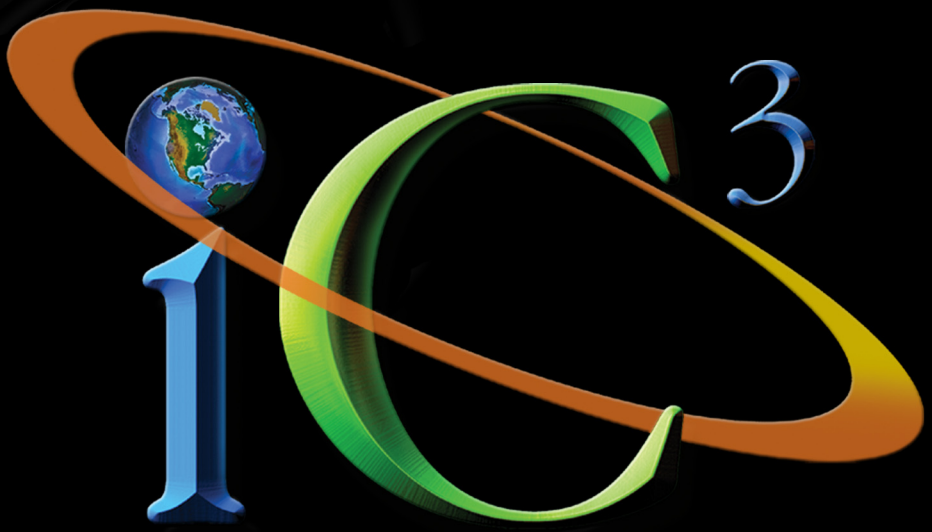


INTERNET CRIME COMPLAINT CENTER

2011 INTERNET CRIME REPORT

This project was supported by Grant No. 2010-BE-BX-K023 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Project 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 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. NW3C has other sections within its organization, including Training (in Computer Crime, Financial Crime and Intelligence Analysis), Research and Investigative Support Services.

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.

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

Table of Contents

2011 Internet Crime Report

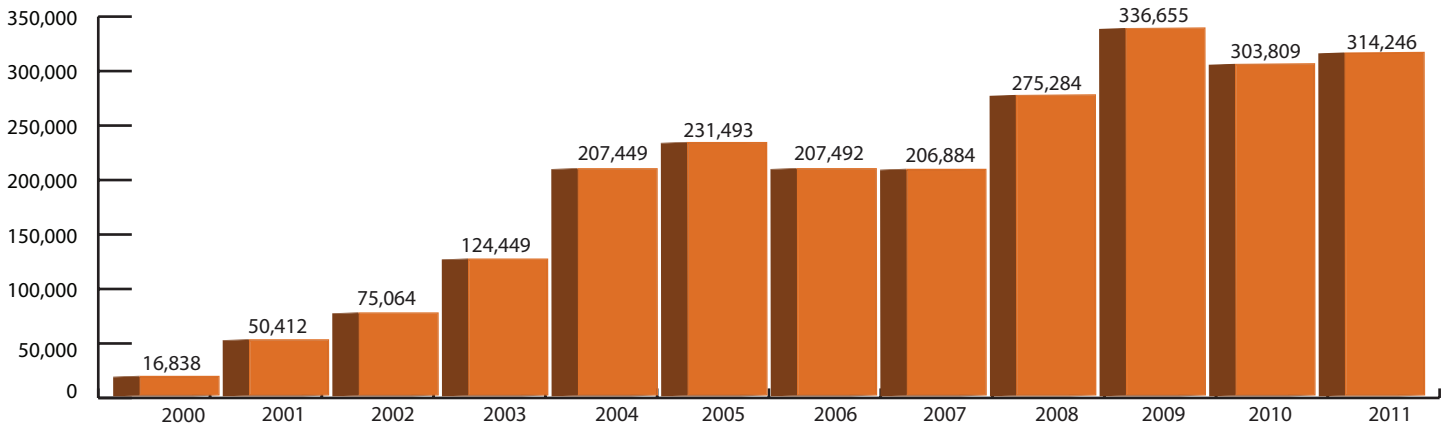
Executive Summary

In 2011, the Internet Crime Complaint Center (IC3) actively pursued its mission to address crimes committed using the Internet, providing services to both victims of online crimes and to law enforcement. Statistics in this report reveal IC3's success. IC3 marked the third year in a row that it received over 300,000 complaints, a 3.4-percent increase over the previous year. The adjusted dollar loss of complaints was $485.3 million.[1]

The *2011 IC3 Internet Crime Report* reveals both the scope of online crime and IC3's battle against it. The most common victim complaints included FBI-related scams, identity theft and advance fee fraud.[2] IC3 received and processed more than 26,000 complaints per month. Based on victim complaints, the top five states were California (34,169), Florida (20,034), Texas (18,477), New York (15,056) and Ohio (12,661). Victims in California reported the highest dollar losses with a total of $70.5 million. For victims reporting financial losses, the average was $4,187.

IC3 serves as a powerful conduit for law enforcement to share information and pursue cases that often span jurisdictional boundaries. Collaboration within this partnership has produced a number of technological advancements to streamline how the public's complaints are processed and referred to investigators. Initially established as simply a convenient method for citizens to report Internet crime information, IC3 has evolved into a vital resource for both victims of online crime and for law enforcement across the country that investigate and prosecute a wide range of cases.

Yearly Comparison of Complaints[3]



[1]Methodology 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 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.

[2]Complaint category statistics that are based on the perceptions of the complaints are not typically accurate for statistical purposes. The statistics pulled from the complaints themselves, however, are considerably more accurate as they are categorized and grouped through the IC3 automated system. IC3 does not verify complaint data.

[3]IC3 started in May 2000.

IC3 Overview

The Internet Fraud Complaint Center — a partnership between NW3C, BJA and the FBI — was established May 8, 2000 to address the ever-increasing incidence of online fraud. Just three years later, in response to the exponential increase in cyber crime of all types, the center changed its name to the Internet Crime Complaint Center (IC3®). Today, IC3 accepts more complaints in a single month than it received in its first six months. With more than two million complaints received since its inception, IC3 serves as the nation's portal for reporting Internet crime and suspicious activity. IC3's success has attracted international interest, with Canada, the United Kingdom and Germany using IC3 as a model for similar cyber crime centers.

Lifecycle of a Complaint

Victims file complaints with IC3, some of which are auto-referred to appropriate law enforcement, while all go into the expansive bank of Internet crime complaints that make up the IC3 database.

While developing a case, Internet crime analysts compile similar complaints, collect relevant case information from both open- and closed-source public information databases and confer with state, local, tribal, federal and international law enforcement personnel. Of all the complaints received in 2011, only 36.9 percent (115,903) reported financial loss. Although IC3 may not immediately build all complaints into referrals, all complaints are helpful in identifying trends and building statistical reports.

IC3 compiles this information into reports that are available to all law enforcement through direct emails and placement on www.ic3.gov. It also develops public awareness documents. IC3 encourages victims of Internet crime to report all incidents to 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.

The Lifecycle of a Complaint at IC3

Resources for Building Cases

IC3 analysts use an automated matching system to identify links and commonalities between numerous complaints and combine the respective complaints into referral groups for law enforcement. Of the 314,246 complaints received in 2011, the IC3 automated complaint grouping system generated 47,592 new groupings for analytical review.

314,246
Complaints reported to IC3

In 2011, IC3 developed remote access, making IC3 data available to over 30,000 FBI employees. Additionally, IC3 established a link to the remote access tool on Law Enforcement Online (LEO), which currently has over 150,000 vetted users. 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 the development of cases.

