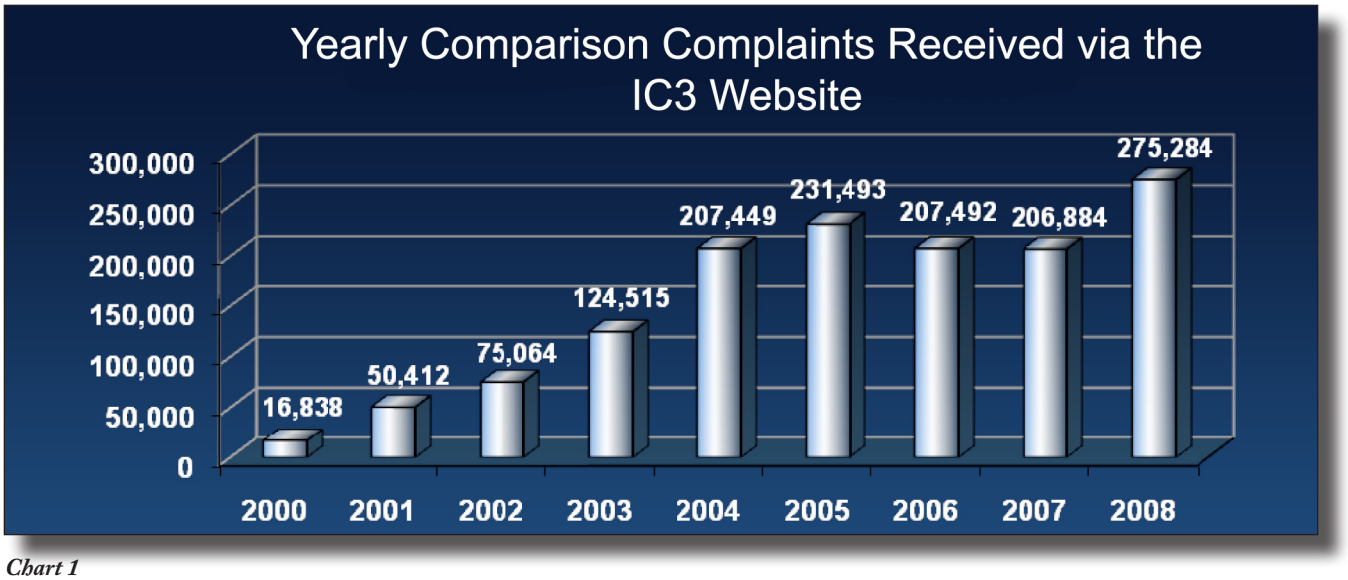


Chart 1

From January 1, 2008 – December 31, 2008, there were 275,284 complaints filed online with IC3. This is a 33.1% increase compared to 2007 when 206,884 complaints were received. Tracking of this data began in 2000, when there were 16,838 complaints. Since then, complaints doubled each year to 2004, when they hit 207,449. From 2004 through 2007 they remained around the same threshold. In 2008, there was again a spike of approximately 75,000 complaints that took it to the 275,284 total.

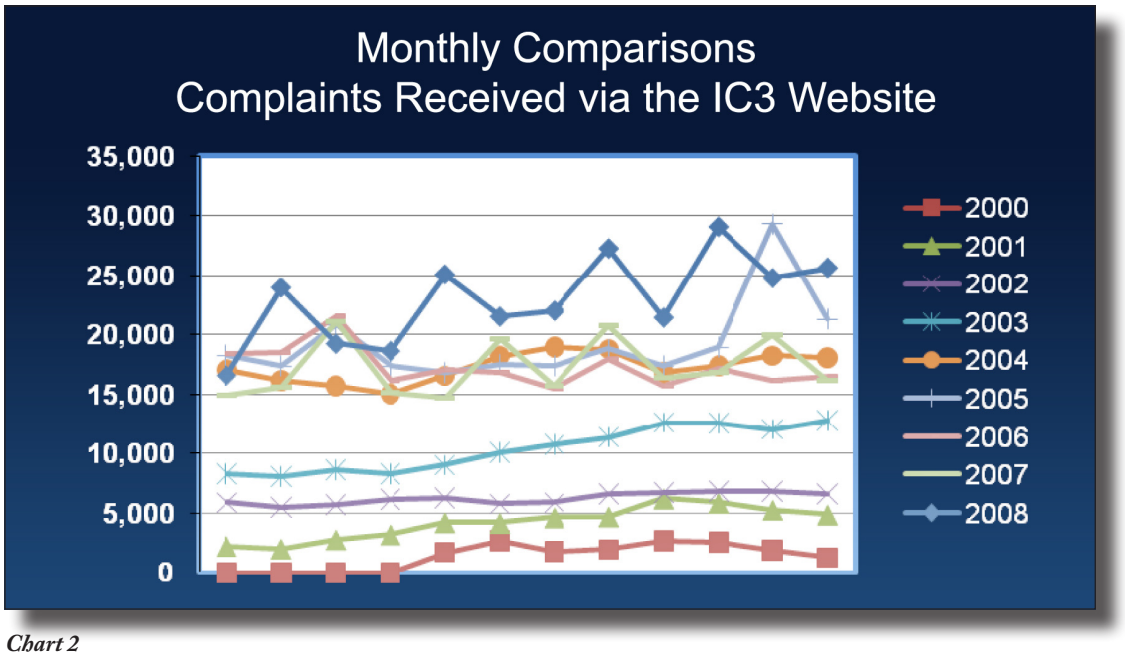


Chart 2
From January 1, 2008 – December 31, 2008 the number of complaints filed per month, last year, averaged 22,940. This is a dramatic increase since the year 2000, when IC3 averaged just over 1,400 compliant a month.

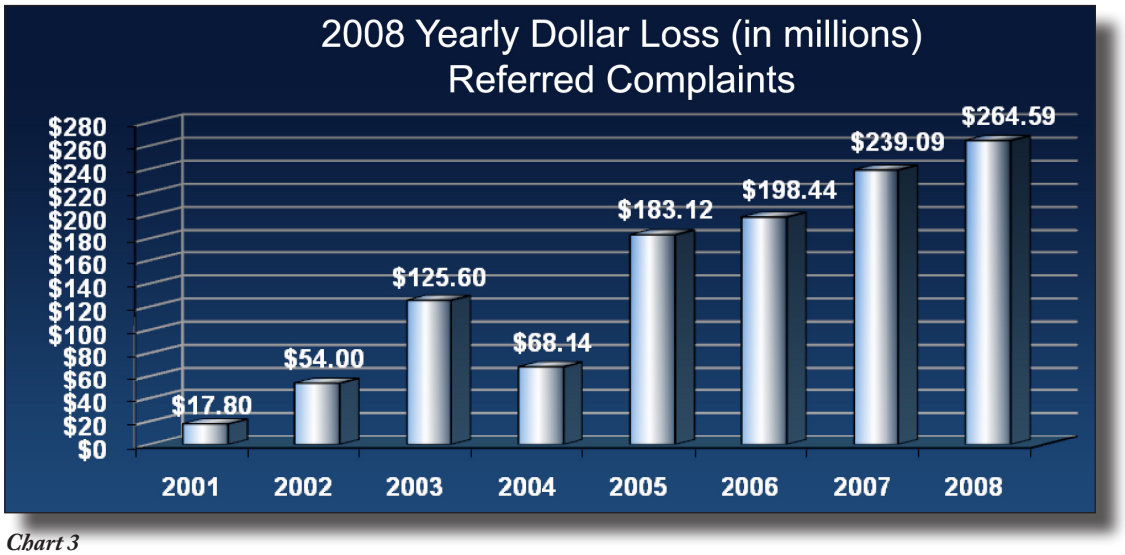


Chart 3
Dollar loss of referred complaints was at an all time high in 2008, $264.59 million, exceeding last year's record breaking dollar loss of $239.09 million. On average, men lost more money than women.

