2013 Internet Crime Report

Table of Contents

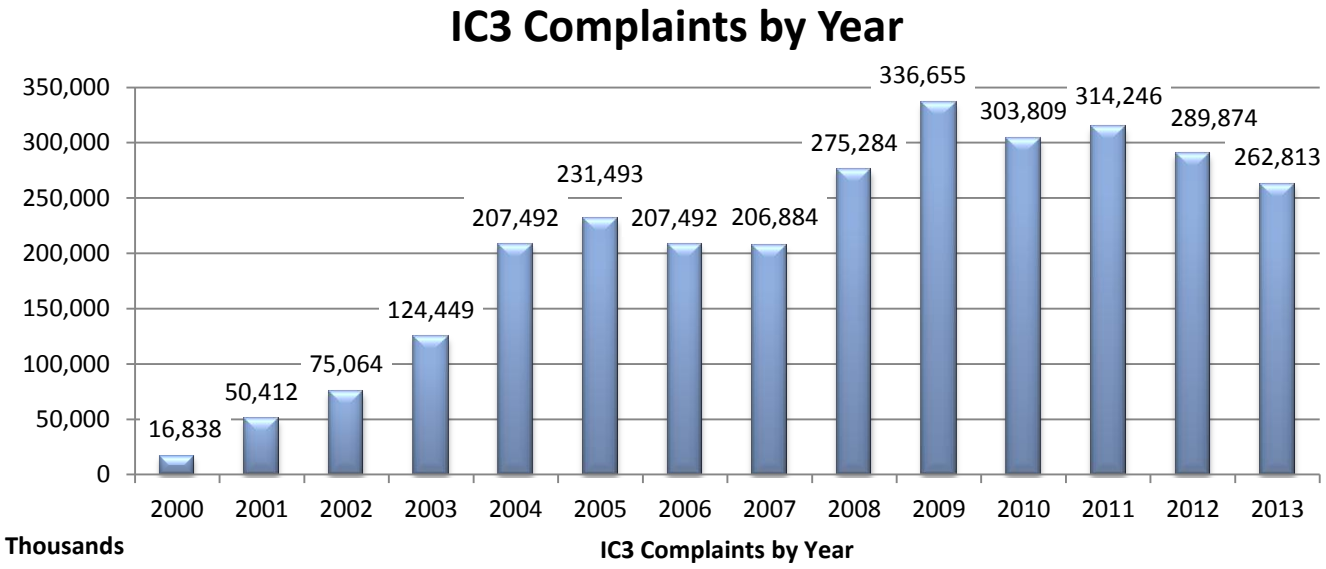
Mission: *To receive, develop and refer criminal complaints regarding the rapidly expanding arena of cybercrime. The Internet Crime Complaint Center (IC3) gives the victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities to suspected criminal violations. For law enforcement and regulatory agencies at the federal, state, local, tribal and international levels, the IC3 provides a central referral mechanism for complaints involving Internet-related crimes.*

2013 Internet Crime Report

Executive Summary

Now in its 14th year of operation, the Internet Crime Complaint Center (IC3) has firmly established its role as a valuable resource for both victims of Internet crime and law enforcement agencies investigating and prosecuting these crimes. For the victims, the IC3 provides a convenient and easy-to-use reporting mechanism that alerts authorities to suspected criminal violations. For law enforcement agencies, the IC3 serves as a conduit to receive Internet-related complaints, to conduct research related to them and to develop analytical reports for state, local, federal, tribal or international law enforcement and regulatory agencies. These agencies then develop investigations based on the forwarded information as appropriate. In 2013, the IC3 received 262,813 consumer complaints with an adjusted dollar loss of $781,841,611[1], which is a 48.8 percent increase in reported losses since 2012 ($581,441,110). The IC3 continues its efforts to inform the general public about online scams by publishing public service announcements and providing tips for Internet consumers.

The IC3's success attracts international interest. Canada, the United Kingdom and Germany use the IC3 as a model for similar cybercrime centers. In furtherance of its continuing support of foreign law enforcement, the IC3 prepared dozens of country-specific statistical reports and disseminated hundreds of complaint referrals to FBI legal attaché offices throughout the world. In 2014, the IC3 continues to pursue its mission to serve both the online public and law enforcement and regulatory agencies throughout the entire global community.



[1] Method of evaluating loss amounts: FBI IC3 Unit staff reviewed for validity all complaints that reported a loss of more than $100,000. Analysts also converted losses reported in foreign currencies to U.S. dollars. The final amounts of all reported losses above $100,000 for which the complaint information did not support the loss amount were excluded from the statistics.

Project Partners

As a threat-based and intelligence-driven national security organization, the mission of the Federal Bureau of Investigation (FBI) is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States and to provide leadership and criminal justice services to federal, state, municipal and international agencies and partners.

The mission of the National White Collar Crime Center (NW3C) is to provide training, investigative support and research to agencies and entities involved in the prevention, investigation and prosecution of economic and high-tech crime. While the NW3C has no investigative authority itself, its job is to help law enforcement agencies better understand and utilize tools to combat economic and high-tech crime. The NW3C has other sections within its organization, including Training (in Computer Crime, Financial Crime and Intelligence Analysis), Research and Investigative Support Services. The NW3C is funded by an annual Congressional appropriation through the Bureau of Justice Assistance.

The IC3

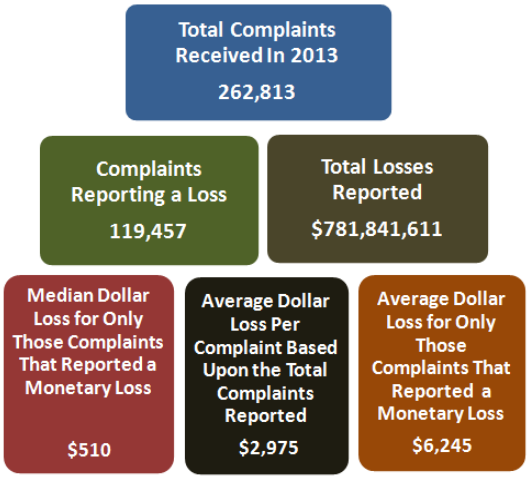
The IC3 is a valuable resource for both victims of Internet crime and the law enforcement agencies identifying, investigating and prosecuting these crimes. For the victims, the IC3 provides a convenient and easy-to-use reporting mechanism that alerts authorities to suspected criminal violations. For law enforcement agencies, the IC3 serves as a conduit to receive Internet-related complaints, to conduct research related to them and to develop analytical reports based on them for state, local, federal, tribal or international law enforcement and regulatory agencies. These agencies then develop investigations based on the forwarded information, as appropriate.

262,813

Complaints Reported to the IC3 in 2013

How it Works

Victims file complaints with the IC3, which go into an extensive database. The IC3's analysts review individual complaint data, identifying and grouping complaints with similar information. These complaints are collated and referred to state, local, federal, tribal and international law enforcement for potential investigation. Analysts also collect relevant case information from both open and closed sources. The IC3 analysts use automated matching systems to identify links and commonalities between numerous complaints and combine the respective complaints into referral groups for law enforcement. Of the 262,813 complaints received in 2013, 45.5 percent (119,457) reported financial loss.



The IC3 offers remote access capability, making data available to law enforcement anywhere. This Web-based access provides users the ability to aggregate victims and losses to substantiate criminal activity within the agency's area of jurisdiction and to enhance development of cases. Although the IC3 may not immediately build all complaints into referrals, all complaints are helpful in identifying trends and building statistical reports. These trends are posted on the IC3's website (www.ic3.gov) as public service announcements in a continuing effort to educate the general public on constantly evolving cyber scams and crime. The IC3 encourages victims of Internet crime to report all incidents to the IC3 – whether or not an actual dollar loss is involved – due to the broad dissemination and varied uses of the data gathered from the complaints.

2013 Complainant Demographics

The following graphs represent the complaint counts according to gender, age, and the associated losses along with maps showing the relative state and country ranking of complaints received by the IC3 during 2013. Previous years' trending has shown equalization between the genders in the number of IC3 complaints with 2013 count numbers closely associated with the same trend. These numbers reflect a trend in recent years in which the number of male and female complainants is equalizing. In 2013, there was a minimal increase in complaints reported to the IC3 by men compared to complaints reported by women in 2012.