NW3C designed the Internet Complaint Search and Investigation System (ICSIS®) to assist with Internet-related investigations. It allows IC3 analysts and law enforcement to build and share case information seamlessly.

IC3 examiners and analysts review complaints and analyze trends in ICSIS for similar complaints. Once they find similar complaints involving an individual, a group of individuals or a business, they compile this information into a case.

ICSIS training, provided by NW3C, is available for law enforcement agencies (local, state, federal and tribal) and allows them direct access to data and trends within their locality, state or region. In addition to allowing all law enforcement agencies to search, analyze and compile information, ICSIS enables users to communicate and share information.

NW3C provides ICSIS training to law enforcement

Complainant Demographics

Of the individuals who filed complaints with IC3 in 2011, 51.76 percent were male and 48.24 percent were female. In 2010, 53.10 percent of complainants were male and 46.89 percent were female. These numbers reflect a trend in recent years where the number of male and female complainants is equalizing.

There was little change between 2010 and 2011 in the age groups that filed complaints. In 2010, those younger than 20 represented 3.2 percent; in 2011 they represented 3.1 percent. Those between ages 20-39 represented 39 percent in 2010, and 40 percent in 2011. The highest percentage of complainants were between ages 40 to 59, which represented 44 percent in 2010 and 43 percent in 2011. For 2010 and 2011, those 60 and older represented 14 percent of the complainants.

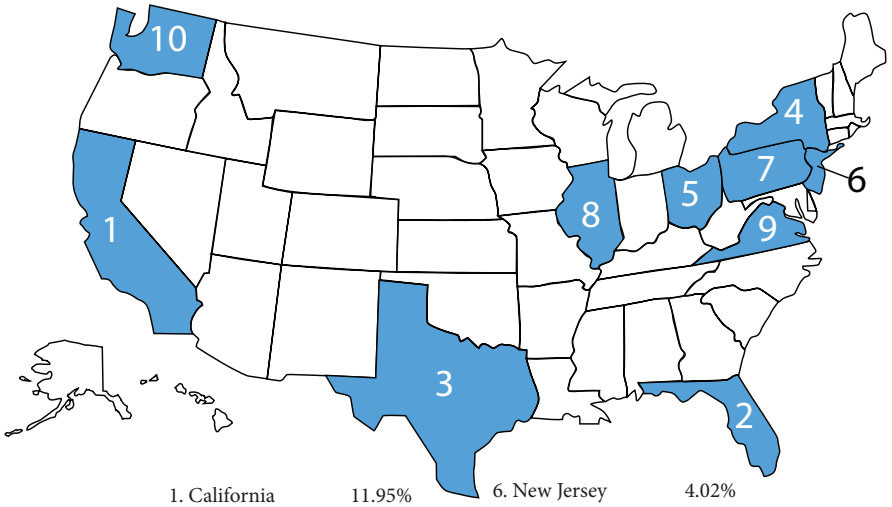
The top four states with the most individual complainants were California, Florida, Texas and New York. Most foreign complainants were from Canada, the United Kingdom, Australia and India.

Top 10 State Complainant Rates per 100,000 Population

State	Per 100,000 Population
1. Alaska	196
2. District of Columbia	137
3. New Jersey	131
4. Nevada	130
5. Colorado	123
6. Ohio	110
7. Maryland	109
8. Florida	107
9. Virginia	106
10. Washington	104

Note: *Based on U.S. Census data.*

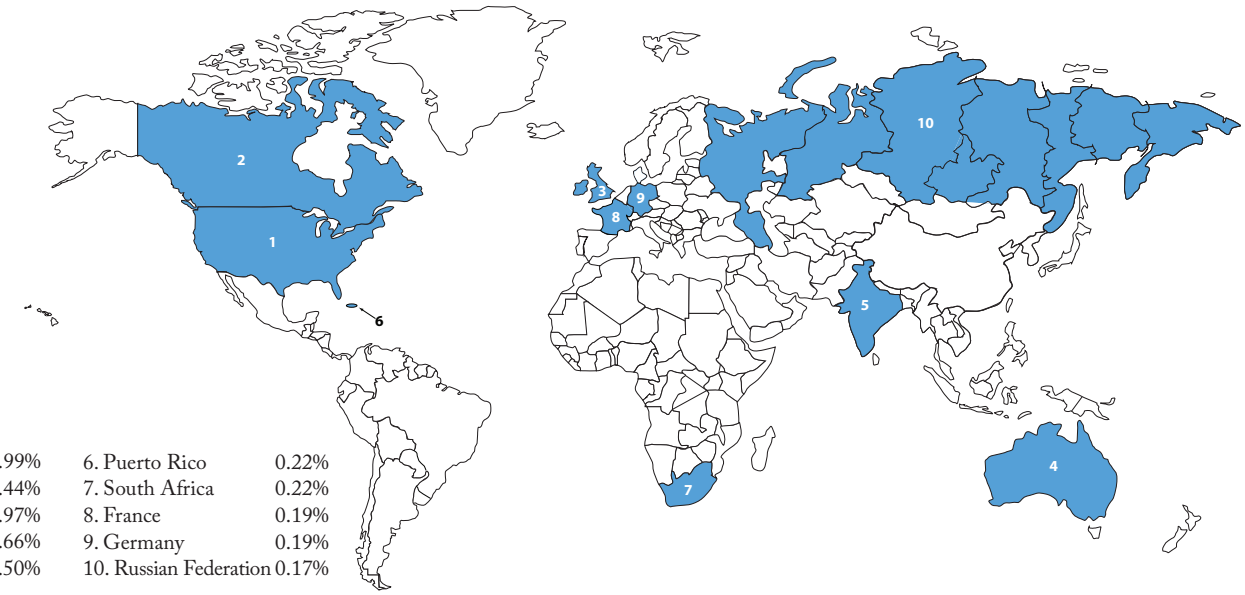
Top 10 States by Count: Individual Complainants (Numbered by Rank)



1. California	11.95%	6. New Jersey	4.02%
2. Florida	7.01%	7. Pennsylvania	3.34%
3. Texas	6.46%	8. Illinois	3.07%
4. New York	5.27%	9. Virginia	2.96%
5. Ohio	4.43%	10. Washington	2.44%

Note: *Of the complainants, 9.19% did not provide location information.*

Top 10 Countries by Count: Individual Complainants (Numbered by Rank)



1. United States	90.99%	6. Puerto Rico	0.22%
2. Canada	1.44%	7. South Africa	0.22%
3. United Kingdom	0.97%	8. France	0.19%
4. Australia	0.66%	9. Germany	0.19%
5. India	0.50%	10. Russian Federation	0.17%

Overall Statistics

Total complaints received: 314,246

Complaints reporting loss: 115,903

Total Loss: $485,253,871*

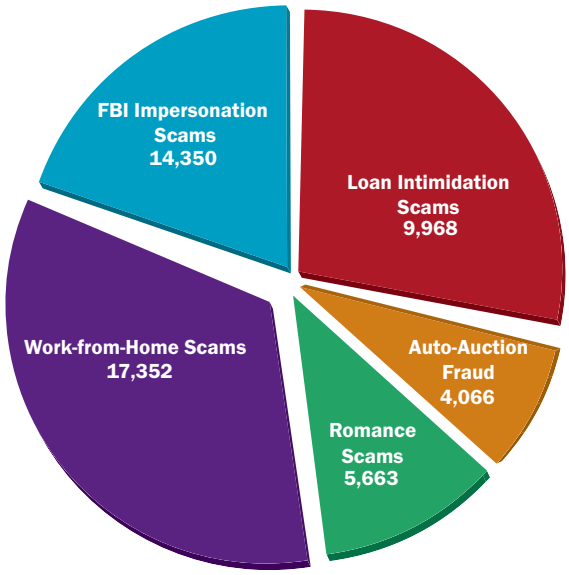
Median dollar loss for those reporting a loss: $636

