2009
Internet Crime Report

Internet Crime Complaint Center

NW3C
National White Collar Crime Center
Integrity Quality Service

BJA
Bureau of Justice Assistance
U.S. Department of Justice

Table of Contents

This project was supported by Grant No. 2009-BE-BX-K042 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice P the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. this document are those of the author and do not represent the official position or policies of the United States Department of Justice. The National White Collar Crime Center (N of this document. This information may not be used or reproduced in any form without the express written permission of NW3C. This publication is also available for download in ***org*** or ***www.ic3.gov.***

2009 Internet Crime Report

Executive Summary

From January 1, 2009 through December 31, 2009, the Internet Crime Complaint Center (IC3) Web site 336,655 complaint submissions. This was a 22.3% increase as compared to 2008 when 275,284 compla received. Of the 336,655 complaints submitted to IC3, 146,663 were referred to local, state, and federa agencies around the country for further consideration. The vast majority of referred cases contained ele and involved a financial loss by the complainant. The total dollar loss from all referred cases was $559. a median dollar loss of $575. This is up from $264.6 million in total reported losses in 2008. Unreferred generally involved complaints in which there was no documented harm or loss (e.g., a complainant rec solicitation email but did not act upon it) or complaints where neither the complainant nor perpetrator r the United States (i.e., there was not an appropriate domestic law enforcement agency for direct referra

Complaints received by IC3 cover many different fraud and non-fraud categories, including auction frau delivery of merchandise, credit card fraud, computer intrusions, spam/unsolicited email, and child porn All of these complaints are accessible to local, state, and federal law enforcement to support active inv trend analysis, and public outreach and awareness efforts.

On January 1, 2009, IC3 implemented a new complaint classification system based on a redesigned que generates an automatic classification of the complaint into one of 79 offense-based categories. This rec a number of changes to the way the system gathers and classifies complaint data. Further information can be found in Appendix I of this report. Significant findings related to an analysis of the complaint dat

- Email scams that used the Federal Bureau of Investigation's (FBI) name (schemes in which the sca to be affiliated with the FBI in an effort to gain information from the target) represented 16.6% of a submitted to IC3. Non-delivered merchandise and/or payment (in which either a seller did not ship item or a buyer did not pay for an item) accounted for 11.9% of complaints. Advance fee fraud (a s the target is asked to give money upfront- often times- for some reward that never materializes) m of complaints. Identity theft and overpayment fraud (scams in which the target is given a fraudule instrument in excess of the agreed-upon amount for the transaction, and asked to send back the o legitimate monetary instrument) round out the top five categories of all complaints submitted to I
- Of the top five categories of offenses reported to law enforcement during 2009, non-delivered mer payment ranked 19.9%; identity thieft, 14.1%; credit card fraud, 10.4%; auction fraud, 10.3%; and (destruction/damage/vandalism of property), 7.9%.
- Of the complaints involving financial harm that were referred to law enforcement, the highest med found among investment fraud ($3,200), overpayment fraud ($2,500), and advance fee fraud ($1,
- In those complaints in which perpetrator information is provided, 76.6% were male and half reside following states: California, Florida, New York, the District of Columbia, Texas, and Washington. The of reported perpetrators (65.4%) were from the United States. A number of perpetrators were also Kingdom, Nigeria, Canada, Malaysia, and Ghana.
- Among complainants, 54% were male, nearly two-thirds were between the ages of 30 and 50, and third resided in one of the following states: California, Florida, Texas, or New York. The majority of c were from the United States (92%). However, IC3 received a number of complaints originating in C United Kingdom, Australia, India, and Puerto Rico.
- Male complainants lost more money than female complainants (ratio of $1.51 lost per male to eve female). Individuals 40-49 years of age reported, on average, higher amounts of loss than other ag
- In addition to FBI scams, popular scam trends for 2009 included hitman scams, astrological readin economic scams, job site scams, and fake pop-up ads for antivirus software.

Overview

The Internet Crime Complaint Center (IC3) began operation on May 8, 2000, as the Internet Fraud Complaint Center. Established as a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI), IC3 serves as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cybercrime. Since inception, IC3 has received complaints across a wide spectrum of cybercrime 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 and civil matters.

IC3 gives the victims of cybercrime 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 local, state, and federal level, IC3 provides a central referral mechanism for complaints involving Internet-related crimes. For affected members of industry, IC3 can leverage both intelligence and subject matter expert resources to identify and craft an aggressive, proactive approach to combating cybercrime.

IC3 2009 Internet Crime Report is the ninth annual compilation of information on complaints received by IC3 and referred 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; (5) popular scams of 2009; and (6) success stories involving complaints referred by IC3. The results in this report are intended to enhance general knowledge about the scope and prevalence of cybercrime in the United States. This report does not represent all victims of Internet crime, or crime in general because it is derived solely from the people who filed a report with IC3.

General IC3 Filing Information

Complaints are submitted to IC3 at ***www.ic3.gov***. Complainants without Internet access are advised to use resources at their local library, educational institution, local law enforcement agency, or local victim's assist office. After a complaint is filed with IC3, the informat is automatically referred to the appropriate local, stat and federal law enforcement agencies.

From January 1, 2009 through December 31, 2009, there were 336,655 total complaints filed with IC3 (se Figure 1). This is a 22.3% increase compared to 2008 when 275,284 complaints were received. The numbe of complaints filed per month, for 2009, averaged 28,055. Dollar loss of complaints referred to law enforcement was at an all time high in 2009, $559.7 million, compared to previous years (see Figure 2).

The number of complaints referred to law enforcement has increased from 72,940 in 2008 to 146,663 in 2009 (see Figure 3). All complaints not directly referred are still accessible by law enforcement, used for trend analysis, intelligence gathering and consumer education. Typically, these non-referred complaints do not involve a documented case of financial or physical harm or involve a situation in which neither the complainant nor perpetrator reside within the United States. In a minority of cases, there is no designated agency to refer a complaint, based on jurisdictional factors or agency-defined thresholds for referral.

During 2009, IC3 implemented a new complaint classification system. This complainant-driven system is based on a logic-driven questionnaire that generate an automatic classification of the complaint into one of 79 offense-based categories. This redesign has also resulted in a number of changes to the way IC3 system gathers and classifies complaint data. The ne classification system improves upon the previous system by making clearer distinctions between complaint elements and by reducing the number of categories used to classify complaints.

The results contained in this report were based on information that was provided to IC3 through the complaint forms submitted at ***www.ic3.gov***. The dat represents both a complete analysis of all the compla and a sub-sample of those complaints that have been referred to law enforcement. Although IC3's primary mission is to serve as a vehicle to receive, develop, a refer criminal complaints regarding cybercrime, those complaints involving other types of crime such as telephone and mail contact were also referred.