Gender	Count	Percentage
Male	137,096	52.27%
Female	125,717	47.73%

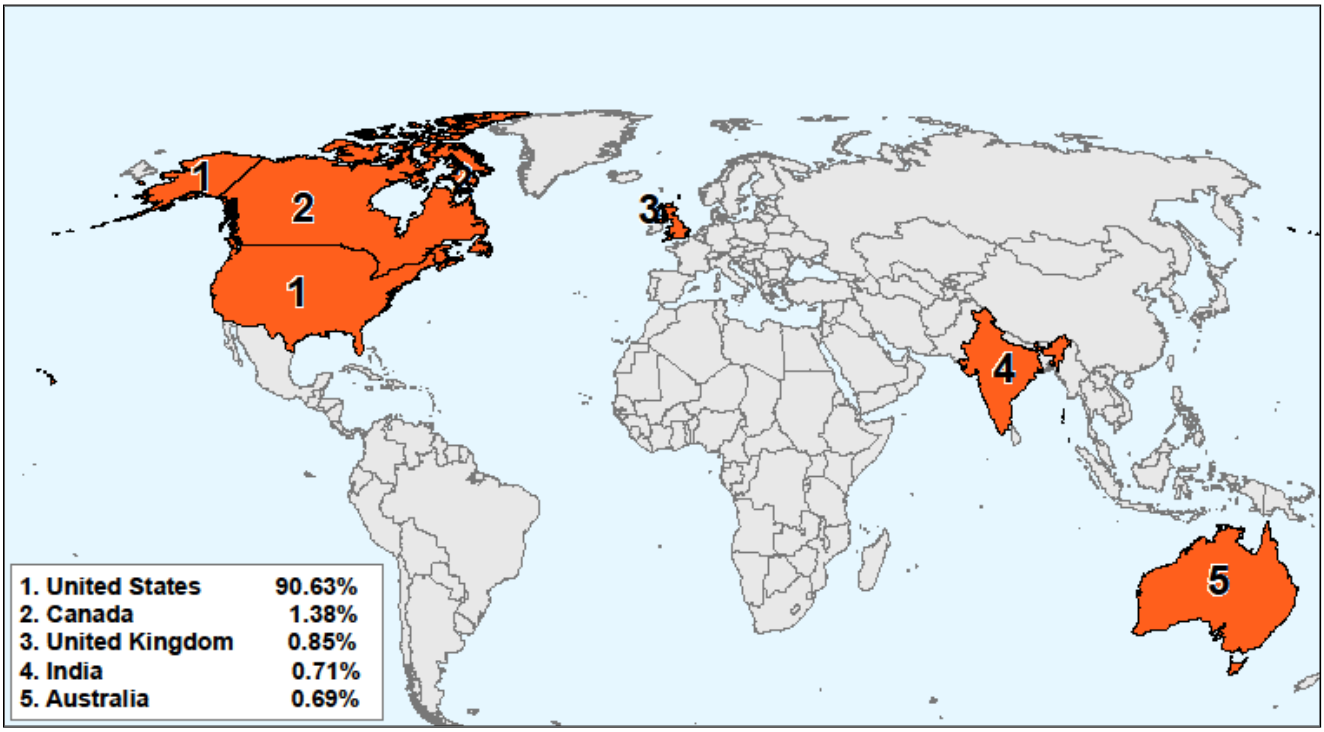
Age	Count	Percentage
Under 20	8,796	3.4%
20 – 29	48,032	18.3%
30 – 39	54,780	20.8%
40 – 49	55,838	21.2%
50 – 59	55,459	21.1%
Over 60	39,908	15.2%

Overall Age Gender 2013 Statistics

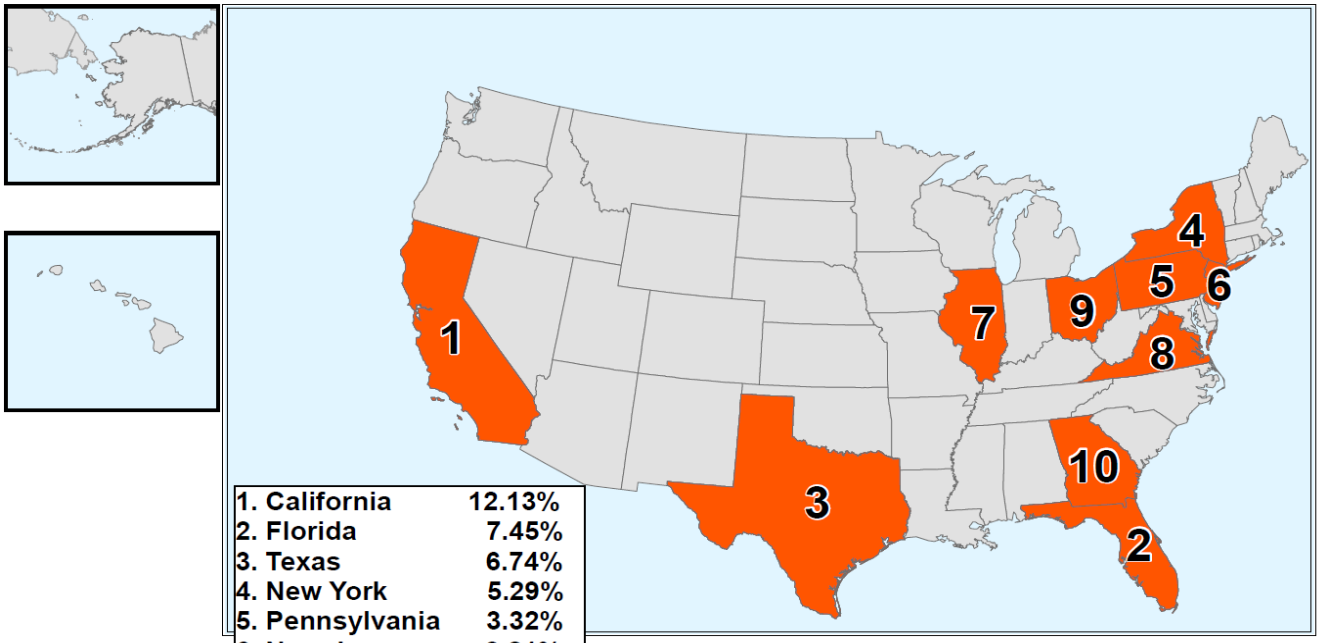
Age Range	Male Count	Male Loss	Female Count	Female Loss	Total Complaints	Total Combined Losses
Under 20	5,194	$103,298,649	3,602	$2,364,515	8,796	$105,663,164
20 – 29	24,549	$42,144,452	23,483	$23,619,502	48,032	$65,763,954
30 – 39	28,391	$71,022,425	26,389	$41,784,048	54,780	$112,806,473
40 – 49	26,668	$89,559,205	29,170	$70,355,407	55,838	$159,914,612
50 – 59	29,220	$93,705,383	26,239	$83,858,340	55,459	$177,563,723
Over 60	23,074	$87,244,816	16,834	$72,884,870	39,908	$160,129,686
Totals	137,096	$486,974,929	125,717	$294,866,681	262,813	$781,841,611

The maps on the following page demonstrate the top five countries and the top 10 states ranked by the number of victim complaints reported to the IC3 during 2013.

Top Five Countries Ranked by the Total Number of Complaints Received by IC3 in 2013



Top Ten States Ranked by the Total Number of Complaints Received by IC3 in 2013



Note: 10.09% of the complaints did not include location information

Internet Scams Reported to the IC3

The IC3 continues to receive a wide variety of complaints on a multitude of crime schemes. The true volume and scope of cyber crime is unknown. What is known is that criminals continue to use a variety of scams to defraud Internet users. These schemes range from simple frauds to complex hacking and malicious software or malware scams. Some recurring and common crime schemes include:

Auto-Auction Fraud – The IC3 has received a significant number of complaints regarding Internet auction fraud involving the sale of automobiles. Many of these listings are for vehicles located outside the United States. In most cases the criminal attempts to sell vehicles they do not own. Criminals create attractive deals by advertising vehicles at prices below book value. Often criminals claims they must sell the vehicle because they are moving or being relocated for work. Due to the pending move, the criminals often refuse to meet with potential buyers or allow vehicle inspections and ultimately try to rush the sale. In an attempt to make the deal appear legitimate, the criminal often instructs victims to send full or partial payments to third-party agents via wire transfers and to fax their payment receipt to the seller as proof of payment. Once payment is made, the criminal pockets the money and the victim never receives the vehicle.

Vehicle Scam Gender/Age Demographics 2013

Age Range	Male Complaints	Losses	Female Complaints	Losses	Total Complaints	Total Combined Losses
Under 20	281	$522,024	260	$461,060	541	$983,084
20 – 29	1,503	$3,770,671	1,189	$2,276,657	2,692	$6,047,328
30 – 39	1,812	$7,007,766	1,139	$3,440,037	2,951	$10,447,803
40 – 49	1,988	$8,338,286	1,141	$4,386,862	3,129	$12,725,148
50 – 59	2,146	$9,178,111	1,000	$3,316,403	3,146	$12,494,513
Over 60	1,312	$7,165,709	398	$1,717,925	1,710	$8,883,634
Totals	9,042	$35,982,566	5,127	$15,598,944	14,169	$51,581,511

Romance Scams – The IC3 continues to receive complaints of romance scams in which scammers target individuals searching for companionship or romance online. Victims believe they are "dating" a good and honest person without ever physically meeting them. The online contact is often a criminal sitting in a cyber café with a well-rehearsed script used to repeatedly and successfully scam others. Perpetrators of these scams search chat rooms, dating sites, and social networking sites looking for potential targets. Although all demographics are at risk, the group targeted the most appears to be people aged 40 years and older, divorced, widowed, disabled, and often elderly.

Romance scammers use poetry, flowers, and other gifts to draw in their victims. They continuously declare their "undying love" for victims. These criminals also use stories of severe life circumstances, tragedies, family deaths, injuries to themselves, or other hardships to keep their victims concerned and involved in their schemes. Scammers also ask victims to send money to help overcome alleged hardships.

Romance Scam Demographics 2013

Age Range	Male Complaints	Losses	Female Complaints	Losses	Total Complaints	Total Combined Losses
Under 20	24	$5,530	18	$4,335	42	$9,865
20 – 29	247	$461,821	194	$568,389	441	$1,030,210
30 – 39	375	$1,833,507	578	$3,668,135	953	$5,501,642
40 – 49	433	$5,614,225	1,454	$14,240,923	1,887	$19,855,148
50 – 59	479	$5,059,941	1,598	$26,036,044	2,077	$31,095,984
Over 60	240	$3,231,036	772	$21,072,285	1,012	$24,303,320
Totals	1,798	$16,206,058	4,614	$65,590,111	6,412	$81,796,169

FBI Scams – Perpetrators attempt to intimidate victims in emails by purporting to be high ranking government officials. Many scams exploit the FBI name or the names of FBI executives such as the current FBI Director, James Comey, and FBI former Director Robert Mueller, both of which had terms as the FBI's Director during 2013. There were 4,391 complaints reported to the IC3 in 2013 that referenced both FBI Directors. The FBI specific schemes typically remain the same as scammers just update their scam verbiage to reflect the current FBI Director's name. FBI impersonation schemes pose a viable threat to national security by undermining public trust that directly impacts law enforcement's ability to do its job. Government agencies do not send unsolicited e-mails of this nature. While FBI, Department of Justice and other United States government executives are briefed on numerous investigations, they do not personally contact consumers regarding such matters. United States government agencies use the legal process to contact individuals. These agencies do not send threatening letters or e-mails to consumers demanding payments for Internet crimes. The total FBI related scams reported to the IC3 during 2013 is represented in the chart below.