Average dollar loss overall: $1,544

Average dollar loss for those reporting loss: $4,187

Complaint Characteristics

Major Fraud Types Reported in 2011

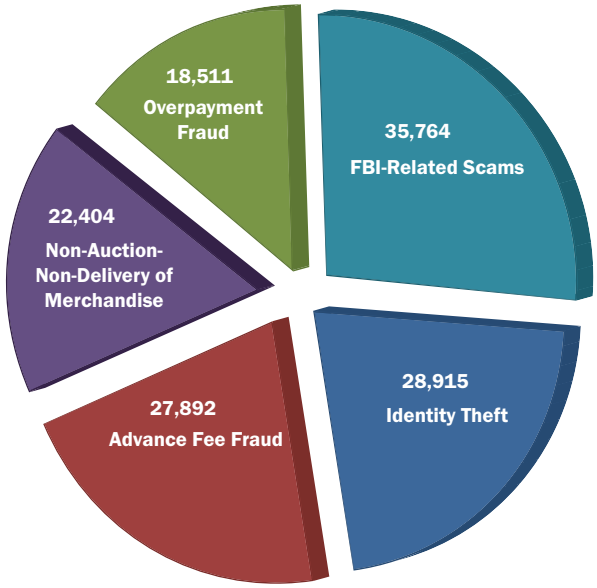


During 2011, FBI-related scams were the most reported offense, followed by identity theft and advance fee fraud.

IC3 primarily refers complaints with claims of dollar losses. Other complaints, which may represent a comparatively large percentage of complaints received, do not contain dollar loss claims, but are intended only to alert IC3 of the scam.

Complaint category statistics may not always produce an accurate picture. They are based on complainant perception. However, the Complaint Management System (CMS) was designed to mitigate a certain degree of subjectivity, allowing complaint categorization to be reported more consistently.

Top Five Reported Crime Types



Definitions of the top five crime types:

- **FBI-related Scams** – Scams in which a criminal poses as the FBI to defraud victims.
- **Identity Theft** – Unauthorized use of a victim's personal identifying information to commit fraud or other crimes.
- **Advance Fee Fraud** – Criminals convince victims to pay a fee to receive something of value, but do not deliver anything of value to the victim.
- **Non-Auction/Non-Delivery of Merchandise** – Purchaser does not receive items purchased.
- **Overpayment Fraud** – An incident in which the complainant receives an invalid monetary instrument with instructions to deposit it in a bank account and send excess funds or a percentage of the deposited money back to the sender.

* Methodology 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 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.

2011 Frequently Reported Internet Crimes

Auto-Auction Fraud

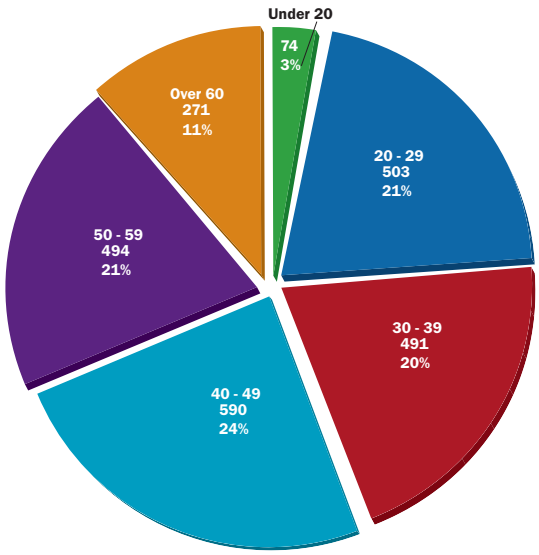
In fraudulent vehicle sales, criminals attempt to sell vehicles they do not own. Criminals create an attractive deal by advertising vehicles for sale at prices below book value. Often the sellers claim they must sell the vehicle because they are moving for work or being deployed for the military. Because of the alleged pending move, criminals refuse to meet in person or allow inspection of the vehicle, and they often attempt to rush the sale. To make the deal appear legitimate, the criminal instructs the victim to send full or partial payment to a third-party agent via a wire transfer payment service and to fax their payment receipt to the seller as proof of payment. The criminal pockets the payment but does not deliver the vehicle.

Victims of these scams reported losses exceeding $8.2 million in 2011. With an average reported loss of more than $2,000, more than $22,700 per day was lost to these frauds, or $946.13 every hour. IC3 received a complaint of this variety approximately every two hours.

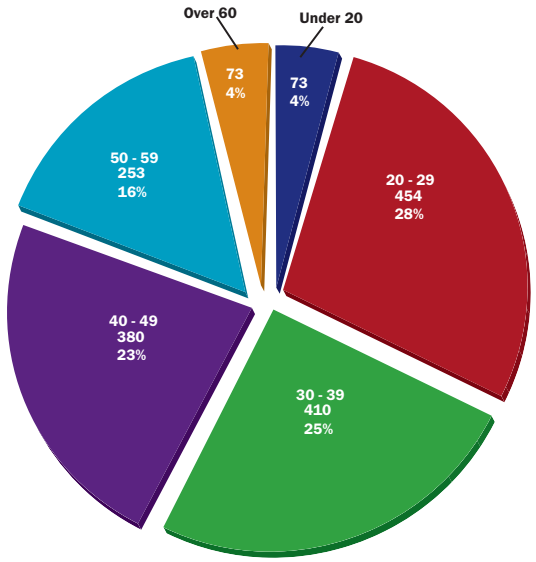
Auto-Fraud Scam Summary

	Male		Female			
Age Range	Complaints	Loss	Complaints	Loss	Total Complaints	Total Loss
Under 20	74	$141,244.39	73	$125,545.71	147	$266,790.10
20 - 29	503	$888,033.90	454	$763,667.57	957	$1,651,701.47
30 - 39	491	$967,194.68	410	$709,244.27	901	$1,676,438.95
40 - 49	590	$1,282,333.20	380	$790,528.10	970	$2,072,861.30
50 - 59	494	$1,031,193.53	253	$448,375.49	747	$1,479,569.02
Over 60	271	$883,705.96	73	$257,031.93	344	$1,140,737.89
Total	**2,423**	**$5,193,705.66**	**1,643**	**$3,094,393.07**	**4,066**	**$8,288,098.73**

Males Count by Age Range



Females Count by Age Range



Romance Scams

In 2011, IC3 received over 5,600 complaints of romance scams in which scammers target individuals who search for companionship or romance online. Victims believe they are "dating" someone decent and honest. However, the online contact is often a criminal with a well-rehearsed script that scammers use repeatedly and successfully. Scammers search chat rooms, dating sites, and social networking sites looking for victims. Although the principal group of victims is over 40 years old, divorced or widowed, disabled and often elderly, all demographics are at risk.

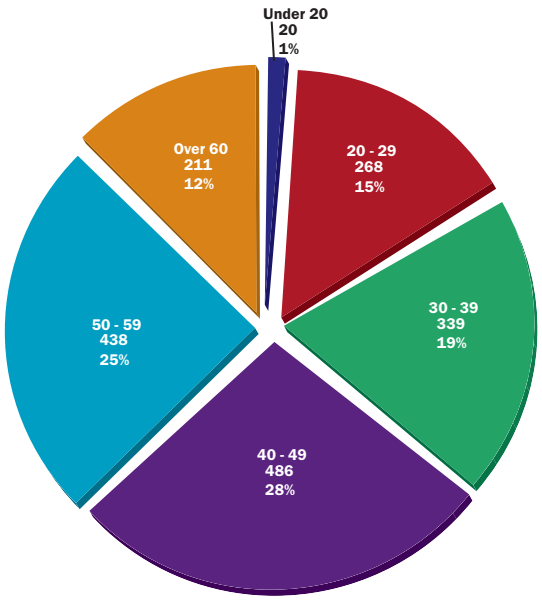
Scammers use poetry, flowers and other gifts to reel in victims, while declaring "undying love." These criminals also use stories of severe life circumstances, tragedies, family deaths, personal injuries or other hardships to keep their victims concerned and involved in their schemes. They also ask victims to send money to help overcome alleged financial hardships.