Figure 1: Yearly Comparison of Complaints Received via the IC3 Web s

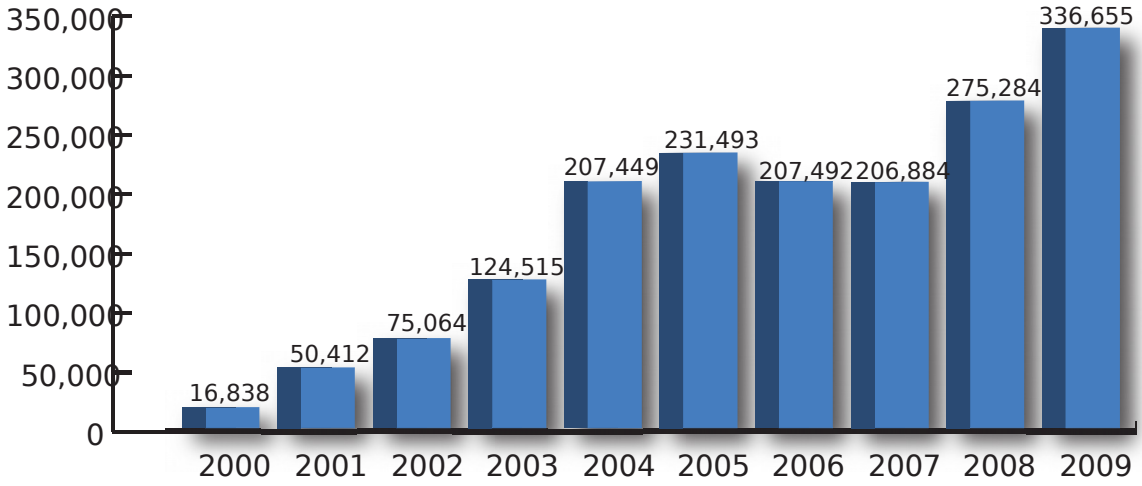


Figure 2: Yearly Dollar Loss (in millions) of Referred Complaints

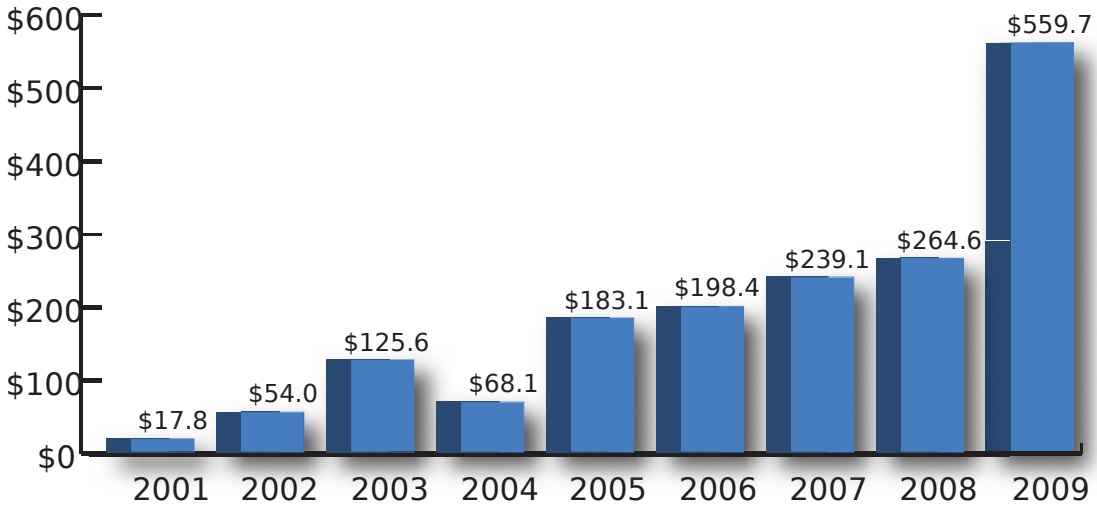
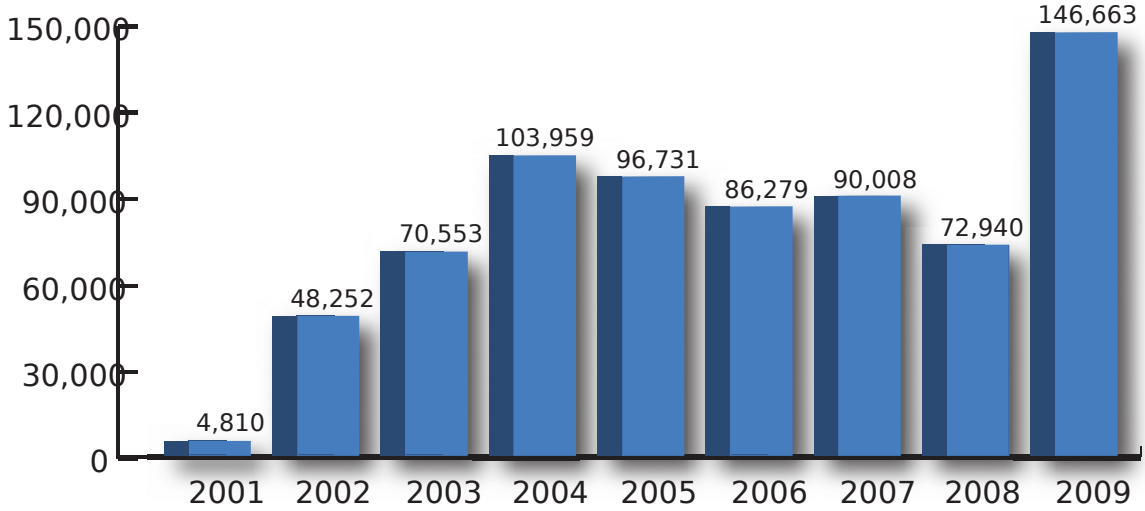


Figure 3: Yearly Number of Referrals



Complaint Characteristics

During 2009, email scams that used the FBI's name was the offense most often reported to IC3, comprising 16.6% of all crime complaints. Non-delivery of merchandise and/or payment represented 11.9% of complaints. Advance fee fraud made up an additional 9.8% of complaints. Other top 10 complaint categories included identity theft (8.2%), overpayment fraud (7.3%), miscellaneous fraud (6.3%), spam (6.2%), credit card fraud (6.0%), auction fraud (5.7%), and destruction/damage/vandalism of computer property, (i.e.,"computer damage," 4.5%) (see Figure 4).

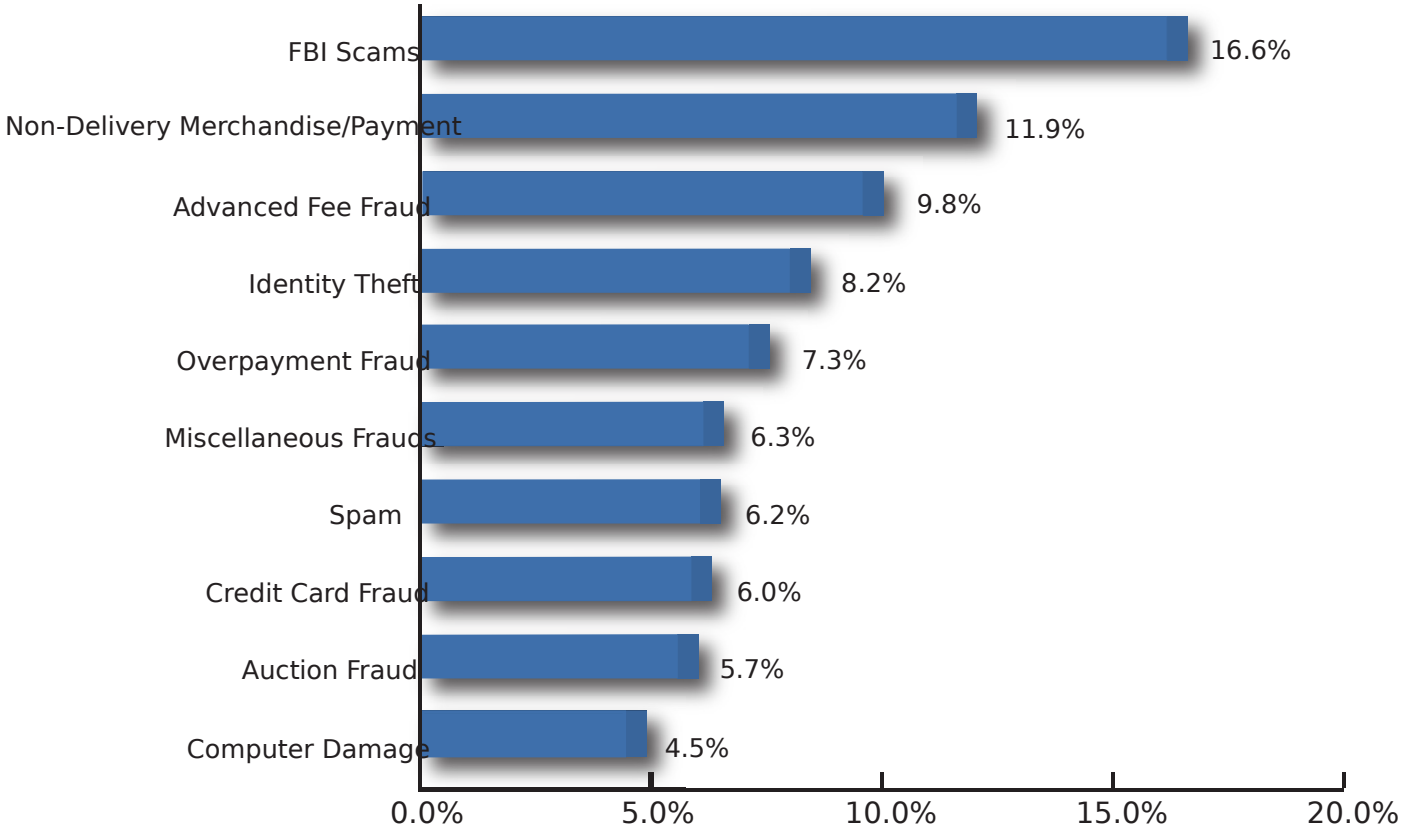
The complaints referred to law enforcement by IC3 were largely those cases involving identifiable loss. That meant certain complaints received in high numbers (e.g. FBI scams) were referred in lower numbers because the complainant's intent was to notify IC3 of the scam rather than report a financial or physical loss.

For a more detailed explanation of complaint categories used by IC3, refer to Appendix I at the end of this report.

Complaint category statistics may not always produce accurate picture of what is occurring. They are based the perception of consumers, and are thus influenced how the complainant characterizes their victimization Two different people may describe the same victimiza in very different ways.