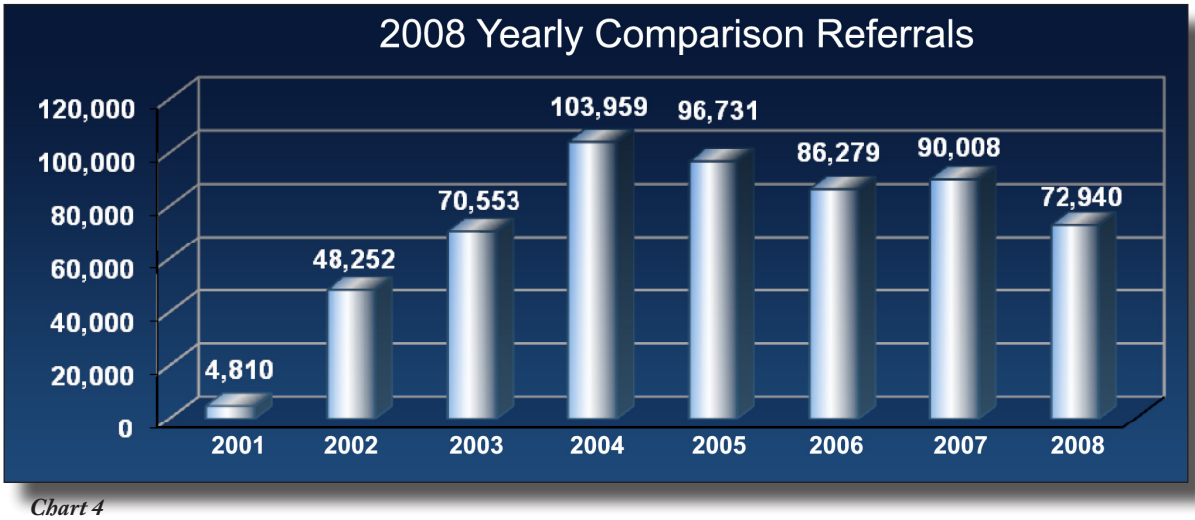


Chart 4
The number of referred complaints has decreased from 90,008 in 2007 to 72,940 in 2008. The 129,349 complaints that were not directly referred to law enforcement in 2008 are accessible to law enforcement, used in trend analysis, and also help provide a basis for future outreach events and educational awareness programs.

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*** by the public; however, the data represents a sub-sample comprised of those complaints that have been referred to law enforcement. While IC3's primary mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime, those complaints involving more traditional methods of contact (e.g., telephone and mail) were also referred. Using information provided by the complainant, the vast majority 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 perpetrator(s) and victims(s).

Complaint Characteristics

During 2008, non-delivery of merchandise and/or payment was by far the most reported offense, comprising 32.9% of referred crime complaints. This represents a 32.1% increase from the 2007 levels of non-delivery of merchandise and/or payment reported to IC3. In addition, during 2008, auction fraud represented 25.5% of complaints (down 28.6% from 2007), and credit and debit card fraud made up an additional 9.0% of complaints. Confidence fraud such as Ponzi schemes, computer fraud, and check fraud complaints represented 19.5% of all referred complaints. Other complaint categories such as Nigerian letter fraud, identity theft, financial institutions fraud, and threat complaints together represented less than 9.7% of all complaints (See Chart 5).

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

Through its relationships with law enforcement and regulatory agencies, IC3 continues to refer complaints to the appropriate agencies. Complaints received by IC3 included confidence fraud, investment fraud, business fraud, and other unspecified frauds. Identity theft complaints are referred to the Federal Trade Commission (FTC) in addition to other agencies. Also, Nigerian (west African, 419, advance loan) letter fraud or 419 scams are referred to the United States Secret Service and child sexual exploitation complaints are referred to the National Center for Missing and Exploited Children. Compared to 2007, there were slightly higher reporting levels of all complaint types, except for auction

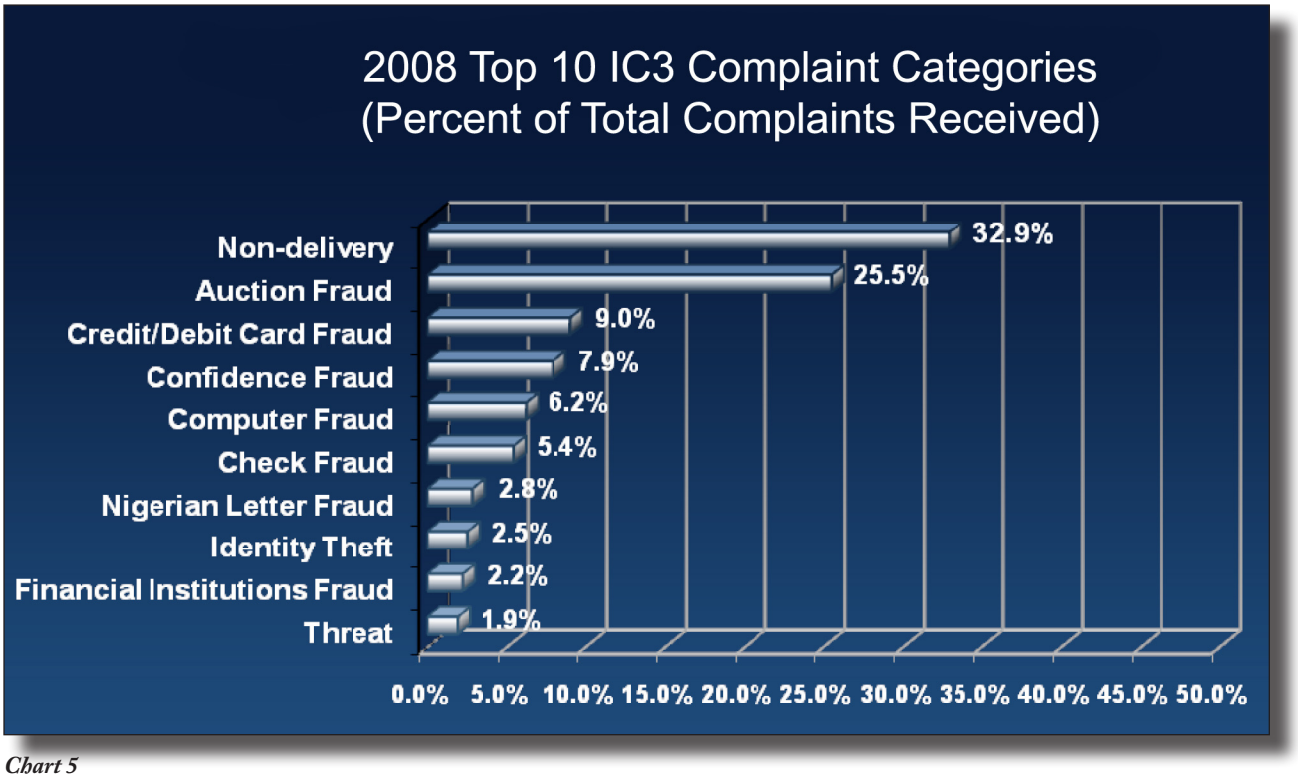


Chart 5

During 2008, non-delivered merchandise and/or payment was, by far, the most reported offense, comprising 32.9% of referred complaints. Internet auction fraud accounted for 25.5% of referred complaints. Credit/debit card fraud made up 9.0% of referred complaints. Confidence fraud, computer fraud, check fraud, and Nigerian letter fraud round out the top seven categories of complaints referred to law enforcement during the year.

fraud, in 2008. For a more detailed explanation of complaint categories used by IC3, refer to Appendix Explanation of Complaint Categories at the end of this report.

A key area of interest regarding Internet fraud is the average monetary loss incurred by complainants contacting IC3 (See Chart 6). 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 that is familiar to the general public: the total dollar amount divided by the total number of complaints. Because the mean can be sensitive to a small number of extremely high or extremely low loss complaints, the median is also provided. The median represents the 50th percentile, or midpoint, of all loss amounts for all referred complaints. The median is less susceptible to extreme cases, whether high or low cost.