These scams not only take a high toll on victims emotionally, but monetarily as well. In 2011, victim reported losses to various romance scams totaled $50.4 million. On average, each victim reported a loss of $8,900. At a rate of 15 complaints received per day, these scams saw daily reported losses of roughly $138,000, or more than $5,700 every hour.

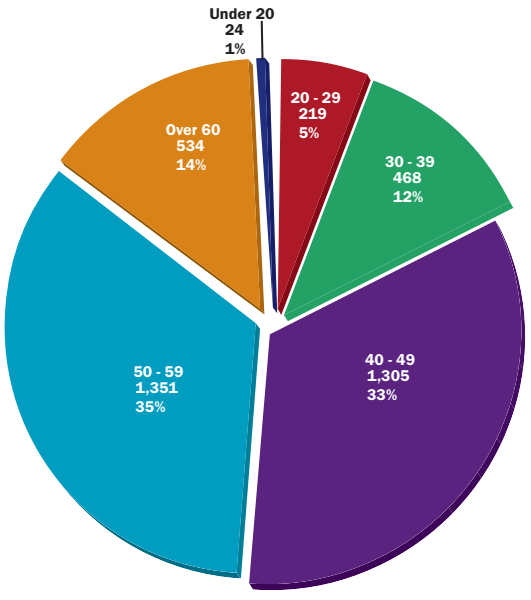
Romance Scam Summary

	Male		Female			
Age Range	**Complaints**	**Loss**	**Complaints**	**Loss**	**Total Complaints**	**Total Loss**
Under 20	20	$2,575.39	24	$28,207.00	44	$30,782.39
20 - 29	268	$667,631.90	219	$530.617.45	487	$1,198,249.35
30 - 39	339	$955,109.47	468	$2,784,399.71	807	$3,739,509.18
40 - 49	486	$2,668,065.76	1,305	$8,481,733.46	1,791	$11,149,799.22
50 - 59	438	$3,645,586.34	1,351	$18,802,678.69	1,789	$22,448,265.03
Over 60	211	$2,551,007.37	534	$9,281,950.62	745	$11,832,957.99
Total	**1,762**	**$10,489,976.23**	**3,901**	**$39,909,586.93**	**5,663**	**$50,399,563.16**

Males Count by Age Range



Females Count by Age Range



Work-from-Home Scams

Consumers continue to lose money from work-from-home scams that cyber criminals use to move stolen funds. Regrettably, due to their participation, these individuals may face criminal charges. Organized cyber criminals recruit their victims through newspaper ads, online employment services, unsolicited emails or "spam," and social networking sites advertising work-from-home "opportunities."

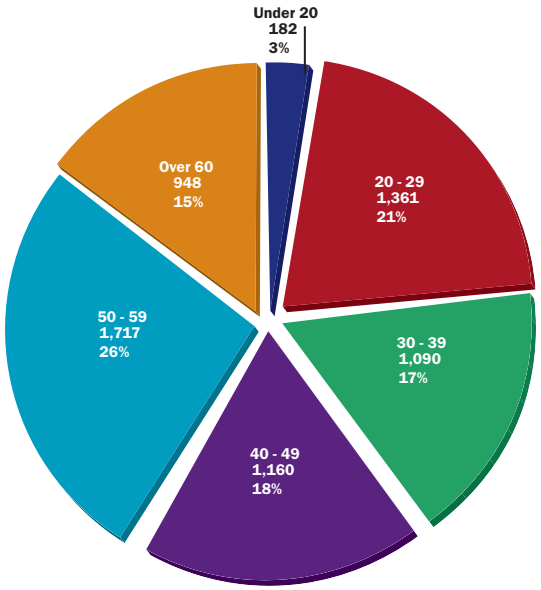
Participating with a legitimate business, the consumer becomes a "mule" for criminals who use the consumer's or other victim's accounts to steal and launder money. In addition, the scammers may compromise the victim's own identity or accounts.

Employment scams reported to IC3 in 2011 showed losses exceeding $20 million. Complaints from victims of these scams averaged two per hour in 2011. With an average reported loss of $1,160 per complaint, victims of employment scams reported losing more than $55,000 per day ($2,297 per hour).

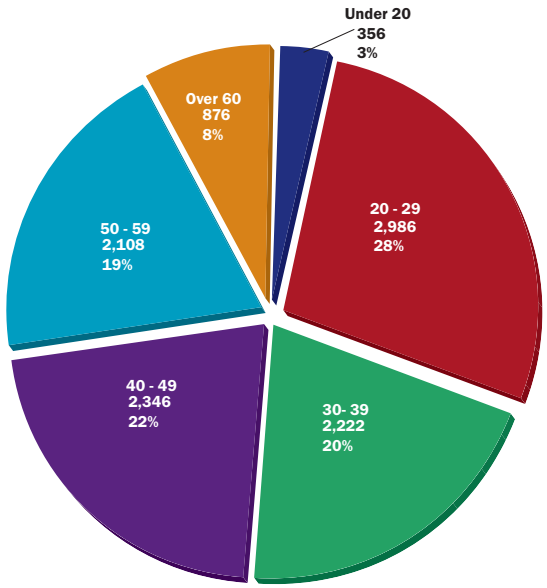
Work-from-Home Scam Summary

	Male		Female			
Age Range	**Complaints**	**Loss**	**Complaints**	**Loss**	**Total Complaints**	**Total Loss**
Under 20	182	$136,735.13	356	$315,968.24	538	$452,703.37
20 - 29	1,361	$1,213,441.54	2,986	$2,462,623.73	4,347	$3,676,065.27
30 - 39	1,090	$1,237,682.12	2,222	$1,924,376.64	3,312	$3,162,058.76
40 - 49	1,160	$1,600,690.90	2,346	$2,861,209.50	3,506	$4,461,900.40
50 - 59	1,717	$2,848,604.41	2,108	$2,035,254.74	3,825	$4,883,859.15
Over 60	948	$2,008,822.68	876	$1,480,017.36	1,824	$3,488,840.04
Total	**6,458**	**$9,045,976.78**	**10,894**	**$11,079,450.21**	**17,352**	**$20,125,426.99**

Males Count by Age Range



Females Count by Age Range



Loan Intimidation Scams

IC3 receives a high volume of complaints from victims of payday loan telephone collection scams. In these scams, a caller claims that the victim is delinquent in a payday loan and must repay the loan to avoid legal consequences. The callers purport to be representatives of the FBI, Federal Legislative Department, various law firms or other legitimate-sounding agencies. They claim to be collecting debts for various companies.

One of the most insidious aspects of this scam is that the callers have accurate information about the victims, including Social Security numbers, dates of birth, addresses, employer information, bank account numbers, and names and telephone numbers of relatives and friends. The method by which the fraudsters obtained 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.

