INTERNET CRIME COMPLAINT CENTER

2010 Internet Crime Report

This project was supported by Grant No. 2009-BE-BX-K042 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

Table of Contents

List of Tables

List of Figures

List of Maps

2010 Internet Crime Report

Executive Summary

Now in its tenth year, the Internet Crime Complaint Center (IC3) has become a vital resource for victims of online crime and for law enforcement investigating and prosecuting offenders.

In 2010, IC3 received the second-highest number of complaints since its inception. IC3 also reached a major milestone this year when it received its two-millionth complaint. On average, IC3 receives and processes 25,000 complaints per month.

IC3 is more than a repository for victim complaints. It serves as a conduit for law enforcement to share information and pursue cases that often span jurisdictional boundaries. IC3 was founded in 2000 as a joint effort between the National White Collar Crime Center (NW3C)/Bureau of Justice Assistance (BJA) and the Federal Bureau of Investigation (FBI). That partnership leveraged the resources necessary to aid law enforcement in every aspect of an Internet fraud complaint.

The most common victim complaints in 2010 were non-delivery of payment/merchandise, scams impersonating the FBI (hereafter "FBI-related scams") and identity theft. Victims of these crimes reported losing hundreds of millions of dollars.

Through a number of technological advancements, IC3 has streamlined the way it processes and refers victim complaints to law enforcement. In 2004, IC3 developed Automatch, an automated internal complaint grouping and analytical search tool. The design of Automatch is based on an assessment of the IC3 partnership aimed at defining a joint workflow for the project partners with different service requirements. IC3 IT staff continually review and update Automatch to meet the needs of analysts who build cases for law enforcement worldwide gathering all related information based on commonalities in the IC3 data. In 2009, NW3C developed the state-of-the-art Internet Complaint Search and Investigation System (ICSIS), which fosters seamless collaboration among law enforcement from multiple jurisdictions. Expert IC3 analysts also provide key analytical and case support.

The 2010 Internet Crime Report demonstrates how pervasive online crime has become, affecting people in all demographic groups. The report provides specific details about various crimes, their victims and the perpetrators. It also shows how IC3 continually adapts its methods to meet the needs of the public and law enforcement.

History

The Internet Fraud Complaint Center (IFCC), a partnership between NW3C/BJA and the FBI, was established on May 8, 2000. The IFCC changed its name to IC3 in 2003 to reflect its expanded mission in the fight against cyber crime.

In May 2010, IC3 marked its 10th anniversary. By early November, IC3 had received two million complaints. IC3 received 303,809 complaints in 2010, averaging 25,317 per month (by comparison, the IFCC received 20,014 complaints in its first six months).

Canada, the United Kingdom and Germany have used IC3 as the model for similar cyber crime centers. IC3's public awareness efforts range from teaching children how to protect themselves online to showing senior citizens how to avoid identity theft. Also, IC3 provides presentations to local, national and international law enforcement and to key industrial leaders.

Cutting-Edge Approach To Fighting Internet Crime

In 2010, IC3 added the remote access feature to the IC3.net database tools. This feature gives all FBI personnel the ability to perform searches and case development work. With this system and last year's launch of ICSIS, IC3 has dramatically expanded the capacity and scope of services offered. The combined power of these two high-tech tools aid law enforcement in identifying and prosecuting cyber crime.

Law enforcement can set complaint thresholds for their jurisdictions within the Complaint Management System (CMS) so agencies can have real-time information of crimes occurring within their jurisdictions. For example, if the New York City Police Department requests to receive only those complaints with a specified dollar loss, IC3 analysts can comply with that request. The system automates approximately 40 percent of the complaints it receives, allowing analysts to process more complaints.