Of the 72,940 fraudulent referrals processed by IC3 during 2008, 63,382 involved a victim who reported a monetary loss. Other complainants who did not file a loss may have reported the incident prior to victimization (e.g., received a fraudulent business investment offer online or in the mail), or may have already recovered money from the incident prior to filing (e.g., zero liability in the case of credit/debit card fraud).

The total dollar loss from all referred cases of fraud in 2008 was $264.6 million. That loss was greater than 2007 which reported a total loss of $239.1 million. Of those complaints with a reported monetary loss, the mean dollar loss was $4,174.50 and the median was $931.00. Nearly fifteen percent (14.8%) of these complaints involved losses of less than $100.00, and (36.5%) 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 (33.7%) of the complainants reported

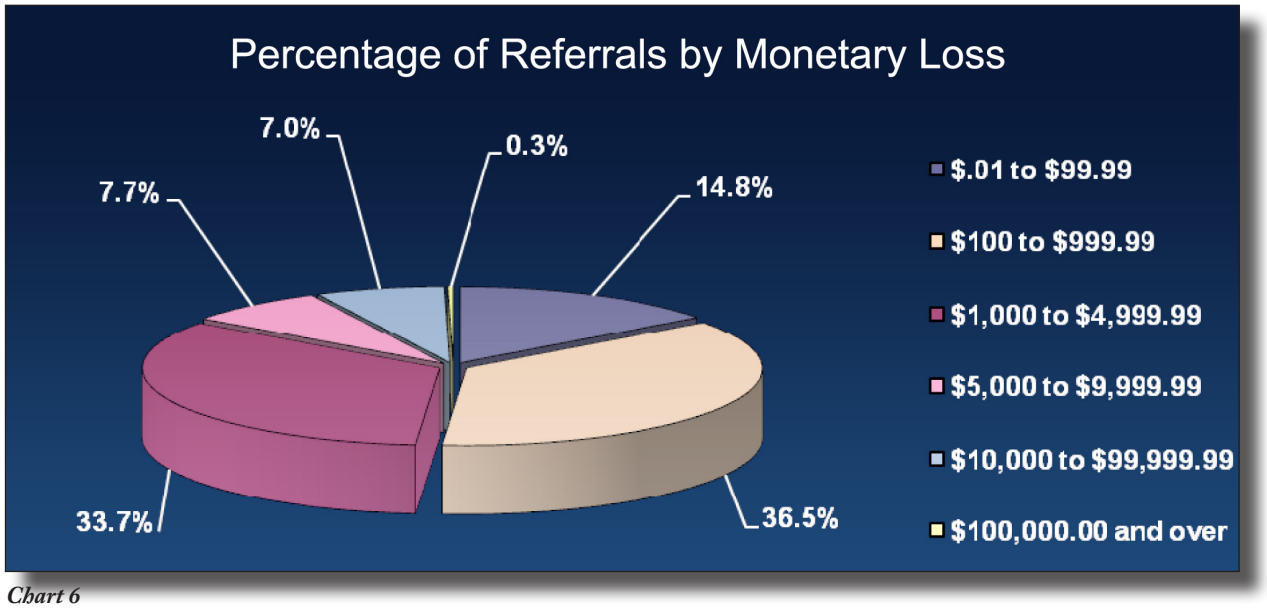


Chart 6
A key area of interest regarding Internet fraud is the average monetary loss incurred by complainants contacting IC3. Of the 72,940 fraudulent referrals processed by IC3 during 2008, 63,382 involved a victim who reported a monetary loss. The total dollar loss from all referred cases of fraud in 2008 was $264.6 million.

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
Check Fraud	7.8%	$3,000.00
Confidence Fraud	14.4%	$2,000.00
Nigerian Letter Fraud	5.2%	$1,650.00
Computer Fraud	3.8%	$1,000.00
Non-delivery (merchandise and payment)	28.6%	$800.00
Auction Fraud	16.3%	$610.00
Credit/Debit Card Fraud	4.7%	$223.00

Table1
The total dollar loss from all referred cases of fraud in 2008 was $264.6 million. That loss was greater than 2007 which reported a total loss of $239.1 million. The highest dollar loss per incident was reported by check fraud (median loss of $3,000). The lowest dollar loss was associated with credit/debit card fraud (median loss of $223.50).

losses between $1,000.00 and $5,000.00 and only 15.0% indicated a loss greater than $5,000.00. The highest dollar loss per incident was reported by check fraud (median loss of $3,000). Confidence fraud victims (median loss of $2,000.00), and Nigerian letter fraud (median loss of $1,650) were other high-dollar loss categories. The lowest dollar loss was associated with credit/debit card fraud (median loss of $223.50). Table 1 illustrates this.

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, District of Columbia, and Washington (see Map 1). These locations are among the most populous in the country. Controlling for population, the District of Columbia, Nevada, Washington, Montana, Florida, and Delaware have the highest per capita rate of perpetrators in the United States (see Table 2). Perpetrators also have been identified as residing in the United Kingdom, Nigeria, Canada, Romania, and Italy (see Map 2). Inter-state and international boundaries are irrelevant to Internet criminals. Jurisdictional issues can enhance their criminal efforts by impeding investigations with multiple victims, multiple states/counties, and varying dollar losses. These statistics highlight the anonymous nature of the Internet. The gender of the perpetrator was reported only 37.3% of the time, and the state of residence for domestic perpetrators was reported only 33.3% of the time.

The vast majority of perpetrators were in contact with the complainant through either e-mail or via websites. (Refer to Appendix III at the end of this report for more information about perpetrator statistics by state). Of these reports 77.4% of perpetrators were male and 22.6% were female.

Map 1 *- Top Ten States (Perpetrators)*

1. California	15.8%	6. Washington	3.9%
2. New York	9.5%	7. Illinois	3.3%
3. Florida	9.4%	8. Georgia	3.1%
4. Texas	6.4%	9. New Jersey	2.8%
5. D.C.	5.2%	10. Arizona	2.6%

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, District of Columbia, and Washington.