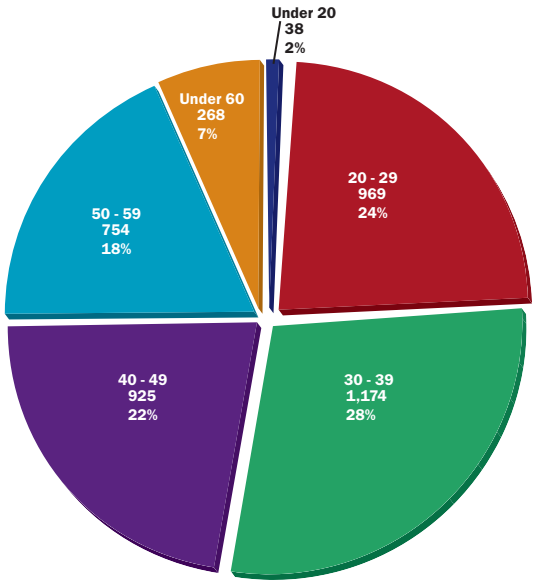
The fraudsters relentlessly call the victims' homes, cell phones and places of employment. They refuse to provide the victims any details of the alleged payday loans and become abusive when questioned. The callers threaten victims with legal actions, arrests, and in some cases physical violence if they refuse to pay. In many cases, the callers even resort to harassment of the victims' relatives, friends and employers.

In 2011, reported losses for victims of loan intimidation scams exceeded $8 million. At the rate of 27 complaints received per day, these scams resulted in reported losses of $934 per hour, or more than $22,000 per day.

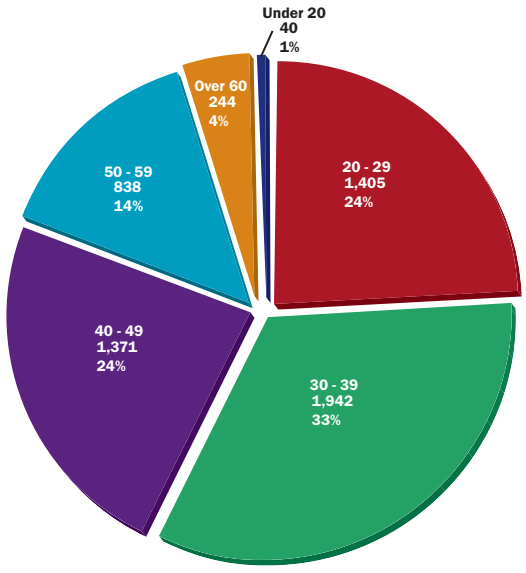
Loan Intimidation Scams

	Male		Female			
Age Range	Complaints	Loss	Complaints	Loss	Total Complaints	Total Loss
Under 20	38	$6,824.77	40	$17,688.99	78	$24,513.76
20 - 29	969	$479,041.08	1,405	$595,085.65	2,374	$1,074,126.73
30 - 39	1,174	$855,926.43	1,942	$794,067.27	3,116	$1,649,993.70
40 - 49	925	$807,032.96	1,371	$1,159,770.34	2,296	$1,966,803.30
50 - 59	754	$569,680.16	838	$969,530.75	1,592	$1,539,210.91
Over 60	268	$1,001,285.03	244	$926,920.65	512	$1,928,205.68
Total	**4,128**	**$3,719,790.43**	**5,840**	**$4,463,063.65**	**9,968**	**$8,182,854.08**

Males Count by Age Range



Females Count by Age Range



FBI Impersonation Email Scams

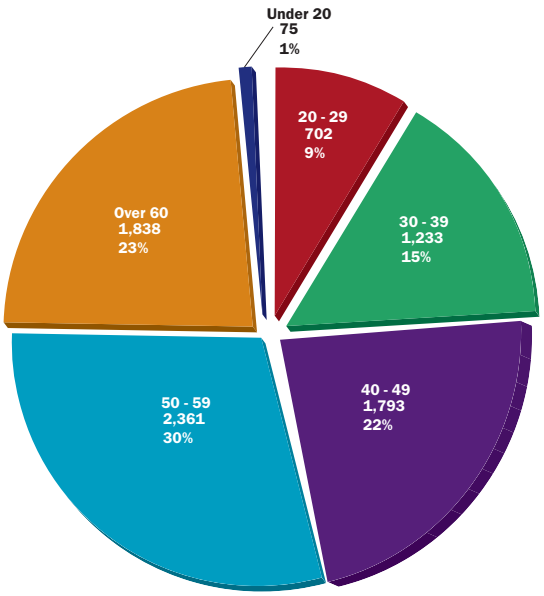
The names of various government agencies and high-ranking government officials have been used in spam attacks in an attempt to defraud consumers. Government agencies do not send unsolicited emails.

Complaints related to spam emails purportedly sent from the FBI continued to be reported with high frequency to IC3. In 2011, IC3 received about 39 complaints per day of this type. With an average reported loss of approximately $245 per complaint, victims reported losing more than $9,600 to this scam every day.

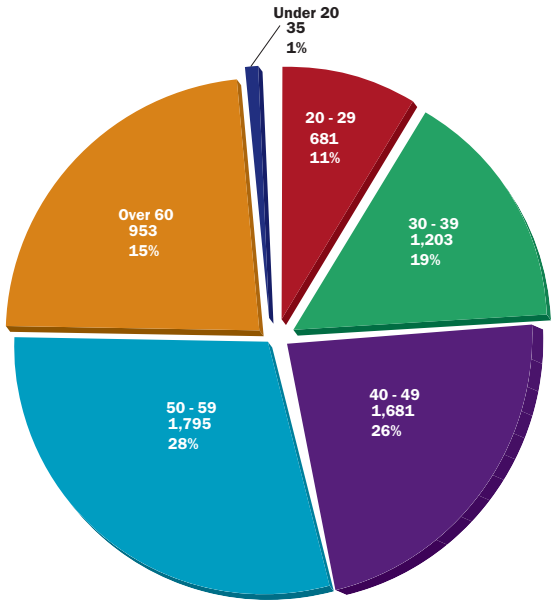
FBI Impersonation Email Scams

	Male		Female			
Age Range	**Complaints**	**Loss**	**Complaints**	**Loss**	**Total Complaints**	**Total Loss**
Under 20	75	$3,487.78	35	$850.00	110	$4,337.78
20 - 29	702	$171,207.57	681	$33,472.00	1,383	$204,679.57
30 - 39	1,233	$220,032.01	1,203	$93,036.71	2,436	$313,068.72
40 - 49	1,793	$577,707.19	1,681	$237,698.99	3,474	$815,406.18
50 - 59	2,361	$327,661.06	1,795	$501,021.39	4,156	$828,682.45
Over 60	1,838	$1,100,782.43	953	$250,098.45	2,791	$1,350,880.88
Total	**8,002**	**$2,400,878.04**	**6,348**	**$1,116,177.54**	**14,350**	**$3,517,055.58**

Males Count by Age Range



Females Count by Age Range



Case Highlights

Attorney Collection Scam

In July 2007, IC3 began receiving complaints from U.S. law firms that subject(s) contacted them via email requesting assistance with third party debt collection. The victims received checks from the alleged debtor along with instructions to wire transfer the collected funds minus attorney fees. In most instances, the funds were wired to banks in Korea, China, Ireland and Canada. In all instances the checks were counterfeit.

In a twist on this scam, the criminals purported to be a divorcee needing the law firm to handle the divorce settlement. In another instance, the scammers tried to purchase real estate in the U.S., using law firms to handle the transaction.

The law firms that wired funds experienced large monetary losses because the checks were usually in excess of $100,000. IC3 received over 600 attorney collection scam complaints from victims who reported more than $16 million in losses.