A key area of interest regarding Internet fraud is the monetary loss incurred by complainants cont IC3. Such information is valuable because it provides foundation for estimating average Internet fraud losse the general population. To present information on ave losses, two forms of averages are offered: the mean median. The mean represents a form of averaging fa to the public: the total dollar amount divided by the n of complaints. Because the mean can be sensitive to number of extremely high or extremely low loss comp the median is also provided. The median represents t percentile, or midpoint, of all loss amounts for all com referred to law enforcement. The median is less susce to extreme cases, whether high or low amounts lost.

Figure 4: 2009 Top 10 Most Common IC3 Complaint Categories (Percent Complaints Received)



Of the 146,663 referrals during 2009, 100,296 involved a victim who reported a monetary loss. The total dollar loss from all cases of fraud in 2009 that were referred to law enforcement by IC3 was $559.7 million; that loss was greater than 2008 when a total loss of $264.6 million was reported. Much of this increase can be attributable to a greater number of higher loss complaint categories (e.g., identity theft) relative to auction fraud, which historically has been among the lowest loss offenses. Of those complaints reporting a monetary loss that were referred to law enforcement, the mean dollar loss was $5,580 and the median was $575. The significant difference between the mean and median losses is reflected by a small number of cases in which hundreds of thousands of dollars were reported to have been lost by the complainant.

Over 20 percent (21.7%) of complaints referred to law enforcement involved losses of less than $100, and 36.7% reported a loss between $100 and $1,000. Just over a quarter (28.3%) of the complaints referred to law enforcement reported losses between $1,000 and $5,000 for a grand total of 86.7% of complaints referred to law enforcement showing a loss of $5,000 or less), and 13.3% indicated a loss greater than $5,000 (see Figure 6). The highest dollar loss per referred incident was reported in overpayment fraud (median loss of $2,500) complaints, Investment fraud (median loss of $1,857) and advance fee fraud (median loss of $1,500) complainants were other high dollar loss categories.

Figure 5: 2009 Top 10 Most Referred IC3 Complaint Categories (Percent of Complaints Referred)

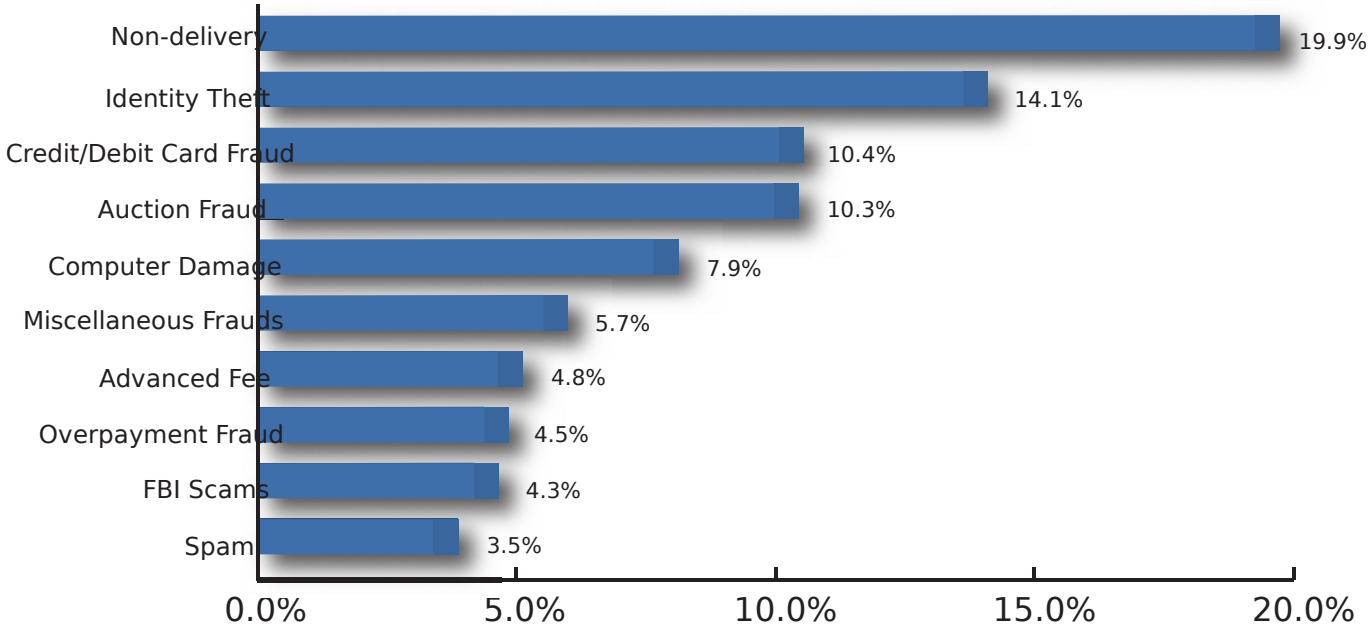
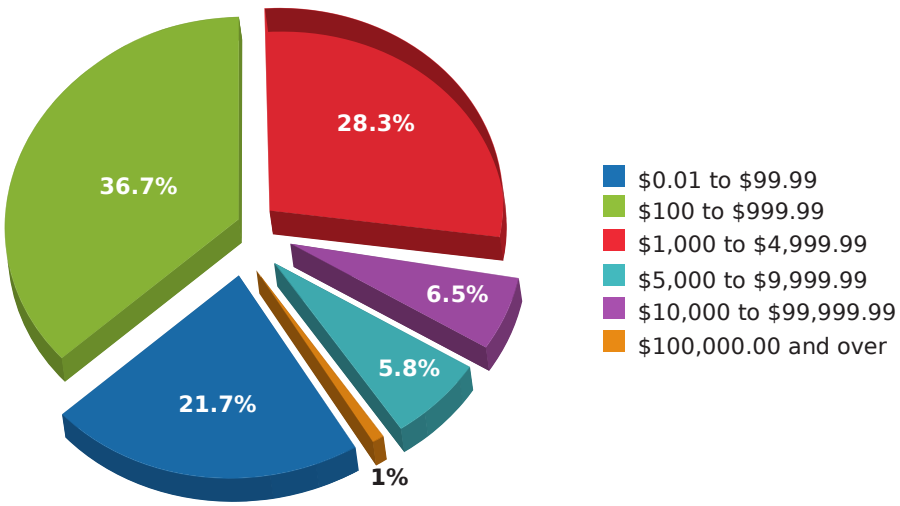


Figure 6: Percent of Referrals by Monetary Loss



Perpetrator Characteristics

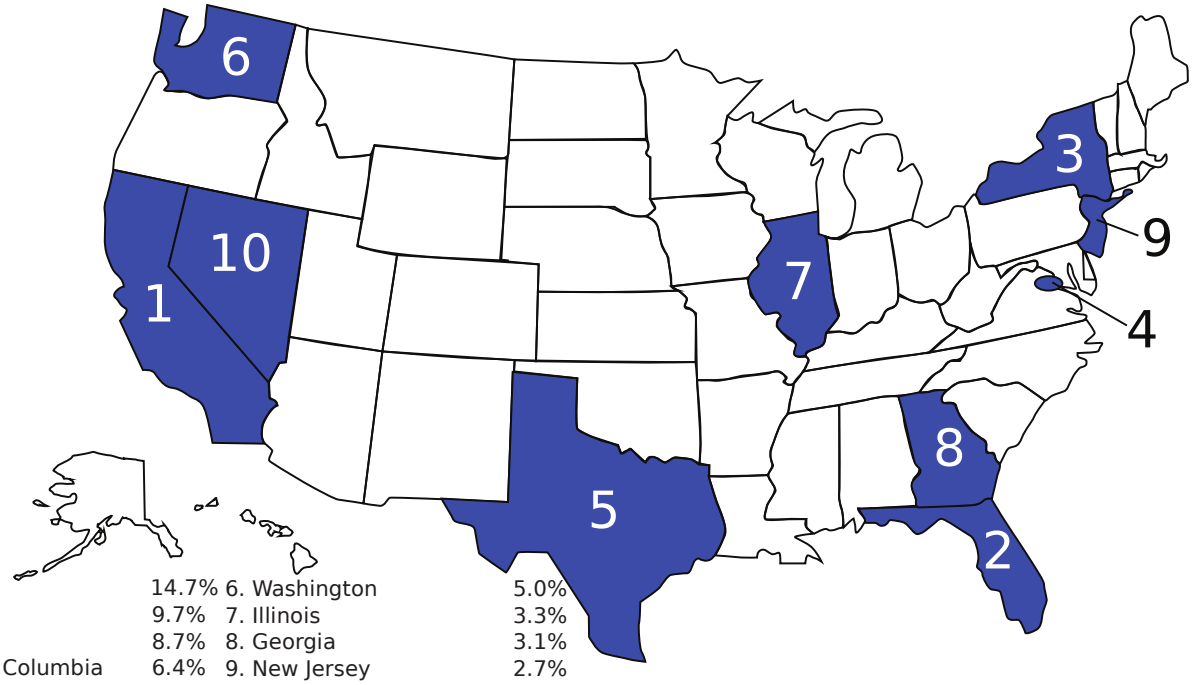
As important as it is to understand the prevalence and monetary impact of cybercrime, it is also vital to gain insight into who the typical perpetrators are. This can prove to be difficult in the world of cybercrime, where a mask of anonymity can impede law enforcement efforts; the gender of the perpetrator was reported only 35.1% of the time, and the state of residence for domestic perpetrators was reported only 38.0% of the time. In those cases in which a complainant was able to provide information about the suspect, over 76% of the perpetrators were male and over half resided in: California, Florida, New York, Texas, Washington and the District of Columbia (see Map 1). The District of Columbia, Nevada, Washington, Montana, Utah, and Florida have the highest per capita rate of perpetrators in the United States (see Table 1). Perpetrators also have been identified as residing in the United Kingdom, Nigeria, Canada, Malaysia, and Ghana (see Map 2). Refer to Appendix III at the end of this report for more information about perpetrator statistics by state. Readers are cautioned to note that throughout this document, perpetrator demographics represents information provided to the victim by the perpetrator and actual perpetrator statistics may vary greatly.