FBI Scams Age Gender 2013 Statistics

Age Range	Male Complaints	Losses	Female Complaints	Losses	Total Complaints	Total Combined Losses
Under 20	94	$22,311	34	$4,245	128	$26,556
20 – 29	524	$72,576	377	$61,842	901	$134,418
30 – 39	681	$348,461	677	$131,169	1,358	$479,630
40 – 49	996	$387,747	983	$368,372	1,979	$756,119
50 – 59	1,408	$1,369,661	1,185	$1,145,591	2,593	$2,515,252
Over 60	1,451	$972,837	759	$1,464,070	2,210	$2,436,907
Totals	5,154	$3,173,593	4,015	$3,175,288	9,169	$6,348,881

Hit Man Scam – The IC3 continues to receive reports about a hit man/extortion e-mail scheme. The scheme has been around for several years but the content used in the e-mailed messages changes. The ultimate goal is for the perpetrators to defraud people through disturbing e-mails. The scam originated as a person sending an e-mail portraying himself as a hit man hired to kill the victim. The e-mail instructs the recipient to pay a fee to remain safe and avoid having the hit carried out. Although the e-mail content is disturbing, the IC3 has not received any reports of the loss of life.

Hitman Scams Age Gender 2013 Statistics

Age Range	Male Complaints	Losses	Female Complaints	Losses	Total Complaints	Total Combined Losses
Under 20	9	$1,092	6	$15	15	$1,107
20 – 29	25	$2,529	28	$2,272	53	$4,801
30 – 39	52	$135,841	110	$34,893	162	$170,734
40 – 49	70	$134,770	101	$664,623	171	$799,393
50 – 59	93	$34,284	105	$865,258	198	$899,542
Over 60	121	$5,805	52	$59,826	173	$65,631
Totals	370	$314,321	402	$1,626,887	772	$1,941,208

Ransomware/Scareware Scams – The IC3 has received multiple complaints surrounding ransomware /scareware schemes. These schemes are used to target and extort funds from victims by intimidating them. These scams began years ago with false claims in which the perpetrators pretended to be federal government officials who were watching or monitoring the victims' Internet usage. Schemes continue to change and some of the most reported schemes involve those discussed below.

- Cryptolocker Ransomware – The IC3 became aware of the CryptoLocker scheme in October 2013. It spreads via e-mail and propagates rapidly. The virus encrypts various file types and then a pop-up window appears on victims' computer that states their data has been encrypted. The only way to get it back is to send a specified monetary payment to the perpetrator. This ransomware provides the victim with a timeline to pay via a displayed countdown clock. If victims do not pay on time, they lose the ability to pay and risk having their data permanently encrypted and rendered unusable. Perpetrators are demanding a $300 to $700 payment sent to the perpetrator using various methods.

- Child Pornography Scareware – This scareware is transmitted when computer users visit an infected website. The victim's computer locks up and displays a warning that the user has violated U.S. federal law. Child pornography is either embedded in a banner image that appears on the victims' screen or revealed via an automatic browser redirecting them to a child pornography website. The scareware is used as an extortion technique by threatening prosecution for visiting or viewing these images. The victim is also informed that they have been recorded using audio, video and other devices. The only way to unlock the computer is to pay the fine, usually between $300 and $5,000.

- Citadel Ransomware – The Citadel ransomware, named Reveton, displays a warning on the victims' computer purportedly from a law enforcement agency claiming that their computer had been used for illegal activities, such as downloading copyrighted software or child pornography. To increase the illusion they are being watched by law enforcement, the screen also displays the victim's IP address and some victims even report activity from their webcam. Victims are instructed to pay a fine to the U.S. Department of Justice to unlock their computer. Many were told to pay the fines via prepaid cash services such as Ucash or Paysafecard. In addition to installing the ransomware, the Citadel malware continues to operate on the compromised computer to collect sensitive data that could potentially be used to commit a variety of financial frauds.

- Fake or Rogue Anti-Virus Software – In this scheme victims are scared into purchasing anti-virus software that would allegedly remove viruses from their computers. A pop-up box appears that informs users that their computers are full of viruses and need to be cleaned. The pop-up message has a button victims can click to purchase anti-virus software that supposedly can immediately get rid of these viruses. If the victims click the pop-up to purchase the anti-virus software, they are infected with malware. In some instances, victims have been infected regardless of clicking on the pop-up box.

Ransomware Scams Age Gender 2013 Statistics

Age Range	Male Complaints	Losses	Female Complaints	Losses	Total Complaints	Total Combined Losses
Under 20	29	$1,005	14	$5	43	$1,010
20 – 29	95	$17,546	55	$1,980	150	$19,526
30 – 39	91	$160,580	71	$15,930	162	$176,510
40 – 49	116	$116,998	108	$2,648	224	$119,646
50 – 59	122	$211,234	87	$2,255	209	$213,489
Over 60	143	$7,969	60	$1,412	203	$9,381
Totals	596	$515,332	395	$24,230	991	$539,562

Real-Estate Rental Scams – Perpetrators search websites that list homes for sale and take information from legitimate ads and post it with their own e-mail addresses on online advertising sites. The houses are usually listed with below-market rental rates to immediately attract potential victims. Those interested contact the perpetrator via e-mail. The perpetrator usually tells some story about having to leave the area quickly due to employment or volunteer work. Many claim they left the United States for missionary or contract work in Africa. Victims are usually instructed to send money overseas—enough to cover the first and last month's rent—via a wire transfer service. In some cases the perpetrators require potential renters to fill out credit applications so they can obtain personal information, e.g., credit history, employment history, Social Security number and any number of other crimes.

Real Estate Scam Age Gender 2013 Statistics

Age Range	Male Complaints	Losses	Female Complaints	Losses	Total Complaints	Total Combined Losses
Under 20	45	$33,021	108	$66,398	153	$99,419
20 – 29	874	$642,457	1,485	$990,078	2,359	$1,632,534
30 – 39	940	$1,031,101	1,445	$981,793	2,385	$2,012,894
40 – 49	812	$893,720	1,326	$2,161,027	2,138	$3,054,747
50 – 59	815	$1,895,945	1,214	$2,399,689	2,029	$4,295,635
Over 60	662	$3,402,049	658	$4,077,148	1,320	$7,479,197
Totals	4,148	$7,898,293	6,236	$10,676,133	10,384	$18,574,426

Grandparent Telephone Scams – Perpetrators target elderly individuals by claiming to be a grandson, granddaughter, or other relative in desperate need of legal or financial assistance. Most schemes involve claims of being arrested or in some type of accident. The callers create a sense of urgency and make desperate pleas for money. The caller begs the grandparents not to tell the parents while often crying to help prevent the potential victims from discovering the scam. Once potential victims appear to believe the caller, they are provided instructions to wire money to an individual, often referred to as a bail bondsman, for their grandchild to be released by law enforcement. Investigations have determined potential victims were identified via mass-produced lead lists that target specific demographics. Perpetrators were identified using telephone numbers generated by free apps to make the phone calls. This seems to be an added attempt to convince the grandparents the call is legitimate (by displaying a recognizable number on the caller ID) and an attempt to mask the real telephone number they are using to make it harder for law enforcement to investigate.

Timeshare Marketing Scams – Timeshare owners across the country are being scammed out of millions of dollars by unscrupulous companies that promise to sell or rent their properties. In the typical scam, timeshare owners receive unexpected telephone calls or e-mails from criminals posing as sales representatives for timeshare resale companies. The representatives promise quick sales, often within 60 to 90 days. The sales representatives frequently use high-pressure sales tactics to add a sense of urgency to the deal. Some victims have reported that sales representatives pressured them by claiming they already had a buyer waiting, either on another line or even in their office. Timeshare owners who agree to sell are told they are required to pay an up-front fee to cover

anything from listing and advertising fees to closing costs. These costs are usually paid via credit card and range from hundreds to thousands of dollars. Once the fee is paid, timeshare owners report that the company becomes evasive as calls go unanswered, numbers are disconnected and websites are inaccessible. In some cases, timeshare owners who have been defrauded by a timeshare sales scheme have been subsequently contacted by an unscrupulous timeshare fraud recovery company as well. The representative from the recovery company promises assistance in recovering money lost in the sales scam. Some recovery companies require up-front fees as well for services rendered. The IC3 has identified some instances in which people involved with the recovery company also have a connection to the resale company, raising the possibility that timeshare owners are being scammed twice by the same perpetrators.

Work-at-Home (Employment) Scams – Work-at-home scams continue to be very successful as more and more people turn to the Internet to look for jobs. Poor economic conditions lead people in financial hardships to accept any job they are offered. Although many work-at-home victims are unwitting in their participation in these scams, others are witting participants. Regardless, these individuals can face criminal charges and, potentially, prosecutions. Victims of work-at-home scams are often recruited by organized cyber criminals through newspaper ads, online employment services, unsolicited e-mails or "spam," and social networking websites. Victims of work-at-home schemes become "mules" for cyber criminals who use their financial accounts to steal and launder money.