In August 2011, a Federal High Court in Lagos, Nigeria granted the extradition of Emmanuel Ekhator to the U.S. Ekhator allegedly defrauded U.S. law firms of more than $29 million in a third party debt collection scam. Ekhator will stand trial on the charges in the U.S. District Court for the Middle District of Pennsylvania.

Deceptive Marketing

IC3 provided information to the Florida Department of Law Enforcement and the Florida Attorney General's Office that was used to reach a settlement with a company over deceptive marketing practices. This company sells non-prescription dietary aids, nutritional supplements and other products online. The Attorney General's Economic Crimes Division began its investigation in December 2009 after consumers complained of receiving and being billed for products they did not order. An investigation revealed that acceptance of a trial product offer triggered a negative option agreement, which imposed automatic monthly shipments and re-occurring costs associated with receiving the trial products.

The company fully cooperated with the investigation and reimbursed or assisted in the reimbursement of approximately $3 million to consumers nationwide. In addition to refunds, it will pay approximately $51,000 to the Attorney General's Office for attorneys' fees and future investigation and enforcement. A special agent involved in the case said, "The (Attorney General's) Office used all of the victim information obtained from IC3 as part of their settlement … I will make sure and contact (IC3) if I need any more assistance, which is very likely."

"IC3 has been an invaluable resource for me in my role as an investigator. The crime analysts provide a wide array of complete investigative support and research to assist me. I look forward to another year of partnering with IC3 to combat economic crime."

Detective Douglas D. Hoffman
University of Toledo Police Department, OH

Infomercial Pitchman Scam

In June 2011, a federal grand jury returned a 41-count indictment against an infomercial pitchman on fraud-related charges for promoting an Internet-based, vitamin-selling business that ensnared more than 226,000 victims who invested about $51.8 million. It recruited victims to establish businesses selling vitamins over the Internet. The pitchman was indicted

on conspiracy, mail fraud, wire fraud, promotional money laundering and transactional money laundering charges.

This takedown was a cooperative effort involving IC3 along with the Phoenix Better Business Bureau, the Arizona Attorney General's Office, the Federal Trade Commission, and the U.S. Postal Inspection Service.

"Rings were matched with 10 victims in our case, nine of which had filed complaints with IC3. If not for IC3, we would not have had a case. They were instrumental in solving this case, putting the crook in jail and recovering property for the victims."

Detective Bill Barrett
San Diego County Sheriff's Department, CA
C.A.T.C.H. Team

Spoofed Website Case

Early in 2011, IC3 received complaints indicating that a non-profit organization that battles child pornography through its reporting hotline had been spoofed. This organization helps parents prevent children from viewing age-restricted material online with the "Restricted To Adults" website label.

The fraudulent company sent threatening emails to operators of adult websites claiming that child pornography was found on their websites. IC3 analysts learned that the group's website was fraudulently registered under the name of a U.S. congresswoman. Ultimately the domain name was transferred to the legitimate organization, ending the operation of the spoofed site.

Distributed Denial of Service (DDoS) Attack by Teen

IC3, working via the Internet Crime Working Group (ICWG), investigated a case that pertained to Distributed Denial of Service (DDoS) attacks by an individual who went by "phr34k1sh" and "verbal vampire." A DDoS attack causes websites to be knocked offline from numerous requests from outside computers at one time. Complainants reported that this individual hacked and perpetrated a DDoS attack on a gaming site. The site claimed to have lost 12 hours of sales, costing $500,000. The gaming site also claimed the hacker had changed their domain name system (DNS) server information, the technology that allows website addresses to appear as names rather than numbers.

International Work-At-Home Scam

Based on information from IC3, police in Long Beach, CA arrested a woman suspected of facilitating a wide-scale, international "work-at-home" scam operated out of Lagos, Nigeria. The defendant was directed to accept packages, sell the contents, retain 20 percent of proceeds and then wire the remaining funds to unknown suspects in Nigeria, according to Long Beach Police Detective Greg McMullen. The victims posted their resumes or ads online seeking job opportunities, Detective McMullen explained. The defendant in this case was charged with grand theft, possession of stolen property and parole violations.

Scam Alerts

Victims' complaints are a vital resource for IC3, law enforcement agencies and industry partners. IC3 uses all complaint data it receives to prepare public service announcements (PSAs) on the latest cyber trends to keep consumers and industry up-to-date on Internet fraud. IC3 distributes these PSAs through media outlets, corporate partners and www.ic3.gov. Below are some of the alerts distributed in 2011 (see Appendix II).

Traffic Ticket Spam

IC3 received more than 70 complaints between July and October 2011 about fraudulent emails claiming the recipients had been issued traffic tickets. The spam, which spoofed a nyc.gov email address, claimed to be from the New York State Police (NYSP). The email instructed victims to print the ticket and mail it to a town court in Chatham Hall.

NYSP is investigating this matter with assistance from the FBI Albany Division. Initial analysis indicated the email campaign is associated with a Russian domain. Some emails included malware associated with bogus anti-virus software.

Fraudster 'Double-Dipping'

In an Internet fraud involving autos, a scammer posts a nonexistent vehicle for sale on the Internet. Often the description and photos of the vehicle are lifted from legitimate websites. A buyer responds and is told that the vehicle is located overseas. The fraudster then instructs the victim to send a deposit via wire transfer to initiate the shipping process.

In a recent twist to this scam, the criminal advised there was a problem with the initial wire transfer and sent the victim a cashier's check. The victim was instructed to cash the check and send a second wire to a different account. Unaware the check was counterfeit, the victim followed the fraudster's instructions. The victim was duped twice, and the fraudster successfully executed his "double-dipping" strategy.

Radio Ad Seeks Mystery Shoppers

Some retailers hire marketing research companies to evaluate their quality of service. These research companies, in turn, use mystery shoppers to make purchases in stores or restaurants and then report on the experience.

Another version of mystery shopping involves consumers "hired" to evaluate the speed and efficiency of a specified money transfer service. The shopper receives a check with instructions to deposit it in a personal bank account, withdraw the amount in cash and wire it to a third party. After wiring the cash to a third party, the victim learns that the check was counterfeit. To appear credible, scammers advertise such opportunities on reputable websites, television stations and in publications. In reality, media outlets are unable to verify the legitimacy of the job opportunity.

Recently, IC3 received information from radio stations in Los Angeles and Palm Springs, California reporting that they had been contacted via email by an individual wanting to purchase ads to promote a mystery shopper program. The stations received signed confirmations and credit card payments, which cleared. The stations ran the ads and then received complaints from listeners who were scammed. Listeners received a check and were instructed to cash it immediately. After deducting $450 for their commission, they were told to wire the difference to a third party. Later, the check was identified as counterfeit. In addition, the credit card used to pay for the ads had been compromised.

Prevention Tips

Consumers who exercise diligence when conducting business online often avoid becoming victims. (Additional prevention tips can be found in Appendix I.)

- *Be cautious when dealing with individuals outside of your own country.*
- *Be wary if the seller only accepts wire transfers or cash, or if the business operates from P.O. boxes or maildrops.*
- *Beware when money is required up front for instructions or products.*
- *Monitor your credit statements monthly for any fraudulent activity and review a copy of your credit report at least once a year.*
- *Do not open spam. Delete it unread. Never respond to spam as this will confirm to the sender that it is a "live" email address.*

Bogus Lawsuits Promise Mortgage Relief

IC3 received several complaints from people who received a letter stating they were a potential plaintiff in a "mass joinder" lawsuit filed against their mortgage companies. The law firm made a variety of claims and sales pitches for legal and litigation services, asking consumers to pay non-refundable, upfront fees of $2,000 to $5,000. Its goal, however, was taking money, not providing a service.