Table 1: Perpetrators per 100,000 People*

Rank	State	Per 100,000 People
1	District of Columbia	116.00
2	Nevada	106.73
3	Washington	81.33
4	Montana	68.20
5	Utah	60.22
6	Florida	57.28
7	Georgia	56.99
8	Wyoming	56.40
9	North Dakota	51.01
10	New York	48.10

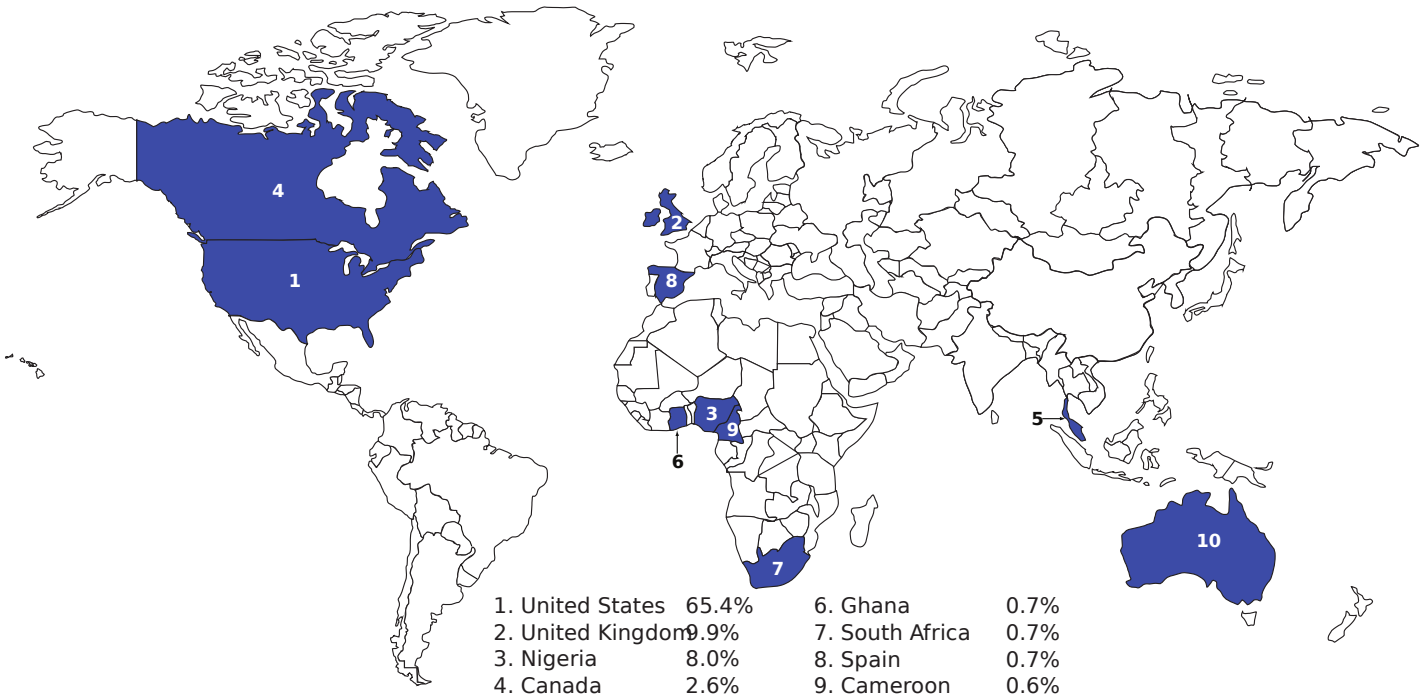
Based on 2009 Census data

Map 1 - Top 10 States by Count: Individual Perpetrators (Numbered by



1. California	14.7%	6. Washington	5.0%
2. Florida	9.7%	7. Illinois	3.3%
3. New York	8.7%	8. Georgia	3.1%
4. District of Columbia	6.4%	9. New Jersey	2.7%
5. Texas	6.4%	10. Nevada	2.6%

Map 2 - Top 10 Countries by Count: Perpetrators (Numbered by Rank)



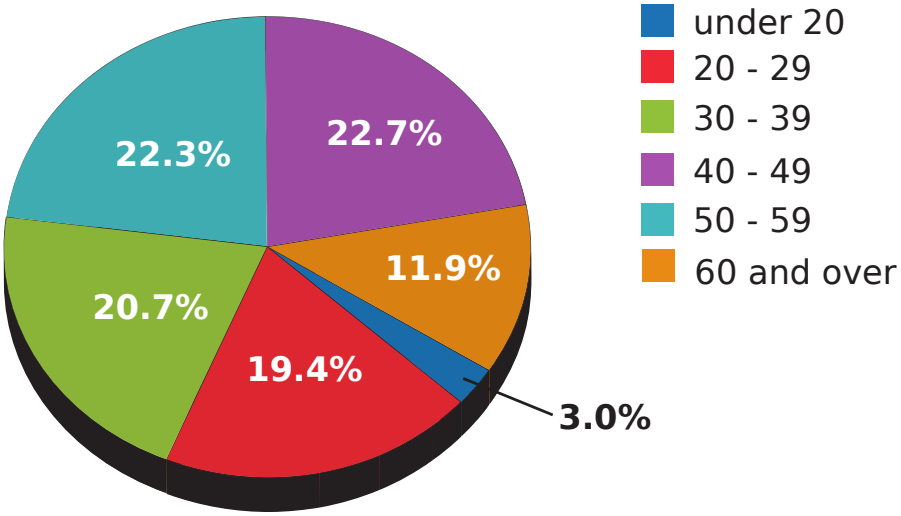
1. United States	65.4%	6. Ghana	0.7%
2. United Kingdom	9.9%	7. South Africa	0.7%
3. Nigeria	8.0%	8. Spain	0.7%
4. Canada	2.6%	9. Cameroon	0.6%
5. Malaysia	0.7%	10. Australia	0.5%

Complainant Characteristics

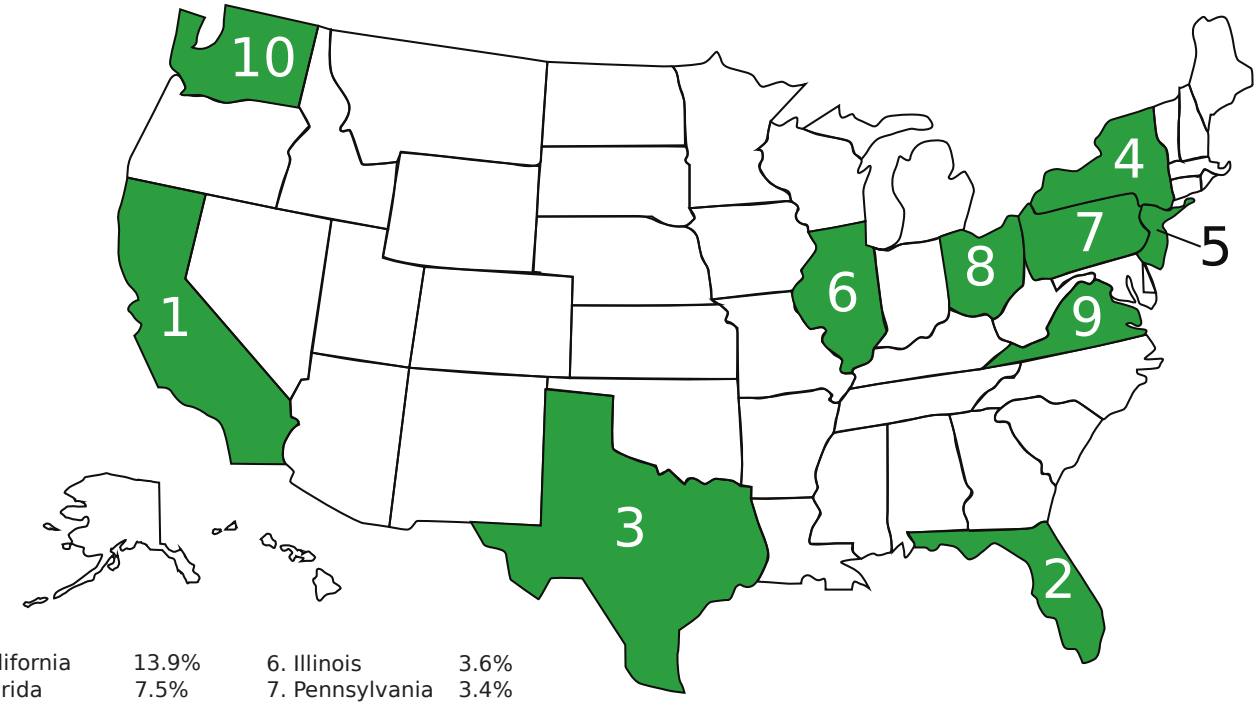
The following graphs offer a detailed description of all individuals who filed a crime complaint through IC3. The average complainant was male, between 40 and 49 (see Figure 7), and likely a resident of one of the four following states: California, Florida, Texas or New York (see Map 3). Alaska, Colorado, Nevada, and the District of Columbia, while possessing a relatively small number of complainants (ranked 44th, 27th, and 47th respectively), had among the highest per capita rate of complainants in the United States (see Table 2). Although most complainants were from the United States, IC3 has also received a number of filings from Canada, the United Kingdom, and Australia (see Map 2).