Software Company Telephone Scams – Victims of these telephone scams began receiving calls from individuals allegedly claiming to be from legitimate, well-known software companies. The victims are advised that malware detected on their computer poses an impending threat. The fraudsters tried to instill a feeling of urgency so victims would take immediate action and log in to their computers. Once the victims did so, the fraudsters directed them to the utility area of the computers, where they appeared to demonstrate how the computers were infected. The fraudsters offered to rid the computers of the malware for fees ranging from $49 to $450. When the victims agreed to pay the fees, they were directed to a website where they entered a code or downloaded a software program that allowed the fraudsters remote access to their computers.

Payday Loan Scams – In the payday loan scam or loan intimidation scam, the perpetrator relentlessly attempts to contact victims via their home, cell and work phone numbers. Victims are told they are delinquent on a payday loan and must repay the loan to avoid legal consequences. The caller fraudulently impersonates being a representative of the FBI, Federal Legislative Department, law firms, or other legitimate-sounding agencies. They claim to be collecting debts for companies such as United Cash Advance, U.S. Cash Advance, U.S. Cash Net, and other Internet check-cashing services. They refuse to provide the victim with any details of the alleged payday loans and often become abusive when questioned. The callers threaten victims with legal actions, arrests and, in some cases, physical violence if they refuse to pay. In many cases, the callers even resort to harassment of victims' relatives, friends, and employers. What makes these schemes so successful is the perpetrator's use of accurate information about the victims, including Social Security numbers, dates of birth, addresses, employer information, bank account numbers, names and sometimes even telephone numbers of relatives and friends. How the fraudsters obtain the personal information is unclear, but victims often relay that they had completed online applications for other loans or credit cards before the calls began.

Loan Modification Scams – A loan modification scam often starts when a bogus loan company contacts a distressed homeowner via phone, e-mail or mailing, and offers them a loan modification plan. In some cases the victim may have initiated the contact by reaching out to these companies after seeing an advertisement. The loan modification typically includes a lower interest rate, an extension in the length of the loan term, a change in the type of loan or any combination of the three.

As a part of this scam, the company instructs the homeowner to cease all communication with lenders and stop making mortgage payments until the loan modification process is complete. The homeowner is required to send money to cover "processing fees" and "closing costs" for the new loan to be processed and approved. After the homeowner sends the money, the loan modification company stops its communications with victims, leaving the homeowner behind on actual mortgage payments and unable to recover funds sent to the bogus company.

Sextortion Scams – Perpetrators of these scams often initiate conversation via social media websites and/or online dating websites. Once a rapport has been established, victims are asked to engage in video chats in which they are manipulated to expose themselves in sexually compromising situations, while their images are secretly recorded.

Subjects then threaten to make the videos available to all the victims' social networking friends and other online contacts unless funds, ranging in the amounts of $50 to $300, are wired to various destinations.

Gun Sale Scams – Fraudsters begin this scam by enticing victims into purchasing firearms by advertising them below market value. They post advertisements using photos and bogus descriptions lifted from legitimate firearm ads. Most complaints reported to the IC3 involved the sale of rifles or long guns. The perpetrators normally ask the victim to e-mail or fax them a copy of a photo ID to make the sale appear more legitimate. The scammers seem to know gun transfer procedures because they obtain federal firearm license transfer information from the victim and pretend to set up the transfer. The victim purchases the gun but never receives it. Victims have lost hundreds to thousands of dollars with this scam to date.

Fraudulent Tech Support Call Scams – Perpetrators of these scams contact victims via phone and impersonate tech support employees from various legitimate companies (e.g., Dell, Microsoft, Western Union, etc.). In some cases the company name is displayed on the victims' caller ID. The callers usually instruct the victims to get online to visit specified web sites the scammers controls. Many ask victims to download files or run various applications that either provide the caller with remote access to the victims' computer or infect it with malware. If remote access is established, the victims are instructed to open and log-in to various accounts to allow the caller to update the system. The victims are then told to turn off their monitors to avoid interference with the update. The victims later discover that the subjects have made wire transfers out of their accounts.

Photo and Mug Shot Scam – Scammers post photos or mug shots of individuals to extort money. Some victims have reported they were juveniles at the time of the arrest and the information should be sealed, while others complain the information is fakery or completely made up. Regardless, the photos and information are posted to sites such as www.bustedmugshots.com, www.mugshots.com, www.justmugshots.com, or www.unpublishmugshots.com. Complainants who request to have their mug shot removed must provide a copy of their driver's license, court record and other personal identifying information. This provides the perpetrator with information they can use for a variety of other crimes. Other complainants have paid removal fees but unfortunately never had their mug shots deleted. If they were removed, the mug shots appeared on similar websites.

College and University Scams – The IC3 has identified two scams involving college or universities. In the first scam the perpetrators register domains similar to domains owned by well-known colleges and universities. Once similar domains are registered, they establish an e-mail address that appears to be from the purchasing department of a legitimate institution. Using logos and information obtained from the home page of the legitimate school, the fraudsters create fake purchase orders or requests for quotations and place orders with various merchants for items such as routers, toner, or hard drives. The merchandise is shipped to various locations so that other scam participants can re-package and re-ship items to overseas locations, usually Nigeria. The second scam involves spear-phishing e-mails that are sent to university employees to dupe them into giving up their log-in credentials to the schools' websites. Once the fraudsters access the website, they can click on an online airline ticket booking tool to purchase airline tickets with compromised credit cards or use credit cards already set up for that account. Itinerary receipts are e-mailed to Yahoo!/Google/Hotmail accounts rather than the accounts with ".edu" extensions.

SIM Card Swap Scam – Subscriber Identification Module (SIM) swap fraud occurs when an individual compromises or steals the SIM card from a cell phone. This card can provide perpetrators with personal identification, cell phone information (number, provider, etc.), and the ability to contact the carrier to request a new SIM card. When the perpetrator receives and activates the new SIM card, the victim's card is deactivated. Victims may notice their phone will no longer transmit messages or calls. All alerts, payment confirmations, and other various messages are then transmitted to the fraudster. SIM swapping is sometimes the second phase of the scam. Initially, the perpetrator will send phishing emails to obtain credit card or bank account information. If the perpetrator receives enough information, he/she can wipe out bank accounts, run up credit cards, and even open new accounts or create fraudulent identification documents.

The scams above are just some of the Internet fraud schemes the IC3 received in 2013. This is by no means a comprehensive list of Internet crimes, but it provides information on some of the most common schemes criminals are using to defraud the public. A detailed list of common schemes is available at http://www.ic3.gov/crimeschemes.aspx. The IC3 also regularly posts fraud alerts detailing newly identified scams

reported to IC3 by law enforcement, industry and online complainants. These alerts are available at: http://www.ic3.gov/media/default.aspx.

IC3 Case Highlights

Grand Theft: Polk County Florida Sheriff's Office

The IC3 provided complaints to the Polk County Sheriff's Office in December 2009. The monetary losses totaled $15,114. In January 2010, the Polk County Sheriff's Office advised the IC3 that its agency initiated an investigation against Jack Loftin. The complainants advised they purchased concert tickets from the subject, but never received them or a refund of their monies. Most of the victims established initial contact with the subject through an eBay auction website. Many of the victims utilized PayPal as the medium for payment. An affidavit released by the Office of the State Attorney, 10th Judicial Circuit stated the subject tricked people into thinking he had VIP tickets for performers like Jimmy Buffet, Miley Cyrus or Aerosmith. The subject was charged with pocketing $92,000 from victims across the country and not providing tickets or refunds. Loftin pleaded guilty to 24 counts of grand theft in November 2012 and was sentenced to 16 months imprisonment and ordered to pay $87,000 in restitution on Jan. 18, 2013. He was also sentenced to 13 years probation during which time all restitution to victims must be paid.

"Your agency provided crucial information that was utilized to locate the victims exploited by Jack Loftin. Because of your assistance, our office was able to have a successful prosecution which resulted in a state prison sentence and an order of restitution to the victims in this case."

David W. Lyon, Investigator
Office of the State Attorney
10th Judicial District
Bartow, Florida

Wire Fraud: United States Secret Service (USSS)

The IC3 has been working with USSS in Springfield, Ill., since March 2008 regarding a subject in a wire fraud investigation. The subject, Chris Sours, advertised Internet-based businesses for sale, collected large sums of money but did not provide legitimate websites to his customers. According to the USSS, victims have sent amounts ranging from $2,000 to $45,000. The IC3 found related complaints from October 2005 to February 2012. Total dollar loss from these complaints was $257,966. On November 13, 2012, Chris Sours was arrested, pled guilty, and was indicted. On April 13, 2013, Chris Sours was sentenced to 60 months incarceration and ordered to pay $343,233 in restitution in the Central District of Illinois, Rock Island, Illinois.

High Yield Investment Fraud: FBI, Southern District of Florida

The IC3 provided multiple complaints with a monetary loss of $390,889 to various FBI field offices in July 2007. The complainants reported that Kerry Deevy and his co-conspirators fraudulently induced purchasers to buy into fake business opportunities. Kerry Deevy and his co-conspirators purported to sell vending machines and greeting card businesses, including assistance in establishing, maintaining and operating such businesses. The companies were operating as Cards-R-Us, Premier Cards Inc., and Nation West. These business opportunities cost thousands

of dollars, and most victims paid at least $10,000 each. Kerry Deevy used various means to make it appear these companies were located in the United States, including registering the corporations and renting office space to make the scheme more authentic. In reality, the subject was operating from Costa Rica.