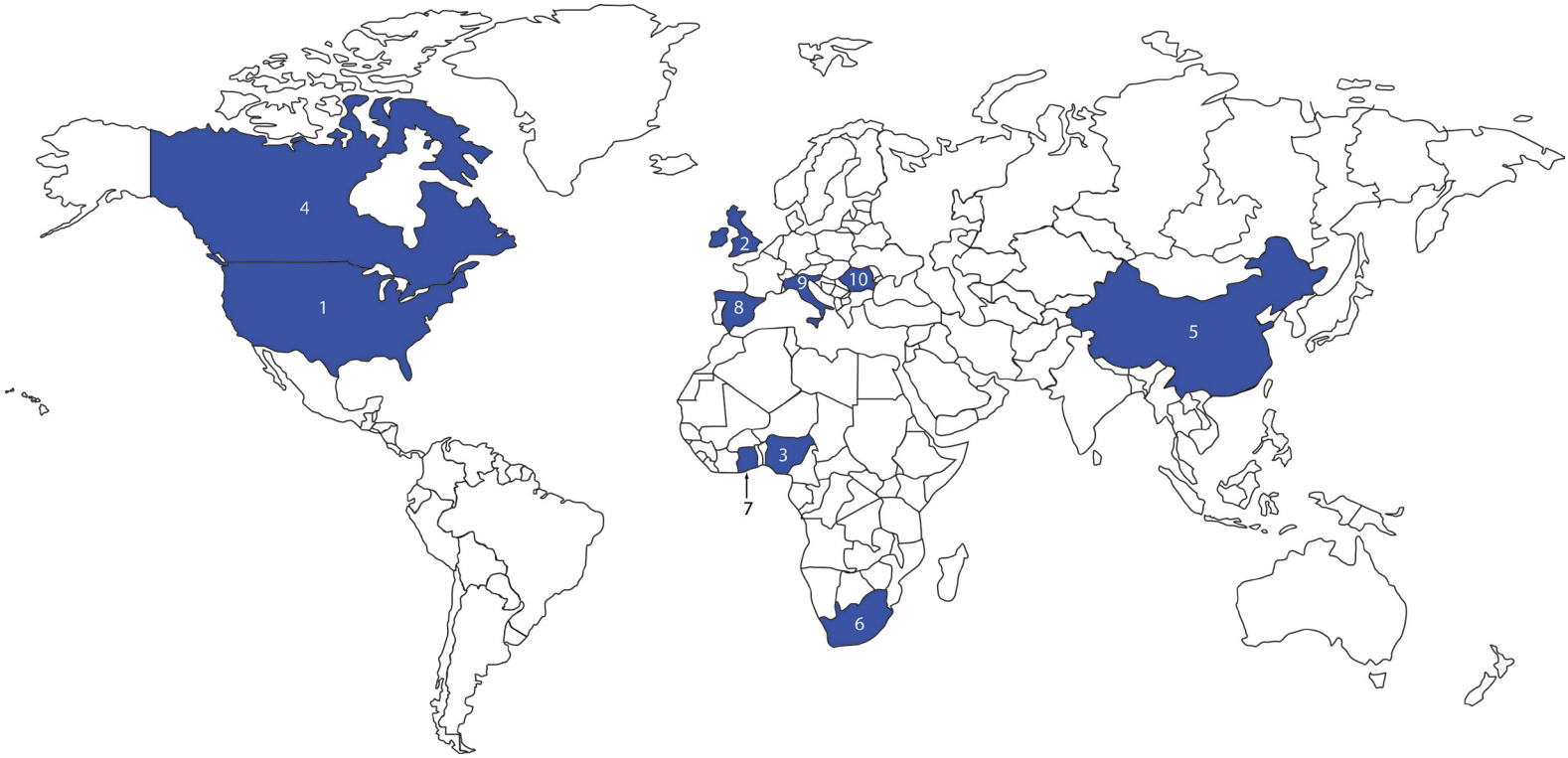
Perpetrators per 100,000 people

Rank	State	Per 100,000 People
1	District of Columbia	81.32
2	Nevada	80.84
3	Washington	55.38
4	Montana	54.47
5	Florida	47.96
6	Delaware	45.75
7	New York	45.47
8	Hawaii	44.55
9	Utah	41.11
10	California	40.09

Table 2

These locations are among the most populous in the country. Controlling for population, the District of Columbia, Nevada, Washington, Montana, Florida, and Delaware have the highest per capita rate of perpetrators in the United States.

Top Ten Countries By Count: Perpetrators



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

1. United States	66.1%	6. South Africa	0.7%
2. United Kingdom	10.5%	7. Ghana	0.6%
3. Nigeria	7.5%	8. Spain	0.6%
4. Canada	3.1%	9. Italy	0.5%
5. China	1.6%	10. Romania	0.5%

Perpetrators also have been identified as residing in the United Kingdom, Nigeria, Canada, Romania, and Italy. Inter-state and international boundaries are irrelevant to Internet criminals. Jurisdictional issues can enhance their criminal efforts by impeding investigations with multiple victims, multiple states/counties, and varying dollar losses.

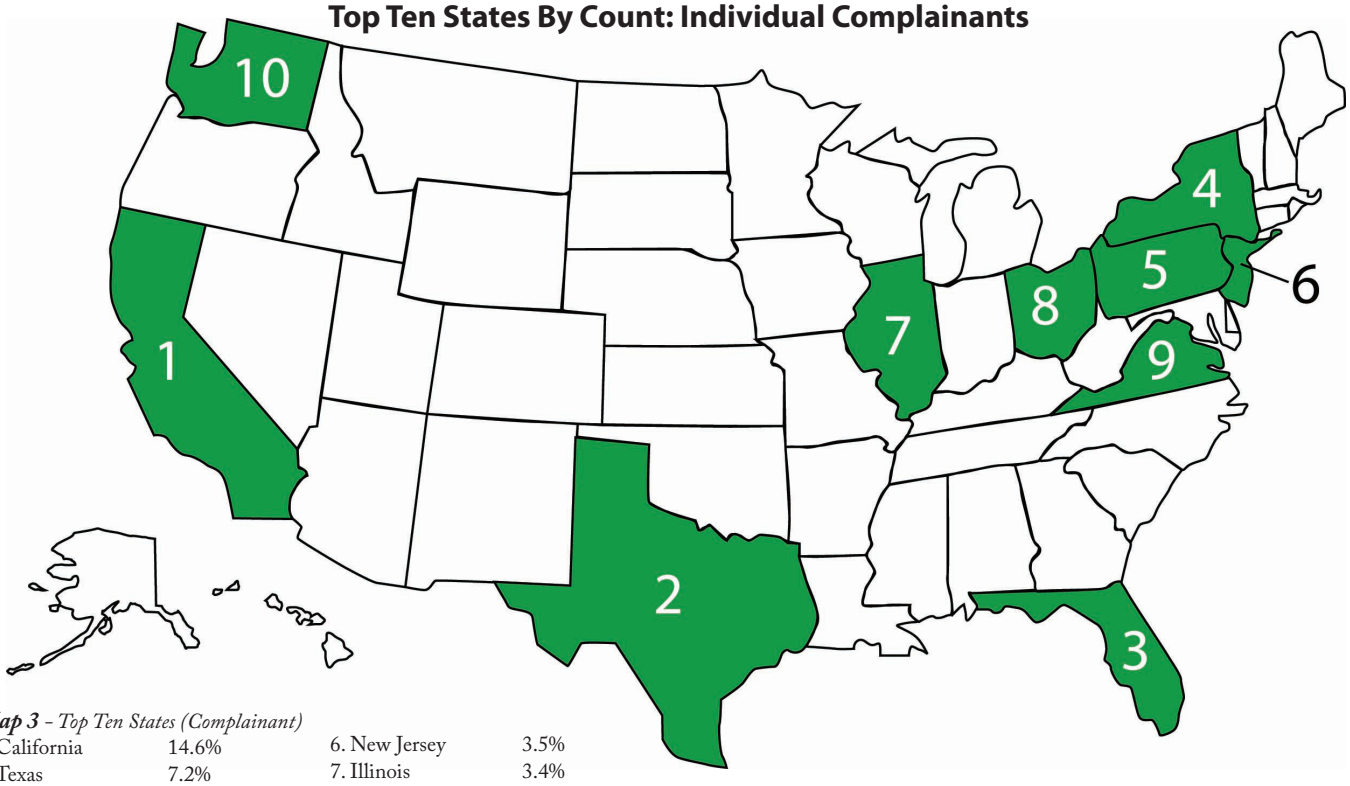
Complainant Characteristics

The following graphs offer a detailed description of the individuals who filed an Internet fraud complaint through IC3 (see Map 3). 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. Alaska, Colorado, and DC, while having a relatively small number of complaints (ranked 31st, 11th, and 45th 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).

Table 4 compares differences between the dollar loss per incident and the various complainant demographics. Males reported greater dollar losses than females (ratio of $1.69 dollars to every $1.00 dollar). Individuals 40-49 years of age reported higher or equal amounts of loss than other age groups.

Top Ten States By Count: Individual Complainants



Map 3 *- Top Ten States (Complainant)*

1. California	14.6%	6. New Jersey	3.5%
2. Texas	7.2%	7. Illinois	3.4%
3. Florida	7.1%	8. Ohio	3.0%
4. New York	5.4%	9. Virginia	2.9%
5. Pennsylvania	3.6%	10. Washington	2.9%

The graph offers a detailed description of the individuals who filed an Internet fraud complaint through IC3.