Table 3 compares differences between the dollar loss per incident and the various complainant demographics. Males reported greater dollar losses than females (ratio of $1.51 to every $1.00). Individuals 40 - 49 years of age reported, on average, higher amounts loss than other age groups.

Figure 7: Age of Complainant



Map 3 - Top 10 States by Count: Individual Complainants (Numbered by



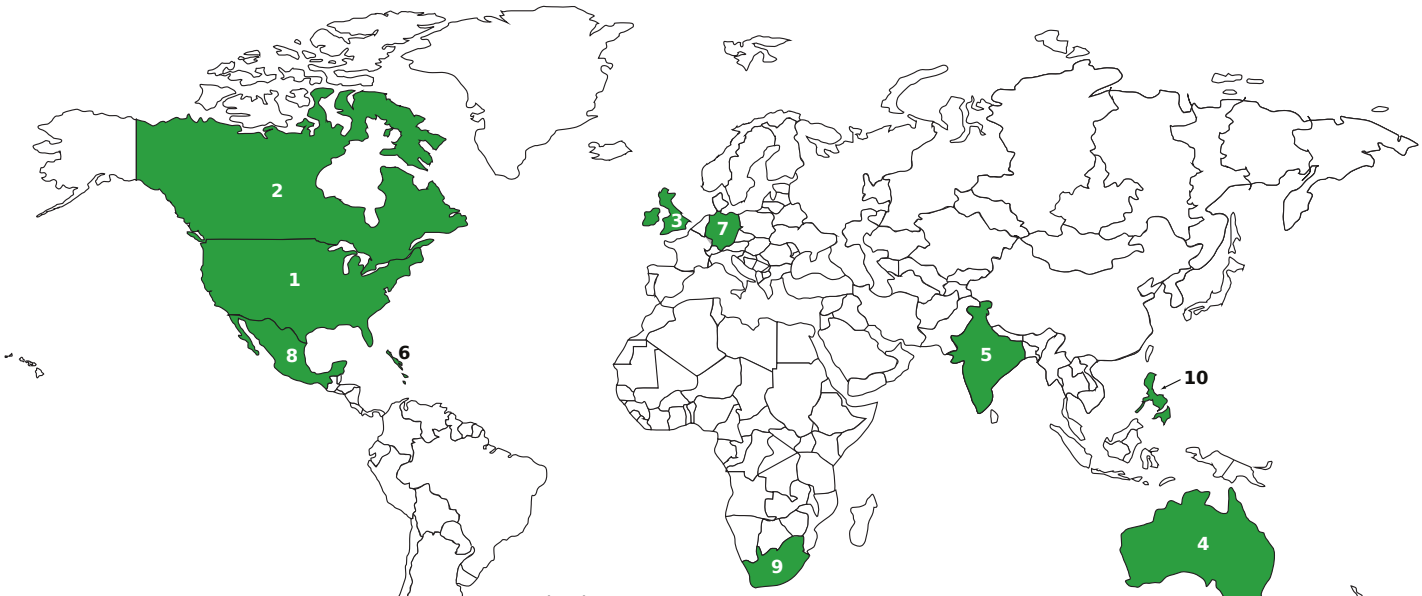
1. California	13.9%	6. Illinois	3.6%
2. Florida	7.5%	7. Pennsylvania	3.4%
3. Texas	7.3%	8. Ohio	3.0%
4. New York	5.2%	9. Virginia	2.9%
5. New Jersey	5.0%	10. Washington	2.8%

Table 2 : Complainants per 100,000 People*

Rank	State	Per 100,000 People
1	Alaska	485.91
2	New Jersey	166.74
3	Colorado	143.21
4	Nevada	135.75
5	District of Columbia	131.90
6	Oregon	124.18
7	Maryland	121.67
8	Arizona	121.01
9	Washington	120.56
10	Florida	116.25

Based on 2009 Census data

Map 4 - Top 10 Countries by Count: Individual Complainants (Numbere



1. United States	92.02%	6. Puerto Rico	0.20%
2. Canada	1.77%	7. Germany	0.17%
3. United Kingdom	0.96%	8. Mexico	0.16%
4. Australia	0.59%	9. South Africa	0.15%
5. India	0.42%	10. Philippines	0.15%

Table 3 : Amount Lost per Referred Complaint Referred to Law Enforcem Complainant Demographics

Complainant Demographics	Average (Median) Dollar Loss Per Referre Complaint
Male	$650.00
Female	$500.00
Under 20	$400.00
20-29	$550.00
30-39	$600.00
40-49	$700.00
50-59	$550.00
60 and older	$500.00

Complainant-Perpetrator Dynamics

One of the components of crime 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 “traditional” crime. This jurisdictional issue often requires the cooperation of multiple agencies to resolve a given case. Table 4 highlights this truly borderless phenomenon. Even in California, in which most of the reported cases originated, only 34.8% of all cases involved both a complainant and perpetrator residing in the same state. Other states h even smaller percentages of complainant-perpetrator similarities in residence. These patterns not only indicate “hot spots” of perpetrators that target poten victims from around the world, but also indicate that complainants and perpetrators may not have had a relationship prior to the incident.

Table 4 : Perpetrators from Same State as Complainant

State	Percent
1. California	34.80%
2. Florida	28.10%
3. New York	24.29%
4. Washington	22.97%
5. Arizona	22.80%
6. Texas	22.26%
7. Nevada	22.20%
8. Georgia	20.95%
9. Delaware	20.91%
10. Massachusetts	20.60%

IC3 Capabilities

Following two years of research, focus-group events, project planning and development, IC3 implemented the Internet Complaint Search and Investigation System (ICSIS), a Web-accessible software solution accessed via a secure, password-controlled Web site. These features make the tool available to any 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, (i.e., i2 Analyst Notebook® link charts) are integrated into the application to supply visual trends and crime patterns within cases including mapping, statistical, and timeline functions.

Searches and case folders 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 receiving notification when new complaints are added that match their criteria, a discussion forum, and user-driven support help and feedback.

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 cases according to each agency's priorities, CMS allows reallocation of human capital for the purpose of improving IC3 services to recipient agencies.

Along with useful productivity tools, IC3 offers analyti staff, ICSIS trainers, and researchers to assist law enforcement with any needs they have regarding cas development. These include: searching and compiling case information, conducting forensic analysis of received data, contacting other agencies that may share interest in collaborative investigations, providin telephonic training support or direct delivery training building link charts, and writing case reports.

Additional Information About IC3 Refe

Although IC3 is dedicated to specifically addressing complaints about Internet crime, it also receives complaints about other crimes. These include violent crimes, robberies, burglaries, threats, and many othe violations of law. The people submitting these types c complaints are directed to make immediate contact w their local law enforcement agency to secure a timely effective response to their particular needs. If warran IC3 personnel may make contact with local law enforcement authorities on behalf of the complainant

Internet Scams of 2009

Hitman Scam

In 2009, IC3 received several complaints presenting a new spin on the media coined "Hitman Scam," a type of email extortion scheme. Victims are reportedly bei threatened in an attempt to extort money. The victim receives an email from a member of an organization such as the "Ishmael Ghost Islamic Group." The emai claims to have been sent to assassinate the victim an the victim's family members. The emailer asserts tha reason for the impending assassination resulted from alleged offense, by the victim, against a member of t emailer's gang. In a bizarre twist however, the emaile reveals that upon obtaining the victim's information, another member of the gang (purported to know a member of the victim's extended family) pleaded for victim's pardon. The emailer alleges that an agreeme was reached with the pleading gang member to allow the victim pardon from assassination, if the victim tak some action such as sending $800 to a receiver in the United Kingdom for the migration of Islamic expatriat from the United States. Victims of this email are typic instructed to send the money via Western Union® or Money Gram® to a receiver in the United Kingdom. The emailer often gives the victim 72 hours to send t money or else pay with his/her life.