On April 11, 2013, the subject pleaded guilty in the U.S. District Court for the Southern District of Florida to 13 counts of an indictment, charging him with conspiracy to commit mail and wire fraud, mail fraud, and wire fraud. The subject was charged in connection with the operation of a series of fraudulent business opportunities after being indicted in November 2012 by a federal grand jury. Following his arrest, the subject was extradited to the United States for prosecution. The subject was sentenced to 60 months in prison and five years' supervised release on Aug. 13, 2013 and ordered to pay $4,541,914 in restitution.

Nigerian Romance Scam: Colorado Attorney General's Office

Between March 2010 and October 2011, the IC3 received complaints from individuals who reported they were defrauded via the Internet by Karen and Tracy Vasseur, a mother-daughter pair. The victims established relationships with the subjects through online dating services and social networks. Often the subjects purported to be overseas for military service. After trust had been built, the subjects began asking for funds to aid in purchasing better cellular phones and technology. Funds were also supposedly being used for leave or military time-off travel. Although funds were sent via MoneyGram and direct bank wires, the relationships were not maintained as promised. Victims reported a combined monetary loss of $34,670.

The Colorado Attorney General's Office opened a case in February 2012. Subsequent searches of the IC3 complaint database revealed an additional 126 complaints for a combined monetary loss of $130,673. It is believed that Karen and Tracy Vasseur collected funds, kept a percentage, and then wired the remainder to unknown Nigerian bosses. On Aug. 28, 2013, the subjects were sentenced for convictions stemming from a "Nigerian Romance Scam."

Counterfeit Check Scheme: Federal Law Enforcement

The IC3 received several hundred complaints related to a scheme in which law firms were the targets of a counterfeit check scheme. The victims of the scam received e-mails that requested the law firms' assistance for debt collection. The victims received checks from the alleged debtor and were given instructions to wire the collected funds minus attorney fees. In most cases, the funds were wired to banks in Korea, China, Ireland and Canada. In all cases, the checks were returned as counterfeit. The IC3 first provided information to various field offices and the U.S. Postal Inspection Service (USPIS) regarding this scheme in October 2008. The IC3 supported many field offices with research and complaints as the scheme evolved.

In 2009, the IC3 obtained information that identified a major West African scammer in the Ontario area that has been connected to the collection scam affecting law firms in the U.S. and Canada. As the IC3 obtained more intelligence and conducted additional research, a nexus was established with FBI Birmingham, the USPIS, and the U.S. Secret Service case against Emmanuel Ekhator, a Nigerian national. The IC3 supported Birmingham with complaints, research, and produced public service announcements related to the subject's fraudulent activity. In 2010, the U.S. District Court for the Middle District of Pennsylvania charged the subject for his crime and in August 2011, he was extradited from Nigeria to the United States. The subject was ultimately sentenced in 2013 to 100 months in federal prison and a three-year term of supervised release for his role in a multi-national scheme that deceived victims of more than $70 million and ordered to pay $11,092,028 in restitution and serve a three-year term of supervised release following incarceration.

New Initiatives

In 2013, the FBI launched Operation Wellspring, an initiative by which the FBI, through the IC3, provides case-specific tactical intelligence and expert analysis to state and local law enforcement agencies engaged in investigating Internet crime. Through Operation Wellspring, the IC3 sends targeted intelligence and fraud packages to participating state, local and tribal law enforcement who successfully leverage FBI resources in developing successful cases. Meanwhile, the participating law enforcement agencies reciprocate by providing the IC3 with a continual flow of information and updates which, ultimately, will help other federal, state, and even

international law enforcement agencies realize success in developing effective investigations and prosecuting perpetrators of Internet crime.

Based on this initiative, as of April 2014, the IC3 had referred out dozens of case referrals representing more than 900 victim complaints with total reported losses over $3.5 million. The FBI and Utah's Cyber Task Force successfully prosecuted two of these cases. The first case involved Darrell Cooper, who pled guilty to felony theft, for stealing hundreds of DVDs from a grocery store rental kiosk and another case involving Shane Call, who pled guilty to communications fraud for his involvement in selling counterfeit jerseys online.

Protecting the Public

The IC3 understands the importance of informing the public about the dangers of cybercrime. The IC3's public service announcements (PSAs) and scam alerts are posted online and distributed to law enforcement and various media outlets. The PSAs keep consumers informed on the latest cyber trends and keep industry partners up-to-date about Internet fraud. The scam alerts are based upon information from law enforcement and complaints submitted to the IC3. These reports detail recent cybercrime trends and new twists to previously existing cyber scams.

The IC3 maintains the website www.lookstoogoodtobetrue.com, an educational site developed by a joint federal law enforcement and industry task force. This site gives consumers an opportunity to submit and review testimonials. Testimonials include stories in which consumers were defrauded by a scam, or they did not fall victim to a scam, and how they avoided becoming a victim. The PSAs, scam alerts and forms are all found on the IC3's website, www.ic3.gov.

Conclusion

This report details the IC3's efforts to prevent and reduce the prevalence and impact of the crimes highlighted. Throughout 2013, the IC3 has supported law enforcement officers in their investigations of Internet-related crimes. In 2013, the IC3 processed 262,813 complaints, representing more than $781 million in losses. In accordance with its mission, the IC3 referred complaints to state, local, federal, tribal and international law enforcement agencies and interacted with these agencies' personnel to support ongoing investigative initiatives and to develop new ones as the cyber-crime landscape evolves. The IC3's support led to numerous investigations that resulted in arrests, seizures, convictions and restitution, among other actions. The IC3 also produced monthly trend analysis reports, public service announcements, scam alerts, and other publications to alert law enforcement and the general public about the pervasiveness of online crime. The IC3 continually reviews its services and analytical tools to incorporate the latest advances in technology and ensure law enforcement needs are met.

Appendix I:
Online Crime Prevention

Every day the IC3 receives complaints from victims who clicked links in an e-mail or paid up-front fees for a product or service only to be conned out of their hard-earned money. Based on the type of scam, there are a number of things a consumer can do to avoid becoming a victim (information from www.ic3.gov/preventiontips.aspx).

Auction Fraud

- Before you bid, contact the seller with any questions you have. Review the seller's feedback.
- Be cautious when dealing with individuals outside of your country.
- Ensure you understand refund, return and warranty policies.
- Determine the shipping charges before you buy.
- Be wary if the seller only accepts wire transfers or cash.
- Consider insuring your item.
- Be wary of businesses that operate from P.O. boxes or mail drops (which are receptacles or slots for mail collection) as this may indicate a less than legitimate purpose.

Employment/Business Opportunities

- Be wary of inflated claims of product effectiveness.
- Be cautious of exaggerated claims of possible earnings or profits.
- Beware when money is required up front for instructions or products.
- Be wary when the job posting claims "no experience necessary."
- Do not give your Social Security number when first interacting with your prospective employer.
- Be wary when replying to unsolicited emails for work-at-home employment.

Identity Theft

- Ensure websites are secure before submitting a credit card number.
- Never throw away credit card or bank statements in usable form. Shred them to protect your identity.
- Be aware of missed bills, which could indicate the account has been taken over.
- Be cautious of scams requiring personal information.
- Never give a credit card number over the phone unless you initiate the call.
- Monitor credit statements monthly for any fraudulent activity. Review a copy of your credit report at least once a year.
- Report unauthorized transactions to bank or credit card companies as soon as possible.

Credit Card Fraud

- If purchasing merchandise, ensure it is from a reputable source. Do research to ensure the legitimacy of the individual or company.
- Beware of providing credit card information through unsolicited emails.
- Promptly reconcile credit card statements to avoid unauthorized charges.

Debt Elimination

- Know whom you are doing business with: Do your research. Contact the state Attorney General's Office or the state corporation commission to see if there are any consumer complaints on file against the business you are interested in.
- Be cautious when dealing with individuals outside of your own country.
- Ensure you understand all terms and conditions of any agreement before you sign it.

Investment Fraud, Ponzi and Pyramid Schemes

- If the opportunity appears too good to be true, it probably is.
- Beware of promises to make fast profits.
- Be wary of investments that offer high returns at little or no risk.
- Be cautious when you are required to bring in subsequent investors.
- Do not invest in anything unless you understand the deal.
- Verify the terms of any investment that you intend to make through independent means. Beware of references given by the promoter.
- Do not assume a company is legitimate based on the appearance of its website.
- Be leery when responding to investment offers received through unsolicited e-mail.

Lotteries

- Be wary if you do not remember entering a lottery or contest.
- Be wary if you receive a telephone call stating you are the winner in a lottery.
- Be wary of lotteries that charge a fee before delivery of your prize.
- Be wary of demands to send additional money to be eligible for future winnings.
- It is a violation of federal law to play a foreign lottery via mail or phone.

Phishing/Spoofing

- Avoid filling out forms in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link to which you are actually directed.
- Research what a company's official website is instead of "clicking a link" from an unsolicited e-mail.
- Contact the actual business that supposedly sent the e-mail to verify if the e-mail is genuine. Do so via your own research or by using the phone number on the back of the card if the message purports to be from a bank or credit card provider or the statements you receive.

Spam

- Do not open spam. Delete it unread.
- Never respond to spam as this will confirm to the sender that it is a "live" e-mail address.
- Have a primary and secondary e-mail address: one for people you know and one for all other purposes.
- Avoid giving out your e-mail address unless you know how it will be used.
- Never purchase anything advertised through unsolicited e-mail.

Reshipping

- Be wary if you are asked to ship packages to an "overseas home office."
- Be cautious if the individual states that his country will not allow direct business shipments from the United States.
- Be wary if the ship-to address is yours but the name on the package is not.
- Do not accept packages you did not order.
- If you receive packages you did not order, either refuse delivery or contact the company that sent the package.
- Be suspicious of any unsolicited e-mail requesting personal information.