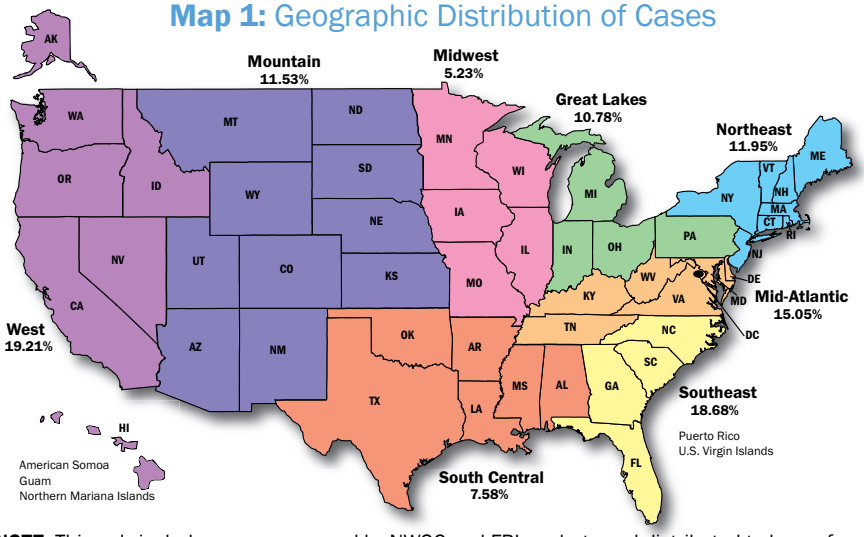
In addition to allowing all law enforcement – local, state, and federal agencies—to search, analyze, and compile information, ICSIS also allows these users to communicate and share information. Users can export case information to other software programs to create link charts and presentations.

IC3 analysts are available to compile data to give law enforcement a more detailed case. Analysts and investigators have the ability to develop case leads with multiple victims and jurisdictions, often involving the same perpetrator. The case analysis in multi-jurisdictional collaboration allows law enforcement access to new levels of information, which they can then use to build stronger cases.

IC3 tracks cases after they are referred to law enforcement. Referred cases are given a disposition code based on the direction law enforcement intends to take. This gives analysts the chance to measure the relative success of a case.

IC3 analysts prepared 1,420 cases (representing 42,808 complaints). Law enforcement prepared 698 cases (representing 4,015 complaints). In addition, law enforcement requested FBI assistance on 598 Internet crime matters. Of the referrals prepared by the FBI analysts, 122 open investigations were reported, which resulted in 31 arrests, 6 convictions, 17 grand jury subpoenas, and 55 search/seizure warrants.

Map 1: Geographic Distribution of Cases



NOTE: This only includes cases prepared by NW3C and FBI analysts and distributed to law enforcement.
Please note that percentages may not add up to 100 percent as a result of rounding.

Of the 303,809 complaints received in 2010, IC3 referred 121,710 to law enforcement. IC3 auto-referred 82,372 of these complaints to 1,629 law enforcement agencies. IC3 referred 2,597 child pornography complaints to the National Center for Missing and Exploited Children. Analysts also referred 1,970 urgent complaints containing threats of bodily harm to local law enforcement agencies. Additionally, Automatch attached 235,275 of the new complaints to 44,101 pre-existing groupings.

All complaints received at IC3 are used for intelligence reports, informational purposes and to identify emerging trends. Those complaints revealing a reported dollar loss or other victimization are referred to law enforcement.

Table 1: ICSIS Statistics

Category	Number
Users	2,472
New Users	862
Searches Performed	82,304
Complaint Views	886,556
Agencies Receiving Auto-Referrals	1,629

Table 2: IC3.gov Statistics

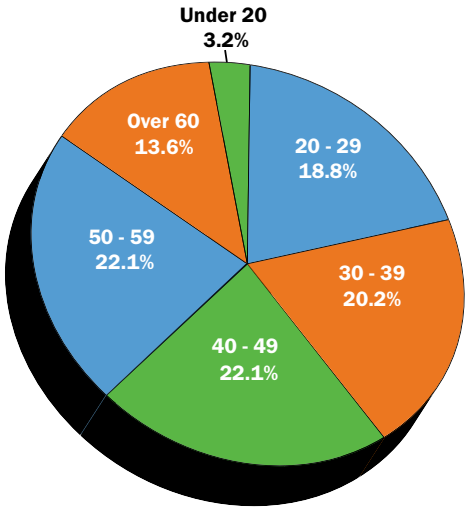
Category	Number
Visits	26,967,461
PDF Downloads	1,170,169

Internet Crime Trends

The IC3 experienced substantial growth in complaints, referrals, and dollar loss claims since 2000. In particular, there has been a significant increase in referrals in the two-year period since CMS and ICSIS were implemented in early 2009.

Historically, auction fraud has been the leading complaint reported by victims, with a high of 71.2 percent of all referrals in 2004. However, in 2010, auction fraud represents slightly more than 10 percent of referrals. This demonstrates the growing diversification of crimes related to the Internet. The steady decline in the total number of complaints and referrals of auction fraud over the last several years has altered the top complaint categories. The reason for this reduction is unknown. However, a possible explanation is that complaint levels are normalizing as businesses and consumers discover and implement ways to make previously uncharted areas of online commerce safer and more reliable.