Complainants per 100,000 people

Rank	State	Per 100,000 People
1	Alaska	337.61
2	Colorado	135.46
3	District of Columbia	119.63
4	Nevada	113.07
5	Maryland	111.60
6	Washington	105.95
7	Arizona	101.46
8	Oregon	101.03
9	Florida	95.25
10	California	95.09

Table 3 *- based on 2008 Census figures*

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. Alaska, Colorado, and DC, while having a relatively small number of complaints (ranked 31st, 11th, and 45th respectively), had among the highest per capita rate of complainants in the United States

Top Ten Countries (Complainant)

Map 4 *- Top Ten Countries (Complainant)*

1. United States	92.93%	6. France	0.15%
2. Canada	1.77%	7. South Africa	0.15%
3. United Kingdom	0.95%	8. Mexico	0.14%
4. Austrailia	0.57%	9. Denmark	0.13%
5. India	0.36%	10. Philippines	0.13%

While most complainants were from the United States, IC3 has also received a number of filings from Canada, the United Kingdom, and Australia

Amount Lost per Referred Complaint by Selected Complainant Demographics	Average (Median) Loss Per Typical Complaint
Male	$993.76
Female	$860.98
Under 20	$500.00
20-29	$873.58
30-39	$900.00
40-49	$1,010.23
50-59	$1,000.00
60 and older	$1,000.00

Table 4

The difference between the dollar loss per incident and the various complainant demographics is shown above. Males reported greater dollar losses than females (ratio of $1.69 dollars to every $1.00 dollar). Individuals 40- 49 years of age reported higher or equal amounts of loss than other age groups.

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 30.6% of all cases involved both a complainant and perpetrator residing in the same state. Other states have an even smaller percentage of complainant-perpetrator similarities in residence. These patterns not only indicate "hot spots" of perpetrators (California for example) that target potential victims from around the world, but also indicate that complainants and perpetrators may not have had a relationship prior to the incident.

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 through e-mail (74.0%) or a webpage (28.9%). Others reportedly had phone contact (15.0%) with the perpetrator or corresponded through physical mail (8.3%). Interaction through chat rooms (2.2%) and in-person (1.7%) meetings were rarely reported. The anonymous nature of an e-mail address or a website allows perpetrators to solicit a large number of victims with a keystroke (see Chart 7).

Perpetrators from Same State as Complainant

State	Percent	1	2	3
1. California	30.6	(New York 8.0%)	(Florida 8.0%)	(Texas 5.1%)
2. Florida	24.4	(California 12.6%)	(New York 8.6%)	(D.C. 5.1%)
3. Arizona	22.7	(California 12.6%)	(New York 7.5%)	(Florida 7.3%)
4. New York	21.7	(California 14.0%)	(Florida 9.2%)	(Texas 5.1%)
5. Nevada	20.0	(California 15.8%)	(New York 7.6%)	(Florida 6.2%)
6. Texas	19.5	(California 12.8%)	(New York 8.5%)	(Florida 7.2%)
7. Georgia	18.6	(California 11.5%)	(New York 9.2%)	(Florida 8.7%)
8. Washington	18.1	(California 14.5%)	(Florida 7.7%)	(New York 7.3%)
9. Illinois	15.6	(California 13.0%)	(New York 8.4%)	(Florida 8.0%)
10. D.C.	15.2	(California 8.9%)	(Texas 5.5%)	(New York 5.5%)

Table 5 *– Other top three locations in parentheses*

The table above highlights this truly "borderless" phenomenon. Even in California, where most of the reported fraud cases originated, only 30.6% of all cases involved both a complainant and perpetrator residing in the same state. Other states have an even smaller percentage of complainant-perpetrator similarities in residence.

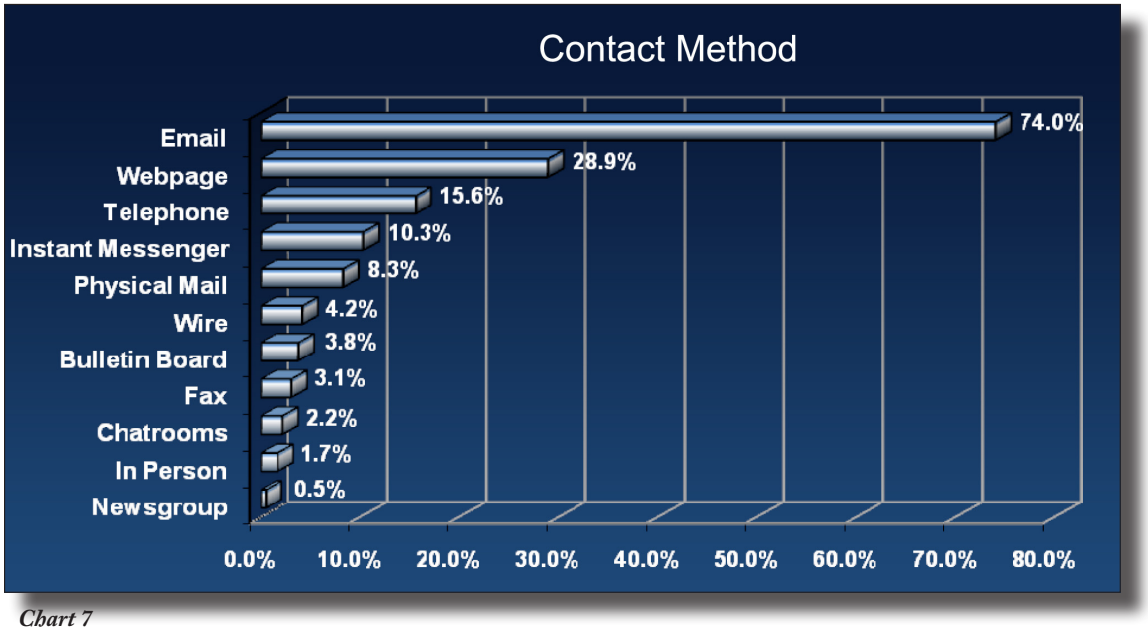


Chart 7

Although complainants in these cases may report multiple contact methods, few reported interacting face-to-face with the vast majority of perpetrators contact through e-mail (74.0%) or a webpage (28.9%). Others reportedly had phone contact (15.0%) with the perpetrator or corresponded through physical mail (8.3%). Interaction through chat rooms (2.2%) and in-person (1.7%) meetings were rarely reported.

Additional Information About IC3 Referrals

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

For those complaints that are computer-related but not considered Internet fraud, IC3 routinely refers these to agencies and organizations that handle those particular violations. For example, if IC3 receives information related to a threat on the President of the United States, the complaint information is immediately forwarded to the United States Secret Service. Spam complaints and cases of identity theft are forwarded to the Federal Trade Commission and referred to federal, state, and local government agencies with jurisdiction.

Scams of 2008

Among the Internet-facilitated scams commonly reported to the IC3 in 2008 were those involving spam, bad checks, roommates, and the names of FBI officials. In an effort to raise public awareness and reduce victimization, this section describes the basic characteristics of these scams, while highlighting their variations and the ways they often overlap with other types of crimes.

One of the more significant scams the IC3 saw during 2008 was the use of fraudulent, unsolicited e-mails to commit identity theft. While the idea of using spam to steal identity information is nothing new, these e-mails are distinguished by their appearance of having been sent by the Federal Bureau of Investigation (FBI). The e-mails solicit personal information, such as one's bank account number, by falsely claiming that the FBI needs such information in order to investigate an impending financial transaction. This transaction typically involves a transfer of funds from a source in a foreign country, often Nigeria, to a bank account belonging to the e-mail recipient. Recipients of these e-mails are led to believe that, by cooperating with this investigation and providing the necessary information, they may help the FBI determine the legitimacy of the transaction and facilitate its processing. Recipients are led to believe they may profit greatly as a result of their cooperation.

The putative source of the funds varies. For instance, the e-mail may claim that the recipient is entitled to an inheritance or has won some obscure lottery. Millions of dollars wait to be moved into the recipient's bank account; however, in order to claim this money, recipients must provide their bank account information so that the FBI can work with foreign bank officials to properly process the transfer. Many of these e-mails also contain an element of extortion. Recipients are told that if they do not comply with the FBI's request for information, they will be prosecuted or suffer some other financial penalty. In some cases, recipients are led to believe that they will become the subject of a terrorist investigation if they fail to cooperate.