Appendix II:
2013 IC3 Warnings/Press Releases

1. Holiday Shopping Tips (November 26, 2013)
2. IC3 Scam Alerts (November 25, 2013)
3. DOJ Awareness of Disaster Fraud Hotline Following Typhoon Haiyan (November 14, 2013)
4. CryptoLocker Ransomware Encrypts User's Files (October 28, 2013)
5. Spam E-Mails Continuing to Capitalize on FBI Officials' Names (September 25, 2013)
6. Beta Bot malware blocks users anti-virus programs (September 18, 2013)
7. Spear-Phishing E-mail with Missing Children Theme (August 22, 2013)
8. IC3 Scam Alerts (August 13, 2013) (August 13, 2013)
9. Spam: Delivering Malware and Advertising Dangerous Counterfeit Goods (August 07, 2013)
10. Consumer Alert: Pirated Software May Contain Malware (August 07, 2013)
11. Citadel Malware Continues to Deliver Reveton Ransomware in Attempts to Extort Money (July 29, 2013)
12. IC3 Scam Alerts (July 18, 2013) (July 18, 2013)
13. Ransomware Purporting To Be From The FBI Is Targeting OS X Mac Users (July 18, 2013)
14. Cyber Criminals Continue to Use Spear-Phishing Attacks to Compromise Computer Networks (June 25, 2013)
15. IC3 Scam Alerts (June 19, 2013) (July 19, 2013)
16. Cyber Criminals Using Photo-Sharing Programs to Compromise Computers (May 30, 2013)
17. IC3 2012 Internet Crime Report Released (May 14, 2013)
18. Phishing Attacks On Telecommunication Customers (May 08, 2013)
19. IC3 Scam Alerts (May 2, 2013) (May 02, 2013)
20. Boston Marathon Fraud (April 25, 2013)
21. IC3 Scam Alerts (January 7, 2013) (January 07, 2013)

Appendix III:
2013 IC3 Subject Country Statistics

Subject Countries by Complaint Count 2013

Rank	Country	Complaint Count	Percentage of Complaints	Rank	Country	Complaint Count	Percentage of Complaints
1	United States	83,799	31.89%	26	Japan	242	0.09%
2	United Kingdom	4,511	1.72%	27	United Arab Emirates	239	0.09%
3	Nigeria	3,598	1.37%	28	Indonesia	229	0.09%
4	China	2,601	0.99%	29	Sweden	168	0.06%
5	Canada	1,782	0.68%	30	Switzerland	167	0.06%
6	India	1,529	0.58%	31	Turkey	154	0.06%
7	Ghana	782	0.30%	32	Pakistan	152	0.06%
8	Philippines	714	0.27%	33	Singapore	140	0.05%
9	Germany	603	0.23%	34	Belgium	131	0.05%
10	Afghanistan	578	0.22%	35	Romania	130	0.05%
11	South Africa	534	0.20%	36	Thailand	128	0.05%
12	Russian Federation	533	0.20%	37	Panama	125	0.05%
13	Malaysia	524	0.20%	38	Morocco	120	0.05%
14	Macedonia, The Former Yugoslav Republic of	508	0.19%	39	Poland	118	0.04%
15	Australia	500	0.19%	40	Brazil	102	0.04%
16	France	486	0.18%	41	Puerto Rico	101	0.04%
17	Benin	409	0.16%	42	Cyprus	94	0.04%
18	Cameroon	387	0.15%	43	Ireland	93	0.04%
19	Spain	386	0.15%	44	Egypt	89	0.03%
20	Mexico	361	0.14%	45	Israel	86	0.03%
21	Hong Kong	344	0.13%	46	Bulgaria	79	0.03%
22	Italy	273	0.10%	47	Vietnam	78	0.03%
22	Netherlands	273	0.10%	48	Greece	77	0.03%
22	Ukraine	273	0.10%	49	Portugal	76	0.03%
25	Jamaica	260	0.10%	50	Senegal	75	0.03%

Note: *This represents a ranking of the top 50 countries that reported to the IC3 in 2013 and is based upon the total number of complaints received with subject information included in the complaint. The term "subject" is the individual or business that a complainant believes victimized them and this chart demonstrates the location of where the subject is allegedly located based upon details submitted in the actual IC3 complaint. The total includes complaints that list dollar loss amounts and complaints that do not list dollar loss amounts. Figures were rounded to the nearest hundredth and do not total 100 percent.*

Subject Countries by Complaint Reporting a Loss 2013

Rank	Country	Complaint Count	Percentage of Complaints	Rank	Country	Complaint Count	Percentage of Complaints
1	United States	49,128	41.13%	26	Japan	91	0.08%
2	United Kingdom	2,464	2.06%	27	Thailand	84	0.07%
3	China	2,237	1.87%	28	Pakistan	78	0.07%
4	Nigeria	1,984	1.66%	28	Romania	78	0.07%
5	Canada	1,006	0.84%	28	Singapore	78	0.07%
6	India	919	0.77%	31	Turkey	74	0.06%
7	Ghana	559	0.47%	32	Switzerland	68	0.06%
8	Philippines	392	0.33%	33	Netherlands	61	0.05%
9	Malaysia	312	0.26%	34	Puerto Rico	57	0.05%
10	Cameroon	310	0.26%	35	Morocco	55	0.05%
11	South Africa	281	0.24%	36	Poland	54	0.05%
12	Hong Kong	278	0.23%	37	Cyprus	51	0.04%
13	Afghanistan	267	0.22%	37	Egypt	51	0.04%
14	Russian Federation	258	0.22%	39	Dominican Republic	50	0.04%
15	Australia	251	0.21%	40	Panama	49	0.04%
16	Spain	223	0.19%	40	Sweden	49	0.04%
17	Mexico	207	0.17%	42	Ireland	48	0.04%
18	Indonesia	186	0.16%	43	Brazil	46	0.04%
19	Germany	181	0.15%	44	Portugal	45	0.04%
20	France	164	0.14%	45	Greece	44	0.04%
21	Jamaica	160	0.13%	45	Israel	44	0.04%
21	Italy	160	0.13%	47	Vietnam	43	0.04%
23	Benin	148	0.12%	48	Belgium	40	0.03%
24	Ukraine	125	0.10%	49	Korea, Republic of	33	0.03%
25	United Arab Emirates	92	0.08%	50	New Zealand	33	0.03%

Note: *This represents a ranking of the top 50 countries that reported to the IC3 in 2013 based upon the total number of complaints received that reported subject information in the complaint and also reported a monetary loss. The term "subject" is the individual or business that a complainant believes victimized them and this chart demonstrates the location of where the subject is allegedly located based upon details submitted in the actual IC3 complaint. Figures were rounded to the nearest hundredth percent and do not total 100 percent.*

Appendix IV:
2013 IC3 Subject State Statistics

Subject States by Complaint Count 2013

Rank	State	Complaint Count	Percentage of Complaints	Rank	State	Complaint Count	Percentage of Complaints
1	California	12,505	14.92%	27	Minnesota	816	0.97%
2	Florida	7,447	8.89%	28	Wisconsin	788	0.94%
3	New York	7,189	8.58%	29	Louisiana	766	0.91%
4	Texas	6,762	8.07%	30	Kentucky	683	0.82%
5	Illinois	2,911	3.47%	31	Nebraska	662	0.79%
6	Georgia	2,800	3.34%	32	Connecticut	635	0.76%
7	Pennsylvania	2,463	2.94%	33	Oklahoma	625	0.75%
8	Washington	2,348	2.80%	34	Kansas	507	0.61%
9	District of Columbia	2,142	2.56%	35	Delaware	505	0.60%
10	New Jersey	2,037	2.43%	36	Arkansas	442	0.53%
11	Ohio	2,014	2.40%	37	Montana	340	0.41%
12	North Carolina	1,782	2.13%	38	Mississippi	333	0.40%
13	Arizona	1,764	2.11%	39	North Dakota	331	0.39%
14	Virginia	1,680	2.00%	40	Iowa	330	0.39%
15	Michigan	1,631	1.95%	41	New Mexico	300	0.36%
16	Nevada	1,538	1.84%	42	Maine	268	0.32%
17	Maryland	1,310	1.56%	43	West Virginia	262	0.31%
18	Colorado	1,195	1.43%	44	New Hampshire	230	0.27%
19	Massachusetts	1,181	1.41%	45	Idaho	223	0.27%
20	Indiana	1,117	1.33%	46	Alaska	221	0.26%
21	Tennessee	1,039	1.24%	47	Hawaii	216	0.26%
22	Missouri	1,021	1.22%	48	Rhode Island	199	0.24%
23	Alabama	979	1.17%	49	Wyoming	147	0.18%
24	Oregon	876	1.05%	50	South Dakota	145	0.17%
25	South Carolina	870	1.04%	51	Vermont	110	0.13%
26	Utah	846	1.01%				

Note: *This represents a ranking of each state and the District of Columbia and is based upon the total number of complaints reported to the IC3 in 2013 that reported subject information in the complaint. The term "subject" is the individual or business that a complainant believes victimized them and this chart demonstrates the location of where the subject is allegedly located based upon details submitted in the actual IC3 complaint. The totals include complaints that list dollar loss amounts and complaints that do not list dollar loss amounts. Also, 5.09 percent (4,268) of the complainants did not provide location information. Figures were rounded to the nearest hundredth and do not total 100 percent.*