Figure 1: Complainant Demographic by Age



The age of those reporting crimes to IC3 is becoming more evenly distributed. Early in IC3's history, the 30-39 age group represented the largest complainant reporting pool. Today, complainants 40-59 years old represent the two largest groups reporting crimes to IC3. However, historic trends indicate a continuing shift toward those in the 50-59 and 60-and-over category, which will further flatten the overall distribution of complainants. Those in the 60-and-over category account for the most dramatic rise in complaints over the entire 10 years.

The gender gap in crime reporting has dramatically narrowed. Early in IC3's history, men reported crime at a ratio of more than 2.5 to 1 over women. Today, men and women report crimes almost equally. In many states, a slightly higher proportion of women than men report crimes to IC3. The narrowed reporting gap between the sexes has significantly impacted the dollar loss between men and women over the last 10 years. During the course of IC3's early history, men reported a loss of more than $2.00 for every $1.00 reported by a woman. According to the 2010 data, men now report a loss of $1.25 for every $1.00 reported by a woman.

Internet Crime Working Group

The Internet Crime Working Group (ICWG) is a collaboration with IC3 analysts and the National Cyber-Forensics and Training Alliance (NCFTA). ICWG uses email to exchange critical unclassified data related to cyber intelligence to enhance cases and intelligence reports.

There were 259 items discussed among ICWG members in 2010. Of those, 101 items resulted in information sent to law enforcement, and 81 items sent to industry representatives. The ICWG recovered and reported 3,530 unique credit card numbers and 92 Social Security numbers, and developed 73 into NCFTA Assessments or IC3 monthly trend report articles.

General IC3 Filing Information

Complaints are submitted to IC3 at www.ic3.gov. The information is reviewed, categorized and, when appropriate, referred to local, state or federal law enforcement.

All complaints are accessible to law enforcement and are used in trend analysis. These complaints help provide a basis for future outreach events and educational awareness programs.