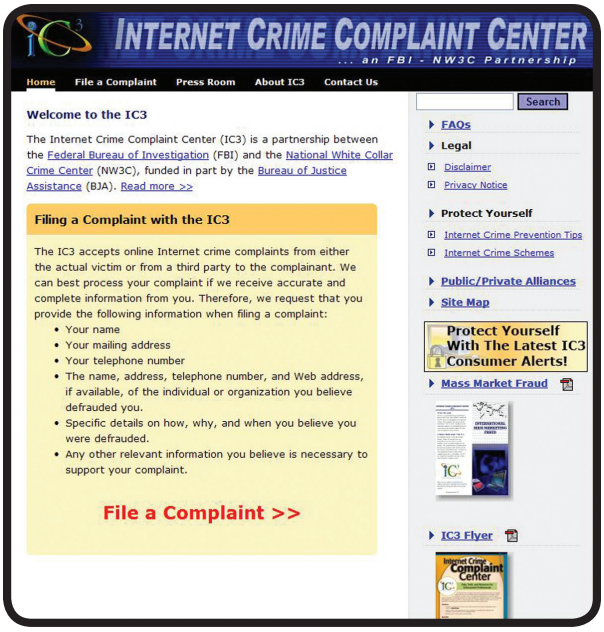
Lawyers seeking plaintiffs to join a class action lawsuit do not seek an up-front commission.

The California Department of Real Estate and the Better Business Bureau posted online warnings about this scam.

Protecting the Public

Over the past decade, Internet fraud has become one of the fastest-growing crime concerns facing the public. Nearly all crime that once was committed in person, by mail or over the telephone can now be committed through the Internet. IC3 serves as a convenient and easy way for victims of Internet crime to alert authorities to a suspected violation.

IC3 also understands how important it is to inform the public about the dangers of cyber crime. Because all age groups are potentially at risk, IC3 is dedicated to providing educational services to both children and adults. IC3 annually visits schools and community organizations to help ensure the public knows how to stay safe while online.



Information about cyber crime or filing a complaint may be found at www.ic3.gov

Through a partnership with the U.S. Postal Inspection Service and other businesses and organizations, IC3 operates the website www.lookstoogoodtobetrue.com, which provides information on the latest schemes and gives victims the opportunity to share their experiences online.

Conclusion

The *2011 IC3 Internet Crime Report* provides a snapshot of the variety of crimes perpetrated online. The report details IC3's efforts to prevent and reduce crime and assist law enforcement.

In 2011, IC3 processed over 300,000 complaints, representing dollar losses approaching a half-billion. IC3 referred complaints to local, state, federal and international law enforcement agencies, providing additional analysis to assist investigations, when relevant. As the case highlights and statistics in this year's report show, IC3's efforts led to the arrests and convictions of many cyber criminals. IC3 also produced trend analysis reports, public service announcements, scam alerts and other publications to alert both law enforcement and the general public.

IC3 will continue to enhance its services and products to keep up with technology and trends in the ongoing war against cyber crime.

Appendix I
Online Crime Prevention

Every day IC3 receives complaints from victims who clicked links in an email or paid up front 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 (This information appears online 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 own 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.

Credit Card Fraud

- If purchasing merchandise, ensure it is from a reputable source. Do research to ensure 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 who 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 registered complaints.
- Be cautious when dealing with individuals outside of your own country.
- Ensure that you understand all terms and conditions of any agreement.
- Be wary of businesses that operate from P.O. boxes or maildrops.

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 leery 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.
- 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 make 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.

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.
- Independently verify the terms of any investment that you intend to make. Beware of references given by the promoter.
- Do not assume a company is legitimate based on appearance of the website.
- Be leery when responding to investment offers received through unsolicited email.

Lotteries

- Be wary if you do not remember entering a lottery or contest.
- Be cautious if you receive a telephone call stating you are the winner of a lottery.
- Beware of lotteries that charge a fee before delivering 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

- Be suspicious of any unsolicited email requesting personal information.
- Avoid filling out forms in email messages that ask for personal information. This could be a phishing scam.
- Always compare the link in the email to the link that you are actually directed to visit.
- Log on to the entity's official website, instead of "linking" to it from an unsolicited email.
- Contact the actual business that supposedly sent the email to verify if the email is genuine.

Spam

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

Reshipping

- Be cautious if you are asked to ship packages to an "overseas home office."
- Be leery 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.

Appendix II
2011 Public Service Announcements*

December

http://www.ic3.gov/media/2011/111229.aspx

- Password Safety Posted
- Operation in Our Sites

November

Holiday Shopping Tips
http://www.ic3.gov/media/2011/111121.aspx

- Fraudulent Classified Ads or Auction Sales
- Gift Card Scams
- Phishing and Social Networking

October

http://www.ic3.gov/media/2011/111017.aspx

- Traffic Ticket Scam
- Fraudster Double-Dipping
- Online Vehicle Scam
- Mystery Shopper Scam
- Use of Government Officials' Identities Scam
- Modeling Scam
- Purported FDIC Email Scam

September

http://www.ic3.gov/media/2011/110901.aspx

- Mass Joinder Lawsuits for Mortgage Relief
- Online Auction Site Sony® Playstation® Bundle ad Scam
- Fraud Trends Effecting E-commerce
- Advisory on Military Addresses
- Email Address Tumbling

August

Automotive Brand Hijackers:
http://www.ic3.gov/media/2011/110815.aspx

Spam Emails Use FBI Officials' Names:
http://www.ic3.gov/media/2011/110809.aspx

July

http://www.ic3.gov/media/2011/110714.aspx

- DDoS Attacks
- Extortion Emails Targeting Physicians
- Scam Promises Large Winnings; Threats for Non-compliance
- Email Impersonating the FBI
- Threatening IC3 Impersonation Calls
- Increase in E-Commerce Fraud

May

http://www.ic3.gov/media/2011/110526.aspx

- Current Events Fraud
- Misrepresentation of the Financial Crimes Enforcement Network

http://www.ic3.gov/media/2011/110510.aspx

- Job Scam Used to Reship Merchandise to Russia
- Counterfeit Check Scam Targeting Realtors and Real Estate Attorneys

Malicious Software Features Osama bin Laden Links:
http://www.ic3.gov/media/2011/110504.aspx

April

Online Romance Scams:
http://www.ic3.gov/media/2011/110429.aspx

Fraud Alert: Unauthorized Wire Transfers to China
http://www.ic3.gov/media/2011/ChinaWireTransferFraudAlert.pdf

http://www.ic3.gov/media/2011/110404.aspx

- Automated Clearing House Spam
- Lottery Scammers Misusing Public Services
- Potassium Iodide Price Gouging

March

Avoiding Fraudulent Charitable Contribution Schemes:
http://www.ic3.gov/media/2011/110311.aspx

http://www.ic3.gov/media/2011/110310.aspx

- Romance Scammers
- Phishing Email Regarding Alleged Rejection of Tax Payments
- Telephone Scam Offering Virus Removal Services

February

http://www.ic3.gov/media/2011/110214.aspx

- Social Network Misspelling Scam
- Fake Online Receipt Scam
- Malicious Code in .gov Email

January

Emails Containing Malware Sent to Businesses Concerning Job Postings:
http://www.ic3.gov/media/2011/110119.aspx