Subject States by Complaint Count Reporting a Loss 2013

Rank	State	Complaint Count	Percentage of Complaints	Rank	State	Complaint Count	Percentage of Complaints
1	California	7,487	15.24%	27	Louisiana	507	1.03%
2	Florida	4,809	9.79%	28	Wisconsin	456	0.93%
3	New York	4,377	8.91%	29	Connecticut	387	0.79%
4	Texas	4,051	8.25%	30	Kentucky	386	0.79%
5	Illinois	1,867	3.80%	31	Nebraska	385	0.78%
6	Georgia	1,554	3.16%	32	Oklahoma	378	0.77%
7	Pennsylvania	1,445	2.94%	33	District of Columbia	320	0.65%
8	Ohio	1,303	2.65%	34	Delaware	307	0.62%
9	New Jersey	1,247	2.54%	35	Kansas	299	0.61%
10	Washington	1,215	2.47%	36	Arkansas	282	0.57%
11	North Carolina	1,073	2.18%	37	Montana	220	0.45%
12	Arizona	1,072	2.18%	38	North Dakota	215	0.44%
13	Nevada	999	2.03%	39	Mississippi	200	0.41%
14	Michigan	983	2.00%	40	Iowa	197	0.40%
15	Virginia	927	1.89%	41	Maine	169	0.34%
16	Maryland	789	1.61%	42	New Mexico	153	0.31%
17	Colorado	700	1.42%	43	New Hampshire	153	0.31%
18	Indiana	698	1.42%	44	West Virginia	148	0.30%
19	Massachusetts	680	1.38%	45	Rhode Island	138	0.28%
20	Tennessee	626	1.27%	46	Idaho	137	0.28%
21	Missouri	610	1.24%	46	Hawaii	137	0.28%
22	Alabama	584	1.19%	48	Alaska	120	0.24%
23	South Carolina	558	1.14%	49	Wyoming	92	0.19%
24	Minnesota	543	1.11%	50	South Dakota	89	0.18%
25	Utah	540	1.10%	51	Vermont	74	0.15%
25	Oregon	540	1.10%				

Note: *This is the total number of complaints from each state and the District of Columbia that reported subject information in the complaint and also reported a monetary loss. The term "subject" is the individual or business that a complainant believes victimized them and this chart demonstrates the location of where the subject is allegedly located based upon details submitted in the actual IC3 complaint. Also, 3.87 percent (1,902) of the complainants did not provide location information. Figures were rounded to the nearest hundredth and do not total 100 percent.*

Appendix V:
2013 IC3 Victim Country Statistics

Victim Countries by Complaint Count 2013

Rank	Country	Complaint Count	Percentage of Complaints	Rank	Country	Complaint Count	Percentage of Complaints
1	United States	238,189	90.63%	25	Malaysia	207	0.08%
2	Canada	3,621	1.38%	27	United Arab Emirates	201	0.08%
3	United Kingdom	2,225	0.85%	28	Colombia	179	0.07%
4	India	1,867	0.71%	29	Argentina	167	0.06%
5	Australia	1,810	0.69%	29	Belgium	167	0.06%
6	Macedonia, The Former Yugoslav Republic of	1,670	0.64%	31	Romania	164	0.06%
7	Mexico	711	0.27%	32	Portugal	163	0.06%
8	Puerto Rico	550	0.21%	33	Saudi Arabia	161	0.06%
9	Brazil	505	0.19%	34	Ireland	156	0.06%
10	South Africa	502	0.19%	34	Afghanistan	156	0.06%
11	France	463	0.18%	34	Hong Kong	156	0.06%
12	Germany	438	0.17%	37	Greece	154	0.06%
13	Philippines	434	0.17%	38	Indonesia	147	0.06%
14	Pakistan	391	0.15%	39	Switzerland	140	0.05%
15	Netherlands	348	0.13%	40	Denmark	136	0.05%
16	Russian Federation	306	0.12%	41	Norway	134	0.05%
17	Spain	293	0.11%	42	Turkey	129	0.05%
18	Sweden	258	0.10%	43	Ukraine	123	0.05%
19	New Zealand	252	0.10%	44	Bulgaria	122	0.05%
20	Italy	244	0.09%	45	Egypt	121	0.05%
21	China	236	0.09%	46	Thailand	113	0.04%
22	Israel	230	0.09%	47	Poland	103	0.04%
23	Nigeria	219	0.08%	47	Venezuela	103	0.04%
24	Singapore	208	0.08%	49	Chile	90	0.03%
25	Japan	207	0.08%	50	Hungary	88	0.03%

Note: *This represents a ranking of the top 50 countries that reported complaints to the IC3 and is based upon the total number of victim originated complaints received by IC3 in 2013 and their countries of residence. As demonstrated by the chart, the majority of victims reside in the United States. Figures were rounded to the nearest hundredth and do not total 100 percent.*

Victim Countries by Complaint Count Reporting Loss 2013

Rank	Country	Complaint Count	Percentage of Complaints	Rank	Country	Complaint Count	Percentage of Complaints
1	United States	106,079	88.80%	26	Hong Kong	122	0.10%
2	Canada	2,207	1.85%	27	Greece	115	0.10%
3	Australia	1,221	1.02%	28	Saudi Arabia	108	0.09%
4	India	1,125	0.94%	29	Indonesia	105	0.09%
5	United Kingdom	986	0.83%	30	Portugal	101	0.08%
6	Mexico	309	0.26%	31	Ireland	96	0.08%
7	Pakistan	294	0.25%	32	Japan	93	0.08%
8	South Africa	286	0.24%	33	Argentina	88	0.07%
9	Puerto Rico	271	0.23%	34	Romania	86	0.07%
10	Brazil	257	0.22%	35	Ukraine	84	0.07%
11	Philippines	249	0.21%	36	Colombia	83	0.07%
12	Russian Federation	223	0.19%	37	Turkey	82	0.07%
13	Germany	204	0.17%	38	Thailand	79	0.07%
14	China	191	0.16%	39	Egypt	76	0.06%
15	France	166	0.14%	40	Bulgaria	73	0.06%
16	Nigeria	161	0.13%	40	Switzerland	73	0.06%
17	Netherlands	157	0.13%	42	Afghanistan	70	0.06%
18	Israel	155	0.13%	42	Denmark	70	0.06%
19	Italy	149	0.12%	42	Poland	70	0.06%
20	Singapore	147	0.12%	45	Norway	69	0.06%
21	Spain	145	0.12%	46	Belgium	68	0.06%
22	New Zealand	142	0.12%	47	Venezuela	66	0.06%
23	Sweden	141	0.12%	48	Chile	59	0.05%
24	United Arab Emirates	136	0.11%	49	Korea, Republic of	58	0.05%
25	Malaysia	132	0.11%	50	Trinidad and Tobago	55	0.05%

Note: *This represents a ranking of the top 50 countries that reported to the IC3 in 2013 and is based upon the number of victim originated complaints that also included a dollar loss amount within the complaint. Figures were rounded to the nearest hundredth and do not total 100 percent.*

Victim Countries by Complaint Total Loss 2013

Rank	Country	Complaint Total Loss	Percentage of Complaints	Rank	Country	Complaint Total Loss	Percentage of Complaints
1	United States	$574,276,422	73.45%	26	Indonesia	$1,011,606	0.13%
2	Pakistan	$100,921,345	12.91%	27	Taiwan, Province of China	$958,833	0.12%
3	Canada	$14,414,723	1.84%	28	Nigeria	$900,164	0.12%
4	United Kingdom	$13,005,869	1.66%	29	France	$898,228	0.11%
5	Australia	$8,940,931	1.14%	30	Finland	$856,030	0.11%
6	India	$4,399,440	0.56%	31	Malaysia	$754,561	0.10%
7	Singapore	$3,679,687	0.47%	32	Thailand	$737,190	0.09%
8	Bangladesh	$3,113,128	0.40%	33	Belgium	$736,042	0.09%
9	Sweden	$2,775,697	0.36%	34	Korea, Republic of	$717,675	0.09%
10	China	$2,697,852	0.35%	35	Norway	$655,262	0.08%
11	South Africa	$2,295,347	0.29%	36	New Zealand	$643,357	0.08%
12	Italy	$2,178,850	0.28%	37	Portugal	$637,159	0.08%
13	Brazil	$2,122,253	0.27%	38	Saudi Arabia	$617,171	0.08%
14	Germany	$2,060,673	0.26%	39	Poland	$610,691	0.08%
15	Mexico	$2,021,526	0.26%	40	Switzerland	$598,970	0.08%
16	Philippines	$1,817,830	0.23%	41	Greece	$592,648	0.08%
17	Kyrgyz Republic	$1,796,751	0.23%	42	Bahrain	$582,661	0.07%
18	Russian Federation	$1,749,575	0.22%	43	Denmark	$563,521	0.07%
19	Spain	$1,721,446	0.22%	44	Kuwait	$547,532	0.07%
20	Hong Kong	$1,577,618	0.20%	45	Trinidad and Tobago	$513,160	0.07%
21	Netherlands	$1,316,352	0.17%	46	Turkey	$511,340	0.07%
22	Japan	$1,180,511	0.15%	47	Venezuela	$497,926	0.06%
23	United Arab Emirates	$1,081,393	0.14%	48	Israel	$483,414	0.06%
24	Puerto Rico	$1,052,505	0.13%	49	Ghana	$458,479	0.06%
25	Lebanon	$1,035,760	0.13%	50	Afghanistan	$453,874	0.06%

Note: *This represents a ranking of the top 50 countries that reported complaints to the IC3 in 2013 and is based upon the reported total dollar losses victims reported in their complaints. Figures were rounded to the nearest hundredth and do not total 100.*