Invariably, the e-mails attempt to create an air of legitimacy by claiming to be from FBI Director Robert Mueller, Deputy Director John S. Pistole, or some other high ranking official or investigative unit within the FBI. For instance, many e-mails refer to the FBI's Anti-Terrorist and Monetary Crimes Division—presumably in an effort to support the idea that if e-mail recipients do not comply, they will become vulnerable to allegations of terrorist activities. Internet users should know, however, that the FBI does not contact U.S. citizens regarding personal financial matters through unsolicited e-mails. Another unmistakable sign of illegitimacy is that these e-mails almost invariably contain gross spelling and grammatical errors. Such errors are characteristic of many Nigerian letter (west African ,419, advance fee) frauds.

Because the IC3 just recently modified its data collection system to isolate complaints involving these kinds of e-mails, the IC3 is unable to quantify the prevalence of such complaints for 2008. However, a cursory glance at a sample of recent complaints shows that these e-mails are targeting a substantial number of complainants, indicating the popularity of this method among identity thieves.

Another scam commonly reported to the IC3 in 2008 combined computer intrusion techniques with social engineering, while exhibiting a more personal appeal in an attempt to defraud people. The scam begins with fraudsters gaining unauthorized access to an e-mail user's account. After gaining access to an account, fraudsters take it over and then use it to send unsolicited e-mails to the victims' contacts. Posing as the owners of the e-mail account, fraudsters claim that they are stranded in Nigeria (or some other country) and desperately need financial assistance to see them through a crisis. In many cases, e-mail recipients are told that their friends were robbed in the street and now need $1,000.00 to cover hotel bills and travel expenses. Recipients who respond to these e-mails by sending money as directed, believing they are helping a friend in trouble, often receive follow up e-mails requesting

more money. In an effort to reassure their victims, the imposters promise to reimburse these people once they fully extract themselves from this bad situation.

As in the spoofed FBI e-mails, these e-mails are often riddled with spelling and grammatical errors, which are usually signs of an illegitimate communication. Those receiving such e-mails should be cautious and contact their friends by some means other than e-mail in order to confirm the request for assistance.

Overpayment scams were also commonly reported to the IC3 in 2008. In these scams, fraudsters negotiate formal or informal contracts requiring payment to victims. Invariably, victims receive payments in excess of the amount owed. Fraudsters then instruct their victims to deposit the money and to wire the excess amount back to them or some third party, usually supplying a credible story explaining the excess amount. If the fraudsters are successful, the victims follow their instructions, only to find out later that the payment instrument the fraudster used was illegitimate. Victims are then held liable by their banks for losses generated by the fraudulent transaction.

Several varieties of the overpayment scam exist. Such scams include the secret shopper and pet schemes discussed in this section of the 2007 IC3 Report. In 2008, one of the most common forms of this scam reported to the IC3 was the roommate variety. In this scam, victims seeking roommates reach a deal with an interested party (the fraudsters). The fraudster invariably agrees to pay the victim with a check or money order. Then, a familiar sequence of financial transactions follows: Victims receive bad checks written in excess of what was originally agreed, deposit them into their bank accounts, and then, following the fraudsters' instructions, wire the excess amount to a third party before the initial check clears. Typically, fraudsters tell their victims that the excess amount is meant to cover moving expenses; and the difference is to be wired back to them or to a business partner (usually a bogus furniture supplier or moving company). The true status of the checks sent by fraudsters usually does not surface until after the excessive funds have been wired and cashed, and victims get saddled with the losses.

Scam Synopsis

The scams detailed above are just a sample of the scams frequently reported to the IC3 in 2008. Although in this section, we focus on a variety of schemes involving spam, theft, and bad checks; this limited survey hardly captures the full spectrum of Internet-facilitated crimes. The fraudster's toolbox is by no means limited to these devices, as the Internet presents fraudsters with myriad opportunities to multiply the devices at their disposal. Internet users should be wary when dealing with people they do not know (and sometimes people they think they know), especially while engaging in online financial transactions.

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 or their identity information in one of them. To learn about the latest scams, we recommend periodically checking the IC3, FBI, and the FTC websites for the latest updates.

Results of IC3 Referrals

IC3 occasionally 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:

- John Childe, the subject of multiple complaints filed with IC3, has been sentenced. IC3 complaints alleged that Childe offered various items for sale on the eBay auction site and either failed to deliver the items or sent inferior or less expensive products. The investigator assigned to the case as part of the San Diego CATCH Team, contacted the IC3 for a database search to determine if there were additional victims that had filed. According to the investigator, Childe pled guilty and will make restitution to his victims. Childe was sentenced to three years probation.
- Rachel Trent, a Virginia woman who scammed sports memorabilia collectors out of $3,000 has been sentenced to four years in prison. Trent was the subject of multiple complaints filed with IC3, used the eBay auction site to bilk collectors out of their money. She offered baseball and football cards on the site, advertising the items as rare. Once the buyer sent payment for the card, Trent would send the buyer a worthless card or a card that was different than the one shown in the auction; in some cases, Trent would send no card at all. The Central Virginia Computer Crimes Task Force arrested Trent after receiving complaints from victims in Virginia, Ohio and Pennsylvania. Trent pled guilty to the charges in Campbell County Circuit Court.

- Kenneth Kranich has been charged with three counts of theft by fraud. A year-long investigation of Kranich's activities was initiated after police received notification of multiple complaints being filed with IC3 involving items that Kranich placed up for bid on the eBay auction site. The complaints allege that Kranich offered numerous Hewlett-Packard computers for sale, receiving between $375 and $465 for each computer sold. The computers, however, were never sent to their purchasers. Investigators built their case by working with eBay, who provided law enforcement with the registered identity associated with Kranich's eBay user ID. Police are currently filing charges in the four cases that presented the most evidence, however, as many as 42 victims spanning 12 states were possibly involved. Prior to the current charges, Kranich possessed no criminal record; he confessed to investigators that he was using the eBay scheme to fund his gambling addiction.
- Michelle Brown, a New Hampshire resident, was arrested by members of the Manchester Police Department for allegedly committing fraud via the eBay auction site. The investigation began when police received a complaint description of fraud via IC3 concerning a non-delivery of merchandise scam. Brown is accused of collecting over $1,000 from a bidder for the sale of a big-screen plasma television that was listed on the auction site. Brown, however, did not have the television in her possession nor did she intend to produce a television to honor her contract. Subsequently, detectives learned that Brown may have perpetrated this type of fraud multiple times; further charges are possible if more victims do come forward. In addition to the auction fraud(s), Brown was also charged with two counts of felony identity theft for allegedly opening credit card accounts in her mother's name. Warrants were obtained for Brown's arrest following a tip to police that she was planning to flee the country.
- Justin Castilyn, of Center Township Pennsylvania, has been arrested for allegedly sending a counterfeit money order to a San Francisco man for the purchase of more than 200 video games. The seller, who had listed the games on Craigslist, shipped the games to Castilyn after receiving payment from him in the form of a money order for $1,950.00. Upon attempting to deposit the money, however, the seller learned that the money order was counterfeit and filed a complaint with IC3, the San Francisco Police, and Pennsylvania authorities. During the investigation, the investigator contacted IC3 and learned that federal authorities already suspected Castilyn of scamming at least eight other victims, either through non-delivery of merchandise or non-payment for merchandise, in online transactions. With this information, a search warrant was obtained and two computers, as well as, twelve other suspected counterfeit money orders were seized from Castilyn's residence. The 28 year old Castilyn was arraigned on charges of forgery, access device fraud, receiving stolen property and unlawful use of a computer and was placed in the county jail on $75,000.00 bond.
- Jive Network, Inc., an organization that has been the subject of complaints filed with the (IC3), has been dealt a major blow by the United States Attorney's Office in the Middle District of Florida. U.S. Attorney Robert O'Neill has announced that Jude LaCour, his father Jeffery LaCour, and Hudsen Smith have been indicted along with eight other defendants. According to the indictment, the defendants conspired to distribute controlled substances and other prescription drugs to customers located across the United States who did not have valid prescriptions. Jude LaCour owned and operated Jive Network Inc., which used the Internet to distribute and dispense the drugs to customers unlawfully. Jeffery LaCour served as the Director of Operations for the organization and Hudsen Smith was the Director of Pharmacy/ Physician operations. The organization distributed approximately 4.8 million dosage units of Schedule III controlled substances and approximately 39.2 million dosage units of Schedule IV controlled substances. Jude and Jeffrey LaCour allegedly agreed to launder the proceeds of the illegal drug conspiracy with the intent to promote and carry on the conspiracy. In addition, they transferred millions of dollars via wire transfer and check to their personal brokerage or bank accounts. The pair has been charged with money laundering and various drug trafficking offenses involving the sale of controlled substances over the Internet. If convicted, the maximum penalty for each count of money laundering ranges from ten to twenty years imprisonment and the maximum penalty for each county of drug trafficking ranges from three to five years imprisonment. For their role in the conspiracy, Hudsen Smith and eight others were charged with drug trafficking offenses only. The case was investigated jointly by the Federal Bureau of Investigation, the Internal Revenue Service, and the Food and Drug Administration and will be prosecuted by the United States Attorney's Office.