Figure 2: Yearly Comparison of Complaints Received Via the IC3 Website

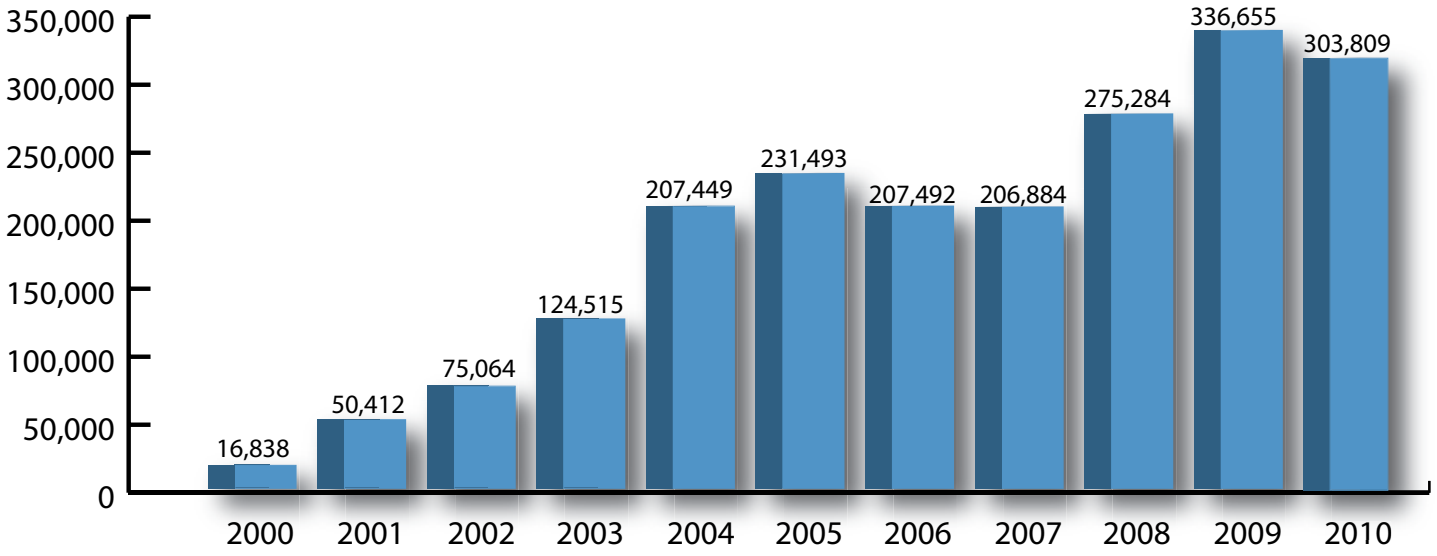
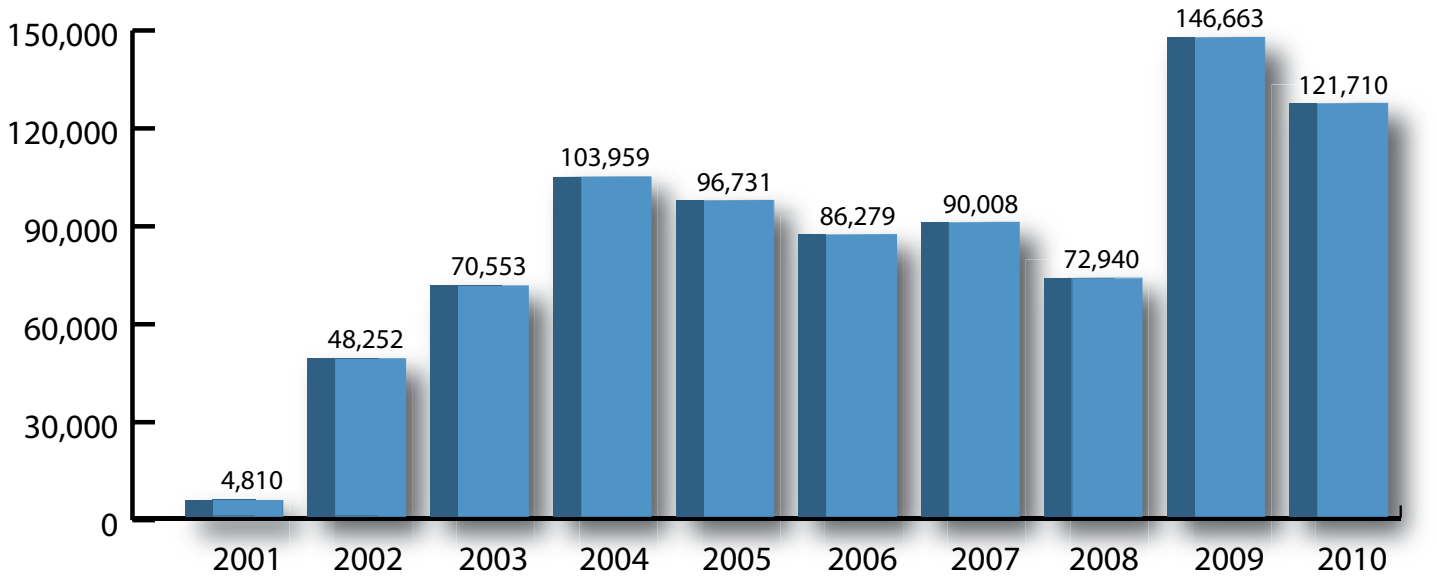


Figure 3: Yearly Number of Referrals



Public Education - Top Five Questions Emailed to IC3

Q: I filed a complaint with IC3. When will I be updated with the status of an investigation?

A: After you file a complaint with IC3, the information is reviewed by an analyst and forwarded to all law enforcement and regulatory agencies with jurisdiction. IC3 does not conduct investigations and is not able to provide the status of filed complaints. Investigation and prosecution is done at the discretion of law enforcement.

The IC3 online complaint form asks victims a number of detailed questions. That information will help investigators with the case.

Q: I received an email asking for my bank account information so that money could be transferred from another country. Should I file a complaint with IC3?

A: Yes, even if you have not lost money. In your complaint, be sure to include as much information as possible (names, email addresses, mailing addresses, etc.). Be sure to copy and paste the entire email, including the header information, in the complaint. For more information, please go to www.ic3.gov and click on Internet Crime Prevention Tips or Internet Crime Schemes. Additionally, to learn more about Internet schemes and ways to protect yourself, please visit www.lookstoogoodtobetrue.com.

Q: I think that I have been defrauded of money or goods. Can I file a complaint with IC3?

A: Yes, include as much information as possible.