Appendix VI:
2013 IC3 Victim State Statistics

Victim States by Average Loss 2013

Rank	State	Average Loss	Rank	State	Average Loss
1	Maine	$5,877	27	Vermont	$2,177
2	California	$3,639	28	Oregon	$2,164
3	Texas	$3,521	29	South Dakota	$2,110
4	North Dakota	$3,478	30	New Mexico	$2,057
5	Utah	$3,347	31	Alabama	$1,964
6	Delaware	$3,188	32	Michigan	$1,948
7	Georgia	$3,039	33	Wisconsin	$1,914
8	New York	$3,015	34	Ohio	$1,888
9	Virginia	$3,004	35	New Hampshire	$1,833
10	Nevada	$2,909	36	Pennsylvania	$1,819
11	Oklahoma	$2,793	37	Maryland	$1,808
12	Nebraska	$2,786	38	Tennessee	$1,787
13	Rhode Island	$2,757	39	Connecticut	$1,779
14	Florida	$2,750	40	New Jersey	$1,753
15	Idaho	$2,697	41	Missouri	$1,744
16	Massachusetts	$2,588	42	North Carolina	$1,742
17	Minnesota	$2,476	43	Kentucky	$1,727
18	Hawaii	$2,433	44	South Carolina	$1,687
19	Arizona	$2,358	45	Arkansas	$1,660
20	Washington	$2,353	46	Wyoming	$1,655
21	Mississippi	$2,347	46	Kansas	$1,587
22	Iowa	$2,324	48	District of Columbia	$1,308
23	Colorado	$2,300	49	West Virginia	$1,272
24	Illinois	$2,265	50	Montana	$1,236
25	Indiana	$2,204	51	Alaska	$426
26	Louisiana	$2,191			

Note: *This represents a ranking of each state and the District of Columbia based upon the average dollar loss per victim originated complaint reported to the IC3 in 2013. Of the complaints, average losses of $1,098 were reported by complainants who did not report a location.*

Victim States by Complaint Count 2013

Rank	State	Complaint Count	Percentage of Complaints	Rank	State	Complaint Count	Percentage of Complaints
1	California	28,888	12.13%	27	Alaska	2,662	1.12%
2	Florida	17,739	7.45%	28	Kentucky	2,385	1.00%
3	Texas	16,056	6.74%	29	Connecticut	2,197	0.92%
4	New York	12,612	5.29%	30	Louisiana	2,112	0.89%
5	Pennsylvania	7,914	3.32%	31	Oklahoma	1,862	0.78%
6	New Jersey	7,647	3.21%	32	Utah	1,775	0.75%
7	Illinois	7,024	2.95%	33	Kansas	1,621	0.68%
8	Virginia	6,764	2.84%	34	Arkansas	1,583	0.66%
9	Ohio	6,541	2.75%	35	Iowa	1,580	0.66%
10	Georgia	6,151	2.58%	36	New Mexico	1,404	0.59%
11	Washington	6,009	2.52%	37	Mississippi	1,314	0.55%
12	North Carolina	5,981	2.51%	38	West Virginia	1,244	0.52%
13	Michigan	5,493	2.31%	39	Idaho	1,019	0.43%
14	Arizona	5,310	2.23%	40	Hawaii	993	0.42%
15	Maryland	5,268	2.21%	41	New Hampshire	918	0.39%
16	Colorado	4,613	1.94%	42	Nebraska	845	0.35%
17	Massachusetts	4,085	1.72%	43	Montana	730	0.31%
18	Tennessee	3,969	1.67%	44	Maine	704	0.30%
19	Indiana	3,695	1.55%	45	District of Columbia	702	0.29%
20	Nevada	3,497	1.47%	46	Delaware	684	0.29%
21	Missouri	3,352	1.41%	47	Rhode Island	588	0.25%
22	Wisconsin	3,335	1.40%	48	Wyoming	454	0.19%
23	Alabama	3,105	1.30%	49	North Dakota	416	0.17%
24	Oregon	2,956	1.24%	50	Vermont	414	0.17%
25	South Carolina	2,868	1.20%	51	South Dakota	364	0.15%
26	Minnesota	2,719	1.14%				

Note: *This represents a ranking of states and the District of Columbia and is based upon the number of victim originated complaints reported to the IC3 in 2013 and their states of residence. Also, 10.09 percent (24,028) of the complaints did not provide location information. Figures were rounded to the nearest hundredth and do not total 100 percent. The top 10 states from this chart are also illustrated in the map on page seven.*

Victim States by Complaint Count Reporting a Loss 2013

Rank	State	Complaint Count	Percentage of Complaints	Rank	State	Complaint Count	Percentage of Complaints
1	California	13,535	12.76%	27	Kentucky	1,084	1.02%
2	Florida	8,269	7.80%	28	Louisiana	1,022	0.96%
3	Texas	7,545	7.11%	29	Connecticut	1,015	0.96%
4	New York	6,281	5.92%	30	Oklahoma	862	0.81%
5	Pennsylvania	3,538	3.34%	31	Utah	777	0.73%
6	Illinois	3,279	3.09%	32	Arkansas	719	0.68%
7	Virginia	3,140	2.96%	33	Iowa	717	0.68%
8	Ohio	2,786	2.63%	34	Kansas	692	0.65%
9	Washington	2,751	2.59%	35	Mississippi	640	0.60%
10	Georgia	2,705	2.55%	36	New Mexico	601	0.57%
11	Maryland	2,682	2.53%	37	West Virginia	537	0.51%
12	North Carolina	2,659	2.51%	38	Hawaii	417	0.39%
13	New Jersey	2,639	2.49%	39	Idaho	402	0.38%
14	Michigan	2,396	2.26%	40	Nebraska	397	0.37%
15	Arizona	2,250	2.12%	41	New Hampshire	362	0.34%
16	Colorado	1,932	1.82%	42	Alaska	347	0.33%
17	Massachusetts	1,792	1.69%	43	Delaware	311	0.29%
18	Tennessee	1,790	1.69%	44	Maine	291	0.27%
19	Alabama	1,686	1.59%	45	Montana	290	0.27%
20	Indiana	1,638	1.54%	46	District of Columbia	281	0.26%
21	Nevada	1,547	1.46%	47	Rhode Island	274	0.26%
22	Missouri	1,514	1.43%	48	North Dakota	192	0.18%
23	Wisconsin	1,477	1.39%	49	Vermont	177	0.17%
24	South Carolina	1,238	1.17%	50	Wyoming	172	0.16%
25	Oregon	1,193	1.12%	51	South Dakota	162	0.15%
26	Minnesota	1,179	1.11%				

Note: *This represents a ranking of states and the District of Columbia and is based upon the number of victim originated complaints that reported a dollar loss figure within the complaint. Also, 9.33 percent (9,897) of the complaints did not provide location information. Figures were rounded to the nearest hundredth and do not total 100 percent.*

Victim States by Complaint Total Loss 2013

Rank	State	Complaint Total Loss	Percentage of Complaints	Rank	State	Complaint Total Loss	Percentage of Complaints
1	California	$105,118,346	18.30%	27	Oklahoma	$5,199,764	0.91%
2	Texas	$56,534,880	9.84%	28	South Carolina	$4,839,453	0.84%
3	Florida	$48,778,217	8.49%	29	Louisiana	$4,627,893	0.81%
4	New York	$38,027,647	6.62%	30	Maine	$4,137,228	0.72%
5	Virginia	$20,319,530	3.54%	31	Kentucky	$4,117,820	0.72%
6	Georgia	$18,693,316	3.26%	32	Connecticut	$3,909,247	0.68%
7	Illinois	$15,907,173	2.77%	33	Iowa	$3,671,707	0.64%
8	Pennsylvania	$14,398,601	2.51%	34	Mississippi	$3,084,199	0.54%
9	Washington	$14,138,154	2.46%	35	New Mexico	$2,888,398	0.50%
10	New Jersey	$13,402,721	2.33%	36	Idaho	$2,748,012	0.48%
11	Arizona	$12,518,439	2.18%	37	Arkansas	$2,628,423	0.46%
12	Ohio	$12,351,755	2.15%	38	Kansas	$2,572,215	0.45%
13	Michigan	$10,697,615	1.86%	39	Hawaii	$2,415,892	0.42%
14	Colorado	$10,611,521	1.85%	40	Nebraska	$2,353,819	0.41%
15	Massachusetts	$10,570,678	1.84%	41	Delaware	$2,180,846	0.38%
16	North Carolina	$10,416,194	1.81%	42	New Hampshire	$1,683,034	0.29%
17	Nevada	$10,171,633	1.77%	43	Rhode Island	$1,620,972	0.28%
18	Maryland	$9,522,259	1.66%	44	West Virginia	$1,582,525	0.28%
19	Indiana	$8,142,650	1.42%	45	North Dakota	$1,446,979	0.25%
20	Tennessee	$7,091,950	1.23%	46	Alaska	$1,134,677	0.20%
21	Minnesota	$6,731,363	1.11%	47	District of Columbia	$918,293	0.16%
22	Oregon	$6,398,079	1.11%	48	Montana	$901,950	0.16%
23	Wisconsin	$6,382,394	1.11%	49	Vermont	$901,275	0.16%
24	Alabama	$6,097,466	1.06%	50	South Dakota	$768,105	0.13%
25	Utah	$5,941,062	1.03%	51	Wyoming	$751,337	0.13%
26	Missouri	$5,845,699	1.02%				

Note: *This is the total dollar losses for complaints from each state and the District of Columbia. Also, 4.59 percent or ($26,383,019.60 in losses) of the complainants did not provide location information. Figures were rounded to the nearest hundredth and do not total 100 percent.*