IC3 Capabilities

Over the past decade, numerous methods have been employed to keep pace with technological changes and information sharing, all of which have been met with only partial success due to a variety of reasons. Perhaps most important is that past efforts typically reach small segments of localized or regionalized law enforcement groups with the end result being limited or restricted data sharing. The speed and ease at which perpetrators can reach across world-wide boundaries further exacerbates the problem. Other barriers include inconsistent training and limited sharing of only post-investigation data.

The FBI's IC3 Unit uses analytical tools to build case referrals from IC3's consumer complaint database. The FBI analysts augment the consumer complaint data with information from open and closed (law enforcement) sources as well as private industry. FBI analytical and case assistance is made available to all law enforcement agencies as part of any IC3 referral or upon request from a law enforcement agency.

Along with useful productivity tools, IC3 and NW3C also offers analytical staff, trainers and researchers to assist law enforcement with any needs they have regarding case development including: searching and compiling case information, conducting forensic analysis of received data, contacting other agencies who may share interest in collaborative investigations, providing training support or direct delivery training, building link charts and writing case reports.

NW3C Software

Over the past two years of intense research, focus-group events, project planning, and project development, NW3C now offers a uniquely designed Internet Complaint Search and Investigation System (ICSIS)*, an accessible software solution, accessed via a secure, password-controlled website. This security makes the tool available to any NW3C approved agency with Internet access and eliminates the need for purchasing any new software or hardware product beyond a typical desktop or laptop computer with a common web browser.

ICSIS includes a search feature that can explore multiple data streams simultaneously and utilizes fuzzy logic to improve compilation analysis. Third party analytical tools along with import/export features, (for example, I2 Analyst's Notebook link charts) are integrated into the application to supply visual trends and crime patterns within cases including mapping, statistical, and timeline functions. Search results and cases can be seamlessly shared among multiple investigators, a user-defined individual or group such as an investigative task force. Users can include comments or assign attributes and categories. Other features include: notification and/or links to other open investigations, automated notification when a new investigation is opened, a discussion forum, user-driven support, help, feedback, as well as I2 Analyst Notebook ixviewer which allows information obtained through ICSIS to be graphically displayed.

Working in concert with the ICSIS system is the Complaint Management System (CMS), a software development project that sets agency threshold preferences among any collected data set or combination thereof and then refers the received complaint to the responsible agency. In addition to quickly referring complaints according to each agency's priorities, CMS allows reallocation of human capital for the purpose of improving services to recipient agencies. A self guided tutorial is available online at ***https://members.nw3c.org/services_databases.cfm*** and Help Desk support during normal business hours is available as well.

** ICSIS is a tool developed by NW3C for use by its members to work with IC3 data and has not been vetted by the FBI.*

Conclusion

The IC3 report has outlined many of the current trends and patterns in Internet crime. The data indicates that instances involving Internet crime are on the increase as seen with the record number complaints submitted, 275,284, in 2008, up from 206,884 in 2007, 207,492 complaints in 2006 and 231,493 in 2005. This total includes many different fraud types and non-fraudulent complaints. However, 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 $264.6 million up from $239.1 million in 2007.

Non-delivered merchandise/payment was the most reported offense followed by auction fraud,and credit card/debit card fraud. Among those individuals who reported a dollar loss from the fraud, the highest median dollar losses were found among check fraud victims ($3,000), confidence fraud victims ($2,000), and Nigerian letter (west African, 419, advance fee) fraud victims ($1,650). 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 2007 and the 2008 reports, e-mail and webpages 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 past three years, the IC3 has begun to update/change its method of gathering data regarding complaints, in recognition of the constantly changing nature of cyber crime, and to more accurately reflect meaningful trends. With this in mind, changes to the IC3 website and complaint form have been implemented, with some of those changes taking effect as of January, 2006 while others have as recently as January 2009. Along with these changes, the IC3 and its partners have launched a public website, www.lookstoogoodtobetrue.com, which will educate consumers to various consumer alerts, tips, and fraud trends.

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

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

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

Appendix - 1

Explanation of Complaint Categories

Although the transition to IC3 better reflects the processing of Internet crime complaints, the fraud complaint categories are still used to categorize complaint information. IC3 Internet Fraud Analysts determined a fraud type for each Internet fraud complaint received and sorted complaints into one of nine fraud categories.

- Business Fraud - When a corporation or business knowingly misrepresents the truth or conceals a material fact[2]. Examples of business fraud include bankruptcy fraud and copyright infringement.
- 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.
- 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[3]. 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.
- Financial Institution Fraud - Knowing misrepresentation of the truth or concealment of a material fact by a person to induce a business, organization, or other entity that manages money, credit, or capital to perform a fraudulent activity[4]. Credit/debit card fraud is an example 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[5]. Sports tampering and claiming false bets are two examples of gaming fraud.
- Government Fraud - A knowing misrepresentation of the truth, or concealment of a material fact to induce the government to act to its own detriment[6]. Examples of government fraud include tax evasion, welfare fraud, and counterfeit currency.
- Insurance Fraud - A misrepresentation by the provider or the insured in the indemnity against loss. Insurance fraud includes the "padding" or inflating of actual claims, misrepresenting facts on an insurance application, submitting claims for injuries or damage that never occurred, and "staging" accidents[7].
- Investment Fraud - Deceptive practices involving the use of capital to create more money, either through income-producing vehicles or through more risk-oriented ventures designed to result in capital gains[8]. Pyramid schemes and market manipulation are two types of investment 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[9].

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.
- Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.
- Examine the feedback on the seller and use common sense. If the seller has a history of negative feedback then do not deal with that particular seller.
- Determine what method of payment the seller is asking for and where he/she is asking to send payment. Use caution when the mailing address is a post office box number.
- Be aware of the difference in laws governing auctions between the U.S. and other countries. If a problem occurs with the auction transaction that has the seller in one country and a buyer in another, it might result in a dubious outcome leaving you empty handed.
- Be sure to ask the seller about when delivery can be expected and warranty/exchange information for merchandise that you might want to return.
- To avoid unexpected costs, find out if shipping and delivery are included in the auction price or are additional.
- Finally, avoid giving out your social security number or driver's license number to the seller, as the sellers have no need for this information.

Steps To Take If Victimized:

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

Non-Delivery of Merchandise

Prevention Tips:

- Make sure you are purchasing merchandise from a reputable source. As with auction fraud, check the reputation of the seller whenever possible, including the Better Business Bureau.
- Try to obtain a physical address rather than merely a post office box and a phone number. Also call the seller to see if the number is correct and working.
- Send them an e-mail to see if they have an active e-mail address. Be cautious of sellers who use free e-mail services where a credit card wasn't required to open the account.
- Investigate other websites regarding this person/company.