Note: *No PSAs were issued in June.*

Appendix III
Complainant Statistics

Complainant Statistics by State*

Rank	State	Percent	Rank	State	Percent
1	California	11.95%	27	Louisiana	1.02%
2	Florida	7.01%	28	Connecticut	0.94%
3	Texas	6.46%	29	Kentucky	0.87%
4	New York	5.27%	30	Oklahoma	0.84%
5	Ohio	4.43%	31	Utah	0.72%
6	New Jersey	4.02%	32	Kansas	0.69%
7	Pennsylvania	3.34%	33	Iowa	0.68%
8	Illinois	3.07%	34	Arkansas	0.67%
9	Virginia	2.96%	35	New Mexico	0.59%
10	Washington	2.44%	36	Mississippi	0.55%
11	Michigan	2.38%	37	West Virginia	0.49%
12	North Carolina	2.35%	38	Alaska	0.49%
13	Arizona	2.29%	39	Idaho	0.44%
14	Georgia	2.23%	40	Hawaii	0.41%
15	Maryland	2.20%	41	New Hampshire	0.39%
16	Colorado	2.16%	42	Nebraska	0.35%
17	Tennessee	1.81%	43	Maine	0.32%
18	Indiana	1.67%	44	Montana	0.30%
19	Massachusetts	1.61%	45	District of Columbia	0.29%
20	Missouri	1.49%	46	Rhode Island	0.27%
21	Wisconsin	1.39%	47	Delaware	0.26%
22	Alabama	1.28%	48	Vermont	0.19%
23	Oregon	1.25%	49	Wyoming	0.18%
24	Nevada	1.23%	50	South Dakota	0.15%
25	Minnesota	1.18%	51	North Dakota	0.13%
26	South Carolina	1.09%			

***Note:** This is the total number of complaints from each state and the District of Columbia. This total includes complaints that list dollar loss amounts and complaints that do not list dollar loss amounts. Also, 9.19% of the complainants did not provide location information. Figures were rounded to the nearest hundreth percent and do not total 100%.*

Complainant Loss by Victim State*

Rank	State	Loss	Percent	Rank	State	Loss	Percent
1	California	$70,479,912	17.78%	27	Louisiana	$3,832,686	0.97%
2	Florida	$31,552,488	7.96%	28	Kentucky	$3,792,044	0.96%
3	Texas	$29,915,173	7.55%	29	Oregon	$3,671,495	0.93%
4	New York	$23,162,563	5.84%	30	Oklahoma	$3,660,524	0.92%
5	Pennsylvania	$12,454,055	3.14%	31	Arkansas	$2,925,389	0.74%
6	Virginia	$11,332,175	2.86%	32	Hawaii	$2,675,128	0.67%
7	Illinois	$11,121,452	2.81%	33	Kansas	$2,632,465	0.66%
8	Arizona	$10,999,652	2.77%	34	New Mexico	$2,557,720	0.65%
9	Ohio	$10,619,201	2.68%	35	Iowa	$2,530,020	0.64%
10	New Jersey	$9,932,889	2.51%	36	Utah	$2,481,421	0.63%
11	Washington	$9,572,357	2.41%	37	Idaho	$2,229,701	0.56%
12	North Carolina	$9,054,427	2.28%	38	Rhode Island	$2,112,805	0.53%
13	Michigan	$8,850,400	2.23%	39	New Hampshire	$2,042,570	0.52%
14	Colorado	$8,110,787	2.05%	40	District of Columbia	$1,825,865	0.46%
15	Georgia	$8,089,934	2.04%	41	West Virginia	$1,814,270	0.46%
16	Maryland	$8,052,280	2.03%	42	Nebraska	$1,683,598	0.42%
17	Indiana	$6,313,102	1.59%	43	Mississippi	$1,577,778	0.40%
18	Massachusetts	$6,183,331	1.56%	44	Montana	$1,475,823	0.37%
19	Nevada	$6,122,688	1.54%	45	Alaska	$1,275,859	0.32%
20	Tennessee	$5,540,995	1.40%	46	Maine	$1,009,523	0.25%
21	Wisconsin	$5,196,383	1.31%	47	Delaware	$872,365	0.22%
22	Minnesota	$4,704,908	1.19%	48	Wyoming	$636,685	0.16%
23	South Carolina	$4,593,741	1.16%	49	North Dakota	$587,752	0.15%
24	Missouri	$4,547,345	1.15%	50	Vermont	$571,938	0.14%
25	Connecticut	$4,434,352	1.12%	51	South Dakota	$498,387	0.13%
26	Alabama	$4,087,028	1.03%				

**Note:* *This is the total number of complaints from each state and the District of Columbia. Of the complainants, 5.17% ($20,478,582) did not provide location information. Percentages were rounded to the nearest hundreth and do not add up to precisely 100%.*

Complaints per 100,000 Population*

Rank	State	Complaint Count	Rank	State	Complaint Count
1	Alaska	196	**27**	Pennsylvania	75
2	District of Columbia	137	**28**	Rhode Island	75
3	New Jersey	131	**29**	Utah	74
4	Nevada	130	**30**	Indiana	74
5	Colorado	123	**31**	Texas	73
6	Ohio	110	**32**	Missouri	71
7	Maryland	109	**33**	Massachusetts	71
8	Florida	107	**34**	North Carolina	70
9	Virginia	106	**35**	Wisconsin	70
10	Washington	104	**36**	Maine	70
11	Arizona	103	**37**	Michigan	69
12	Oregon	94	**38**	Kansas	69
13	California	92	**39**	Illinois	68
14	Wyoming	90	**40**	South Carolina	68
15	Vermont	88	**41**	Georgia	66
16	Montana	87	**42**	Arkansas	66
17	New Hampshire	86	**43**	Louisiana	64
18	Hawaii	85	**44**	Oklahoma	64
19	Delaware	83	**45**	Iowa	64
20	Tennessee	82	**46**	Minnesota	64
21	New Mexico	82	**47**	Kentucky	58
22	Idaho	80	**48**	North Dakota	56
23	New York	78	**49**	Nebraska	55
24	Alabama	77	**50**	Mississippi	53
25	West Virginia	76	**51**	South Dakota	52
26	Connecticut	75			

Note: *Based on U.S. Census data.*

Average Dollar Loss by Victim State per 100,000 Population*

Rank	State	Average Loss	Rank	State	Average Loss
1	District of Columbia	$1,119.70	27	Orgeon	$80.33
2	Rhode Island	$727.28	28	Colorado	$74.11
3	Wyoming	$631.07	29	Arizona	$71.91
4	North Dakota	$536.11	30	Minnesota	$71.83
5	Vermont	$516.39	31	Louisiana	$69.81
6	Montana	$514.35	32	Wisconsin	$63.59
7	Alaska	$508.90	33	Indiana	$57.31
8	Hawaii	$430.32	34	Alabama	$56.44
9	South Dakota	$375.54	35	Washington	$56.24
10	New Hampshire	$374.77	36	Massachusetts	$53.05
11	Idaho	$360.10	37	Maryland	$51.14
12	Delaware	$348.22	38	Tennessee	$47.22
13	Nebraska	$254.65	39	Missouri	$47.01
14	Maine	$231.70	40	New Jersey	$43.77
15	New Mexico	$207.02	41	Virginia	$41.49
16	Nevada	$178.80	42	North Carolina	$36.06
17	West Virginia	$157.67	43	Michigan	$35.73
18	Arkansas	$134.85	44	Georgia	$33.14
19	Kansas	$129.22	45	Ohio	$32.13
20	Utah	$125.22	46	Illinois	$27.81
21	Connecticut	$118.27	47	Pennsylvania	$25.69
22	Iowa	$116.81	48	Florida	$21.60
23	Oklahoma	$112.94	49	New York	$20.27
24	Kentucky	$89.17	50	Texas	$16.36
25	South Carolina	$81.61	51	California	$14.73
26	Mississippi	$81.55			

**Note:* *Average based on complaints reporting dollar loss. Based on U.S. Census data.*


IC3
INTERNET CRIME COMPLAINT CENTER

www.ic3.gov