Astrological Reading Scam

A familiar scam has resurfaced in which a victim receives spam or pop-up messages offering free astrological readings. The victim must provide his/her birth date and birth location to receive a free reading. After receiving the reading, the victim is enticed to purchase a full reading with the promise that something favorable is about to happen. The victim pays for the full reading but never receives it, and most attempts to contact the "Professional Astrologer," via email, return as undeliverable.

Economic Stimulus Scam

Another popular scam of 2009 involved unsolicited calls regarding fraudulent "government stimulus money." IC3 received numerous complaints from victims receiving unsolicited telephone calls with a recorded message. The recorded voice message reportedly sounds very much like President Barrack Obama discussing allegedly government funds available for those who apply. Victims are warned that the offer is only available for a limited time and are instructed to visit the Web sites ***www.nevergiveitback.com*** or ***www.myfedmoney.com*** to receive their money. These sites require victims to enter personal identifying information after which they are directed to a second page to receive notification of eligibility. Upon completion of an online application and payment of $28 in fees, victims are guaranteed to receive a large sum of stimulus money, but they never do.

Job Site Scams

IC3 has received numerous complaints about work-at-home scams and survey scams related to online job sites. With work-at-home scams, victims fall prey to fraudulent postings for a variety of positions, ranging from personnel managers to secret shoppers. Victims are lured into providing the fraudster with personal identifying information with promises of above average hourly wages or several hundred dollars per week. Some victims are promised the hardware and/or software equipment needed to perform the job. These sites can be so convincing that victims are oftentimes scammed into cashing checks or money orders that they receive; then redistributing a portion of the funds by way of their personal check, cash, money orders, or wire transfers to a third party.

In survey scams, fraudsters post ads for participation in a survey regarding employee/employer relationships during the current economic crisis. Those who apply are required to send a copy of their payroll check as proof of employment. After sending the copy, the victim ne hears from the fraudster again; however, the employ account is drained of thousands of dollars by way of fraudulent checks.

Fake Pop-up Ads for Anti-Virus Software

Other complaints commonly reported to IC3 in 2009 appeared in the form of pop-up ads for rogue anti-viru software. Victims reportedly receive ads warning ther the existence of threatening viruses and/or illegal con allegedly found on the victim's computer. When victim click on the fake pop-ups, malicious code is download onto their computers. Victims are directed to purchas anti-virus software to repair their computers, but in so instances this resulted in viruses, Trojans, or key logg downloaded onto their computers. Attempts to conta the anti-virus software companies were unsuccessful.

Success Stories

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 ca and arrest warrants. IC3 can only gather this data fro the agencies that voluntarily return enforcement resu and it has no authority to require agencies to submit return status forms.

IC3 has assisted law enforcement with many success case resolutions. Some of the cases include the follow

- The Alamance County Sheriff 's Office of North Carolina received a referral from IC3 in April 2009 regarding a series of alleged fraud cases wit an international nexus. At least one of the alleged suspects was residing in their jurisdiction. Accordi to complaints related to this case, the alleged vict posted advertisements on Craigslist and were subsequently contacted by a potential buyer. In al cases, the buyer would pose as a wealthy individu (usually a doctor or CEO) claiming to be out of the country at the time (either in Ireland or Nigeria). The buyer would then send a check for more than the price of the item, requesting that the victim w the remaining funds back to the buyer. Complaints related to this case filed with IC3 culminated in $6,849.99 in reported losses. Currently, this series of investigations is continuing. Other jurisdictions may subsequently become involved. The United States Secret Service is adopting the case for fede prosecution, and the Office of the United States

Attorney will be reviewing aspects of the case. At the time of this release, the following suspects have been arrested and charges have been filed:

Patrick Michael Stone has been charged with 50 counts of forgery of an endorsement; 50 counts of forgery of an instrument; three counts of feloniously accessing a computer (damage or loss in excess of $1,000); 10 counts of common law forgery; and 19 counts of third degree sexual exploitation of a minor. Devon Ashley Crouse was charged with three counts of felonious aiding and abetting. Eddie Leon Watkins has been charged with one count of obtaining property by false pretense. He was placed under a $1,000 secured bond.

- In July 2009, NW3C was contacted by Detective Rick Arias of the Miami Beach Police Department, Miami Beach, Florida, requesting an investigative search on the name Michael Reece. This search initially turned up two complaints. Detective Arias responded by providing additional information that may be linked to Reece's activities, including email addresses, aliases, and alleged victims. The case was referred to IC3. After expanding the search criteria, IC3 analysts were able to build a case against Reece that spanned 16 cases with $31,167.50 in reported losses. According to the filed complaints, Reece, using the aliases Joe Essels, John Mills, and Michael Seren, listed ads on Craigslist for vacation rental properties. After the victims signed and mailed the contracts for the properties, Reece would then coerce victims to send him deposits that ranged from $1,000 to $4,000. The victims would not receive any further contact from him. Using this information, Detective Arias was able to arrest Michael Reece on July 31, 2009, marking the third arrest of Reece by Detective Arias.

- In July 2009, IC3 referred a case to the New York State Police Department regarding a series of alleged thefts. The case involved 13 complaints totaling $17,243.95 in losses. The suspect businesses involved were East Coast Engines, Auto Computer Tech, and Muscle Sports and Imports, all in Altamont, New York. According to the complaints, victims alleged that they had sent items to the owner for repair/upgrade, but services were not performed and items were not returned. Additionally, a number of complainants paid for parts but did not receive them. Investigator Paul Ruckert contacted IC3 in October 2009 with an update. Subject Jeff Roberts with Auto Computer Tech was arrested for Grand Larceny/Fraud by the Albany County Sheriff and the New York State Police.

- The Derby Police Department, Derby, Kansas received a referral from IC3 regarding suspect Lorraine Robles. Complainants alleged that they had purchased cra items online but did not receive the merchandise. The case contained six complaints with a total loss $352. Robles was charged with computer crime an the case was filed in the District Court.

- In November 2009, IC3 sent a case to the Tampa Police Department, Tampa, Florida regarding suspe James Diebold. A few days prior, a victim contacte IC3 about the suspect. Other victims with similar complaints were found in the ICSIS database. The complainants alleged that Diebold sold them ticke for everything from sporting events to theme park but did not deliver about $3,500 in goods after the payments were received. Diebold was arrested on November 20, 2009 by the Tampa Police Departm and charged with organized crime and third-degre grand theft.

- In April 2009, IC3 created a case with involving 10 complaints totaling $362,465.18 in losses. Victims this case purchased vehicles through both Craigsli and eBay®, sending their payment through a bog eBay® financing center agent. The perpetrator suggested that the victim use this eBay® financin center, claiming that it served the same function a PayPal®. The financial services appeared legitima and even contained the eBay® logo. Once the vic wired the money to the bogus "eBay®" agent, the funds were lost and the victims did not receive the product. In July 2009, Sergeant Scott Dugan of the Reno Police Department, Reno, Nevada contacted IC3 to inform them that an arrest had been made.

- IC3 sent a case to the Broward County Sheriff's Of Fort Lauderdale, Florida in May 2009 regarding the suspected business owner of Godfather Motors. Vi purchased motorcycles but did not receive them a payment was made. The Sheriff's Office sent an u in November 2009 indicating that the owner, Sam Paniaqua, was arrested in June 2009 for 3rd Degre Grand Theft and is in federal custody in Miami, Flo After additional research, it was determined that t perpetrator, in fact, owned another company in wh complaints had been lodged.

Conclusion

In 2009, IC3 implemented significant updates and changes to 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 Web site and complaint form were implemented in January 2009. The new data collection method has afforded IC3 a greater opportunity to examine all complaints through a unique categorization system that specifically assigns any complaint to one of 79 complaint types regardless of referral status, unlike the previous system.

The 2009 IC3 report has outlined many of the current trends and patterns in cybercrime. This data indicates that reports of cybercrime are increasing. Annual crime complaints reported to IC3 have increased 667.8% when comparing data from the 2001 annual report with 2009. Complaint submissions for 2009 were 336,655, a (22.3%) increase from 275,284 in 2008, and a (62.7%) increase from 206,884 complaints in 2007. This total includes many different complaint types, including both fraudulent and non-fraudulent crimes. 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 dollar loss from all cases of crime referred to law enforcement totaled $559.7 million, up from $264.6 million in 2008.