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

Credit Card Fraud

Prevention Tips:

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

Businesses

Prevention Tips:

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

Investment Fraud

Prevention Tips:

- Do not invest in anything based upon appearances. Just because an individual or company has a flashy website doesn't mean it is legitimate. Websites can be created in just a few days. After a short period of taking money, a site can vanish without a trace.
- Do not invest in anything you are not absolutely sure about. Do your homework on the investment to ensure that it is legitimate.
- Thoroughly investigate the individual or company to ensure that they are legitimate.
- Check out other websites regarding this person/company.
- Be cautious when responding to special investment offers (especially through unsolicited e-mail) by fast talking telemarketers. Know who 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 (west African, 419, Advance Fee)

Prevention tips:

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

Business Fraud

Prevention Tips:

- Purchase merchandise from reputable dealers or establishments.
- Try to obtain a physical address rather than merely a post office box and a phone number, and call the seller to see if the number is correct and working.
- Send them an 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 an e-mail that may not have been sent by a reputable company. Always investigate before purchasing any products.

Identity Theft

Prevention Tips:

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

Steps To Take If Victimized:

1. Contact the fraud departments of each of the three major credit bureaus and report that your identity has been stolen.
2. Get a "fraud alert" placed on your file so that no new credit will be granted without your approval.
3. Contact the security departments of the appropriate creditors and/or financial institutions for any accounts that may have been fraudulently accessed.

Close these accounts. Create new passwords on any new accounts that you open.

4. File a report with your local police and/or the police where the identity theft took place.

5. Retain a copy of the report because it may be needed by the bank, credit card company, or other businesses to prove your innocence.

Cyberstalking

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

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

Appendix - 3

References

1. National White Collar Crime Center, *The National Public Survey on White Collar Crime*, August 2005.
2. Black's Law Dictionary, Seventh Ed., 1999.
3. Ibid.
4. Ibid.
5. Ibid.
6. Black's Law Dictionary, Seventh Ed., 1999. The Merriam Webster Dictionary, Home and Office Ed., 1995.
7. Fraud Examiners Manual, Third Ed., Volume 1, 1998.
8. Barron's Dictionary of Finance and Investment Terms, Fifth Ed., 1998.
9. Ibid.

Appendix - 4

Complainant/Perpetrator Statistics, by State

2008 Complainants by State

Rank	State	Percent	Rank	State	Percent
1	California	14.6	27	Louisiana	1.1
2	Texas	7.2	28	Alaska	1.0
3	Florida	7.1	29	Connecticut	1.0
4	New York	5.4	30	Kansas	1.0
5	Pennsylvania	3.6	31	Kentucky	1.0
6	New Jersey	3.5	32	Oklahoma	1.0
7	Illinois	3.4	33	Utah	0.9
8	Ohio	3.0	34	Arkansas	0.7
9	Virginia	2.9	35	Iowa	0.7
10	Washington	2.9	36	New Mexico	0.6
11	Arizona	2.8	37	Idaho	0.6
12	Colorado	2.8	38	Hawaii	0.5
13	Georgia	2.7	39	Mississippi	0.5
14	Michigan	2.7	40	Nebraska	0.5
15	North Carolina	2.7	41	New Hampshire	0.5
16	Maryland	2.6	42	West Virginia	0.5
17	Indiana	1.9	43	Delaware	0.3
18	Massachusetts	1.9	44	D.C.	0.3
19	Tennessee	1.9	45	Maine	0.3
20	Missouri	1.8	46	Montana	0.3
21	Oregon	1.6	47	Rhode Island	0.3
22	Minnesota	1.5	48	South Dakota	0.2
23	Wisconsin	1.5	49	Vermont	0.2
24	Alabama	1.3	50	Wyoming	0.2
25	South Carolina	1.2	51	North Dakota	0.1
26	Nevada	1.1			

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)

2008 Perpetrators by State

Rank	State	Percent	Rank	State	Percent
1	California	15.8	27	Minnesota	1.0
2	New York	9.5	28	South Carolina	0.9
3	Florida	9.4	29	Wisconsin	0.9
4	Texas	6.4	30	Kentucky	0.7
5	D.C.	5.2	31	Louisiana	0.7
6	Washington	3.9	32	Oklahoma	0.7
7	Illinois	3.3	33	Hawaii	0.6
8	Georgia	3.1	34	Kansas	0.6
9	New Jersey	2.8	35	Montana	0.6
10	Arizona	2.6	36	Delaware	0.5
11	Pennsylvania	2.6	37	Iowa	0.5
12	Ohio	2.5	38	Maine	0.5
13	Nevada	2.3	39	Arkansas	0.4
14	Michigan	2.2	40	Nebraska	0.4
15	North Carolina	1.8	41	New Hampshire	0.4
16	Virginia	1.8	42	Rhode Island	0.4
17	Massachusetts	1.6	43	Idaho	0.3
18	Maryland	1.5	44	West Virginia	0.3
19	Colorado	1.4	45	Mississippi	0.3
20	Indiana	1.3	46	New Mexico	0.3
21	Missouri	1.3	47	Alaska	0.2
22	Tennessee	1.3	48	North Dakota	0.2
23	Utah	1.2	49	South Dakota	0.2
24	Oregon	1.1	50	Vermont	0.2
25	Alabama	1.0	51	Wyoming	0.2
26	Connecticut	1.0			

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	337.61	27	Rhode Island	71.28
2	Colorado	135.46	28	Texas	70.35
3	D.C.	119.63	29	Pennsylvania	69.91
4	Nevada	113.07	30	Delaware	69.75
5	Maryland	111.60	31	North Carolina	69.16
6	Washington	105.95	32	Massachusetts	69.13
7	Arizona	101.46	33	Minnesota	68.54
8	Oregon	101.03	34	Georgia	67.25
9	New Jersey	95.25	35	West Virginia	67.13
10	California	95.09	36	New York	66.75
11	Florida	92.40	37	South Carolina	66.59
12	Virginia	90.53	38	Oklahoma	66.36
13	Wyoming	88.99	39	Connecticut	65.06
14	Idaho	88.79	40	Michigan	64.80
15	Kansas	87.93	41	Alabama	64.31
16	New Hampshire	86.56	42	Ohio	63.43
17	Hawaii	84.92	43	Illinois	62.39
18	Utah	82.33	44	Wisconsin	62.35
19	Vermont	78.07	45	Louisiana	60.78
20	New Mexico	74.03	46	Arkansas	60.20
21	Nebraska	73.57	47	Iowa	54.32
22	Indiana	72.90	48	Kentucky	54.27
23	Missouri	72.38	49	North Dakota	49.88
24	Maine	72.16	50	South Dakota	48.37
25	Montana	71.74	51	Mississippi	44.31
26	Tennessee	71.65			

Table 8 *- based on 2008 Census figures*

Complainant/Perpetrator Statistics, by State (Continued)

Perpetrators per 100,000 people

Rank	State	Per 1,000	Rank	State	Per 1,000
1	D.C.	81.32	27	Illinois	23.90
2	Nevada	80.84	28	Massachusetts	22.34
3	Washington	55.38	29	Nebraska	22.14
4	Montana	54.47	30	Virginia	21.04
5	Florida	47.96	31	Idaho	20.54
6	Delaware	45.75	32	Michigan	20.37
7	New York	45.47	33	Missouri	20.21
8	Hawaii	44.55	34	Ohio	20.14
9	Utah	41.11	35	Alabama	19.88
10	California	40.09	36	Tennessee	19.85
11	Arizona	37.84	37	Kansas	19.52
12	Maine	33.11	38	Pennsylvania	19.40
13	North Dakota	32.73	39	Indiana	19.24
14	Rhode Island	31.30	40	North Carolina	18.57
15	Alaska	30.89	41	Minnesota	18.44
16	Georgia	29.99	42	Oklahoma	18.36
17	New Jersey	29.61	43	South Carolina	18.34
18	South Dakota	27.48	44	West Virginia	17.19
19	Colorado	27.00	45	Kentucky	16.27
20	Wyoming	26.28	46	Arkansas	16.10
21	Oregon	26.27	47	Louisiana	14.98
22	Vermont	25.91	48	Wisconsin	14.81
23	Connecticut	25.36	49	New Mexico	14.76
24	New Hampshire	25.30	50	Iowa	14.35
25	Maryland	25.08	51	Mississippi	10.00
26	Texas	24.60			

Table 9 *- based on 2008 Census figures*

www.ic3.gov