Non-delivered merchandise and/or payment represents the offense that was most referred to law enforcement, followed by identity theft accounted credit card fraud. Of those complaints that were referred to law enforcement in which a dollar loss was reported, the highest median losses were found among investment fraud ($3,200), overpayment fraud ($2,500), and advanced fee fraud ($1,500). Male complainants reported greater losses than female complainants.

Although this report can provide a snapshot of the prevalence and impact of cybercrime, it is worth noting that knowledge of the “typical” victim or perpetrator of these types of crimes does not imply that atypical Internet users are safe, or that atypical individuals do not commit Internet crimes. Anyone who uses the Internet is susceptible. IC3 has received complaints from both males and females ranging in age from 10 to 100. Complainants can be found in all 50 states including the District of Columbia and in dozens of countries worldwide. They 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 use or experience), many organizations agree that education and awareness are major tools to protect individuals. Some individuals may find themselves the victims of computer-related criminal activity even when following the best prevention strategies. Various consumer alerts, tips and fraud trends can be accessed via ***www.lookstoogoodtobetrue.com***, a Web site to help provide the educational tips consumers need to protect themselves.

References

1. *National White Collar Crime Center, The National Public Survey on White Collar Crime, August 2006*

appendix - I

Methodology

IC3 made a number of changes to the way it gathers and classifies complaint data. Beginning January 1, 2009, IC3 implemented a new complaint classification. This system is based on an updated questionnaire, designed to capture data on various aspects of a complaint and generate an automatic classification in terms of the complaint's offense content.

Prompting the redesign of the classification system were criticisms of the previous system's ability to protect validity and reliability. The previous system had as many as 157 complaint categories; many of which were either vague, non-mutually exclusive, or both. The application of these categories produced inconsistencies and classification errors, making it difficult to discern the prevalence of certain types of victimization. The new classification system was designed to minimize such errors.

Although a degree of overlap among complaint categories is unavoidable because of an array of factors—including the multi-faceted nature of complaints, subjective interpretations of incidents, and IC3's adherence to the Hierarchy Rule—the new classification system improves upon the previous system by making clearer distinctions and by reducing the number of categories used to classify complaints. The new system uses a fixed set of 79 categories, representing nearly a 50% reduction in the number of categories. For reporting purposes these 79 categories are collapsible into 27 main complaint types. The intent behind this reduction in categories was to reduce the likelihood of classification error, thus protecting data validity.

The automated classification process also achieves a level of reliability that could not be attained by the previous system. Under the previous system, manual sorting of complaints added another layer of subjective interpretation to the classification procedure, leading to inconsistencies in measurement. Under the new system, responses to survey questions yield a sequence of data values translated by the system into one of 79 complaint types, each corresponding to a unique numeric code. Systematic field tests conducted in January and February 2009 show the new system to be both reliable and accurate in classifying complaints. Since then, IC3 has made only minor changes to the questionnaire to clarify survey questions for complainants.

An effort was also made to make IC3 data more compatible with the National Incident-Based Reporting System (NIBRS). For example, "Destruction/Damage/Vandalism of Property" is a NIBRS Group "A" Offense, defined as "To willfully or maliciously destroy, damage, deface, or otherwise injure real or personal property without the consent of the owner or the person having custody or control of it." In the new IC3 classification system, this category is used to classify complaints involving crimes that target and cause damage to computers, or "true computer crimes." Definitions of the Top 10 complaint types reported in 2009 can be found in Appendix II.

The introduction of the new classification system creates discontinuities between the 2009 IC3 report and all previous reports. For instance, "FBI Scams" is a new category that was created to capture instances of unsolicited email containing fraudulent messages from FBI personnel. In previous reports, such complaints would have been classified as either "spam" or "threat," depending on the level of information concerning the email content contained in the complaint. The flood of complaints involving fake FBI email received by IC3 in recent years elicited greater attention from law enforcement. This growing concern justified the creation of a separate category to distinguish these complaints from those involving spam or other kinds of threat. It should be noted that as new crime trends surface, IC3 may, in response to these developments, create new complaint categories to capture information deemed useful to law enforcement agencies in addressing emergent patterns of victimization. Such changes in the classification system will be duly noted in the annual report.

If you are interested in conducting a longitudinal study of IC3 data that includes data from 2009, special care

must be taken to adjust the data so that the 2009 report is compatible with previous reports. Please contact Research Manager John Kane at ***jkane@nw3c.org*** for assistance.

ICSIS

At the same time the new classification system was introduced, IC3 also implemented a new data storage and retrieval system, the Internet Complaint Search and Investigation System (ICSIS). In addition to storing IC3 complaint data, ICSIS incorporates search and analytical tools that allow users to mine complaint data and develop cases. Among the applications available to users is the "fuzzy logic" search tool. This tool enables users to collate complaints that have identical or nearly identical user-specified parameters such as the names and addresses of suspects. This application is especially useful in building cases against repeat offenders who alter fragments of their identity information to avoid positive identification by law enforcement.

ICSIS also facilitates collaboration between investigat Research on cases that span multiple jurisdictional boundaries. Users may not only search the database complaints to build their own cases; they may also se case folders created by other users who are intereste similar, if not the same, complaints. Users converging the same modus operandi may then communicate wi each other through the internal messaging service an coordinate efforts to further investigate far-flung crim enterprises. Such networking and sharing of informat across jurisdictions may bring cases into sharper focu and expedite their disposition. With its fuzzy logic sea tool and information-sharing capabilities, ICSIS has the potential to revolutionize the way law enforcemen officers fight Internet-facilitated crime.

References

1. *Federal Bureau of Investigation. 2000. Uniform Cr Reporting: National Incident-Based Reporting Syst Washington, D.C.:GPO, p. 25.*

appendix - II

Definitions of Top 10 Complaint Types

1. **FBI Scams** – Scams in which it appears that the FBI is trying to get something from the complainant (e.g., money, identity information, etc.).
2. **Advance Fee Fraud** – An incident involving communications that would have people believe that to receive something, they must first pay money to cover some sort of incidental cost or expense.
3. **ID Theft** – An incident in which someone stole or tried to steal an identity (or identity information), but only when there is no other discernible crime involved (e.g., credit card theft).
4. **Non-Delivery of Merchandise (non-auction)** – An incident in which the complainant bought something, but it never arrived.
5. **Overpayment Fraud** – An incident in which the complainant receives an invalid monetary instrument, with instructions to deposit it in a bank account and to send excess funds or a percentage of the deposited money back to the sender.
6. **Miscellaneous Fraud** – Incidents involving a fraudulent attempt to get the complainant to s money and where nothing is bought or sold.
7. **SPAM** – Unsolicited and unwelcome email, usually mass distributed.
8. **Credit Card Fraud** – An incident in which someone is attempting to charge goods and se to the complainant's credit card or account.
9. **Auction Fraud** – A fraudulent transaction or exchange that occurs in the context of an onlin auction site.
10. **Computer Damage (Destruction/Damage/ Vandalism of Property)** – This category is use to classify complaints involving crimes that target and cause damage to computers, or "tru computer crimes."

Table 5 - Complainant Categories and Subcategories

Complaint Types
Advanced Fee Fraud
Auction Fraud
Auction Fraud - Consumer Complaint
Auction Fraud - Fake
Auction Fraud - Forged or Counterfeit Payment
Auction Fraud - Fraudulent Refund
Auction Fraud - Insufficient Funds
Auction Fraud - No Such Account
Auction Fraud - Non-Delivery
Auction Fraud - Non-Payment
Auction Fraud - Other
Auction Fraud - Payment Fraud - Other
Auction Fraud - Stolen
Auction Fraud - Stolen Payment
Unauthorized Auction Purchases

Complaint Types
Blackmail/Extortion
Blackmail
Extortion/Hitman Emails
Charity Fraud
Consumer Complaint (non-auction)
Counterfeiting/Forgery
Spoofing
Non-Auction - Forged or Counterfeit Payment
Non-Auction - Fraudulent Refund
Non-Auction - Delivery of Fake Product
Credit Card Faud
Destruction/Damage/Vandalism of Property (i.e. Property Crime)
Adware
Computer Abuse (other or unknown)
Computer Virus
Spyware
Theft of Computer Services (where offense almost invariably involves computer hacking)
Hacking
Account Hacking
Drug/Narcotic Offenses
Drug Trafficking
Trafficking in Prescription Drugs
Employment Fraud
FBI Scams
Gambling Offenses
Online Gambling
Crooked Gambling
ID Theft
Identity Theft - Trafficking in Identifying Information
Identity Theft
Illegal Business
Misc. Illegal Business
Trafficking in Illegal Goods (selling things that are stolen or counterfeit)
Intimidation (non-terrorist-related threats and cyber-stalking)
Other Threatening Behavior
Threat
Cyber-Stalking/Forum Abuse
Investment Fraud
Investment Fraud
Pyramid Schemes
Non-Delivery of Merchandise (non-auction)
Miscellaneous Fraud

Complaint Types
Miscellaneous Fraud
Non-Auction Consumer Fraud - Other
Overpayment Fraud
Payment Fraud (bad checks, insufficient funds or no such account, but not counterfeited or forged methods of payment)
Non-Auction Non-Payment Fraud (other)
Non-Auction - Non-Payment
Non-Auction - Stolen Payment
Non-Auction - No Such Account
Non-Auction - Insufficient Funds
Unauthorized Purchases (use of credit card)
Pornography/Obscene Material
Child Pornography
Obscenity
Making Available Sexually Explicit Materials to Minors
Sexual Solicitation/Obscene Communications with Minors
Transmitting Obscene Materials to Minors
Sexual Abuse
Sexual Harassment
Sexual Offenses - Other
Luring/Traveling
Prostitution (NIBRS: Prostitution Offenses)
Relationship Fraud
Rental Fraud
Rental Fraud - Not Their House
Rental Fraud - Other
Rental Fraud - Overpayment
SPAM
Stolen Property Offenses
Music Piracy
Software Piracy
Non-Auction - Sale of Stolen Goods
Online Copyright Infringement
Terrorist Threat (5 subcategories)
Terrorist Threat
Terrorist (other)
Terrorist Funding
Terrorist Information
Terrorist Recruiting

appendix - III

Complainant/Perpetrator Statistics by State

Table 6 - 2009 Complainants by State*

Rank	State	Percent	Rank	State	Percent
1	California	13.9%	27	Alaska	1.2%
2	Florida	7.5%	28	Louisiana	1.2%
3	Texas	7.3%	29	Kentucky	1.0%
4	New York	5.2%	30	Oklahoma	0.9%
5	New Jersey	5.0%	31	Connecticut	0.9%
6	Illinois	3.6%	32	Kansas	0.9%
7	Pennsylvania	3.4%	33	Utah	0.9%
8	Ohio	3.0%	34	Arkansas	0.7%
9	Virginia	2.9%	35	Iowa	0.7%
10	Washington	2.8%	36	New Mexico	0.6%
11	Arizona	2.8%	37	Mississippi	0.5%
12	Georgia	2.7%	38	Idaho	0.5%
13	North Carolina	2.6%	39	West Virginia	0.5%
14	Colorado	2.5%	40	New Hampshire	0.5%
15	Maryland	2.4%	41	Hawaii	0.4%
16	Michigan	2.3%	42	Nebraska	0.4%
17	Tennessee	1.9%	43	Maine	0.4%
18	Indiana	1.9%	44	Montana	0.3%
19	Massachusetts	1.8%	45	Rhode Island	0.3%
20	Missouri	1.8%	46	Delaware	0.3%
21	Oregon	1.7%	47	District of Columbia	0.3%
22	Minnesota	1.4%	48	Vermont	0.2%
23	Wisconsin	1.3%	49	Wyoming	0.2%
24	Alabama	1.3%	50	South Dakota	0.1%
25	Nevada	1.3%	51	North Dakota	0.1%
26	South Carolina	1.2%			

**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 statis from 50 states and the District of Columbia. The table above does not represent statistics from other U.S. territories or Canada.)

Table 7 - 2009 Perpetrators by State*

Rank	State	Percent	Rank	State	Percent
1	California	14.7%	27	Alabama	0.8%
2	Florida	9.7%	28	Wisconsin	0.8%
3	New York	8.7%	29	South Carolina	0.8%
4	District of Columbia	6.4%	30	Louisiana	0.7%
5	Texas	6.4%	31	Kentucky	0.7%
6	Washington	5.0%	32	Oklahoma	0.7%
7	Illinois	3.3%	33	Montana	0.6%
8	Georgia	3.1%	34	Iowa	0.6%
9	New Jersey	2.7%	35	Kansas	0.6%
10	Nevada	2.6%	36	Delaware	0.5%
11	Arizona	2.5%	37	Nebraska	0.4%
12	Ohio	2.4%	38	Arkansas	0.4%
13	Pennsylvania	2.4%	39	Idaho	0.4%
14	North Carolina	2.0%	40	Maine	0.4%
15	Michigan	1.9%	41	New Mexico	0.4%
16	Colorado	1.9%	42	Hawaii	0.4%
17	Virginia	1.8%	43	Mississippi	0.3%
18	Maryland	1.6%	44	North Dakota	0.3%
19	Utah	1.5%	45	West Virginia	0.3%
20	Tennessee	1.4%	46	Wyoming	0.3%
21	Massachusetts	1.4%	47	New Hampshire	0.3%
22	Indiana	1.3%	48	South Dakota	0.2%
23	Missouri	1.3%	49	Alaska	0.2%
24	Minnesota	1.1%	50	Rhode Island	0.2%
25	Connecticut	0.9%	51	Vermont	0.2%
26	Oregon	0.9%			

**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 statis from 50 states and the District of Columbia. The table above does not represent statistics from other U.S. territories or Canada.)

Table 8 - Complainants per 100,000 People*

Rank	State	Per 1,000	Rank	State	Per 1,000
1	Alaska	485.91	27	Indiana	82.74
2	New Jersey	166.74	28	Georgia	79.56
3	Colorado	143.21	29	Massachusetts	79.34
4	Nevada	135.75	30	North Carolina	78.95
5	District of Columbia	131.90	31	Alabama	78.83
6	Oregon	124.18	32	Illinois	78.60
7	Maryland	121.67	33	Michigan	78.23
8	Arizona	121.01	34	Rhode Island	78.80
9	Washington	120.56	35	Pennsylvania	78.20
10	Florida	116.25	36	West Virginia	76.32
11	California	107.56	37	Connecticut	76.05
12	Virginia	103.76	38	New York	75.62
13	New Hampshire	101.24	39	South Carolina	75.39
14	Hawaii	97.82	40	Ohio	75.05
15	Idaho	94.77	41	Minnesota	74.03
16	Delaware	93.43	42	Louisiana	73.46
17	Wyoming	92.78	43	Oklahoma	73.33
18	Vermont	92.64	44	Arkansas	70.63
19	New Mexico	90.06	45	Wisconsin	67.99
20	Utah	89.99	46	Nebraska	65.51
21	Montana	89.12	47	Kentucky	65.39
22	Kansas	89.04	48	Iowa	64.99
23	Tennessee	88.22	49	North Dakota	57.81
24	Missouri	85.47	50	South Dakota	51.82
25	Texas	84.09	51	Mississippi	51.21
26	Maine	83.89			

**Based on 2009 Census figures*

Table 9 - Perpetrators per 100,000 People*

Rank	State	Per 1,000	Rank	State	Per 1,000
1	District of Columbia	116.60	27	Oregon	25.17
2	Nevada	106.73	28	Virginia	24.12
3	Washington	81.33	29	Tennessee	23.20
4	Montana	68.20	30	Massachusetts	23.12
5	Utah	60.22	31	Minnesota	22.93
6	Delaware	57.28	32	Missouri	22.89
7	Florida	56.99	33	Rhode Island	22.88
8	Wyoming	56.40	34	Ohio	22.80
9	North Dakota	51.01	35	North Carolina	22.75
10	New York	48.10	36	Indiana	21.60
11	California	43.16	37	Kansas	21.49
12	Arizona	40.45	38	Iowa	21.37
13	Colorado	40.36	39	New Hampshire	21.13
14	Alaska	35.36	40	Michigan	20.57
15	Georgia	34.04	41	Pennsylvania	20.36
16	New Jersey	33.63	42	Oklahoma	19.74
17	Maine	33.52	43	New Mexico	19.60
18	South Dakota	31.63	44	Alabama	18.79
19	Maryland	29.72	45	South Carolina	18.45
20	Hawaii	29.10	46	Kentucky	17.45
21	Idaho	29.04	47	Louisiana	16.98
22	Texas	28.02	48	West Virginia	16.92
23	Connecticut	27.96	49	Arkansas	15.95
24	Illinois	27.84	50	Wisconsin	15.15
25	Nebraska	26.71	51	Mississippi	12.19
26	Vermont	26.69			

**Based on 2009 Census figures*

The 336,655 complaints represent an all-time high in reported submissions to IC3 and account for a total loss of nearly $727 million. The median loss per complaint totaled $508, somewhat less than that reported for complaints that were referred to law enforcement. The large difference between the total loss figure of all complaints and referred complaints is due in large to complaints in which neither the complainant nor perpetrator resides within the United States. This accounts for the vast majority of non-referred complaints. However, a minority of those cases could not be referred, because the agencies to whic they would otherwise be referred required a minimum threshold to be met before accepting the complaints.

www.ic3.gov