Q: I have evidence that supports my complaint information. Can I send it to IC3?

A: IC3 does not collect evidence regarding complaints. While you may include information in our electronic complaint form, you should consider keeping all original documents in a secure location. In the event that law enforcement opens an investigation, they may request the information directly from you.

Q: Am I going to get my money back from my loss?

A: Some states have victim assistance provisions that allow restoration of loss occurring from Internet crime, but that is fairly rare. When complaints are filed at IC3, they are referred to law enforcement with jurisdiction. Procedures and protocol vary across the country, but typically the case would be assigned to an investigator. In nearly all instances, recovery of your loss is contingent on a perpetrator being identified, tried and convicted. To learn more about victim services in your area, contact your state attorney general's office or your local prosecutor's office.

Complaint Characteristics

During 2010, the non-delivery of payment or merchandise was the most reported offense, followed by FBI-related scams and identity theft.

Table 3: Top 10 Crime Types

Type	Percent
1. Non-delivery Payment/Merchandise	14.4%
2. FBI-Related Scams	13.2%
3. Identity Theft	9.8%
4. Computer Crimes	9.1%
5. Miscellaneous Fraud	8.6%
6. Advance Fee Fraud	7.6%
7. Spam	6.9%
8. Auction Fraud	5.9%
9. Credit Card Fraud	5.3%
10. Overpayment Fraud	5.3%

IC3 primarily refers complaints with claims of dollar losses (dollar loss claims). 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. For a more detailed explanation of complaint categories used by IC3, refer to Appendix I.

Table 4: Top 10 Crime Types (Referred Complaints)

Type	Percent
1. Non-delivery Payment/Merchandise	21.1%
2. Identity Theft	16.6%
3. Auction Fraud	10.1%
4. Credit Card Fraud	9.3%
5. Miscellaneous Fraud	7.7%
6. Computer Crimes	6.1%
7. Advance Fee Fraud	4.1%
8. Spam	4.0%
9. Overpayment Fraud	3.6%
10. FBI-Related Scams	3.4%

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

Complainant-Perpetrator Demographics

Investigating and prosecuting cyber crime is unique because the victim and perpetrator can be separated by a few blocks or thousands of miles. Successful investigations often require the cooperation of multiple agencies to resolve cases. Table 5 highlights this truly borderless phenomenon. A minority of perpetrators reside in the same state as the complainants. This underscores the national and global nature of Internet crime and the need for multi-jurisdictional cooperation to combat it.

Table 5: Perpetrators from Same State as Complainant

Type	Percent
1. California	39.1%
2. Florida	30.9%
3. New York	29.4%
4. Washington	27.4%
5. Massachusetts	27.1%
6. Texas	25.4%
7. Arizona	24.6%
8. Oregon	23.0%
9. Illinois	22.3%
10. District of Columbia	21.8%

Complainant Demographics

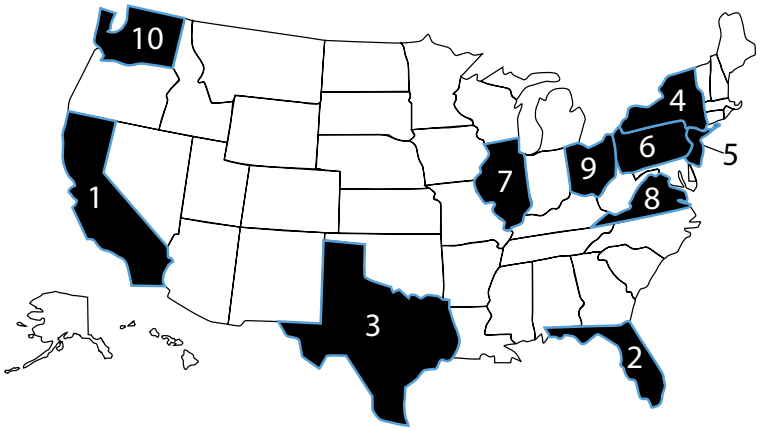
Most complainants were in the U.S., male, between 40 and 59 and a resident of California, Florida, Texas or New York. Most foreign complainants were from Canada, the United Kingdom, Australia or India (see Map 3).

Men reported greater dollar losses than women (at a ratio of $1.25 to every $1.00). Individuals 60-and-over reported higher median amounts of loss than other age groups.

Table 6: Top 10 State Complainant Rates per 100,000 Population

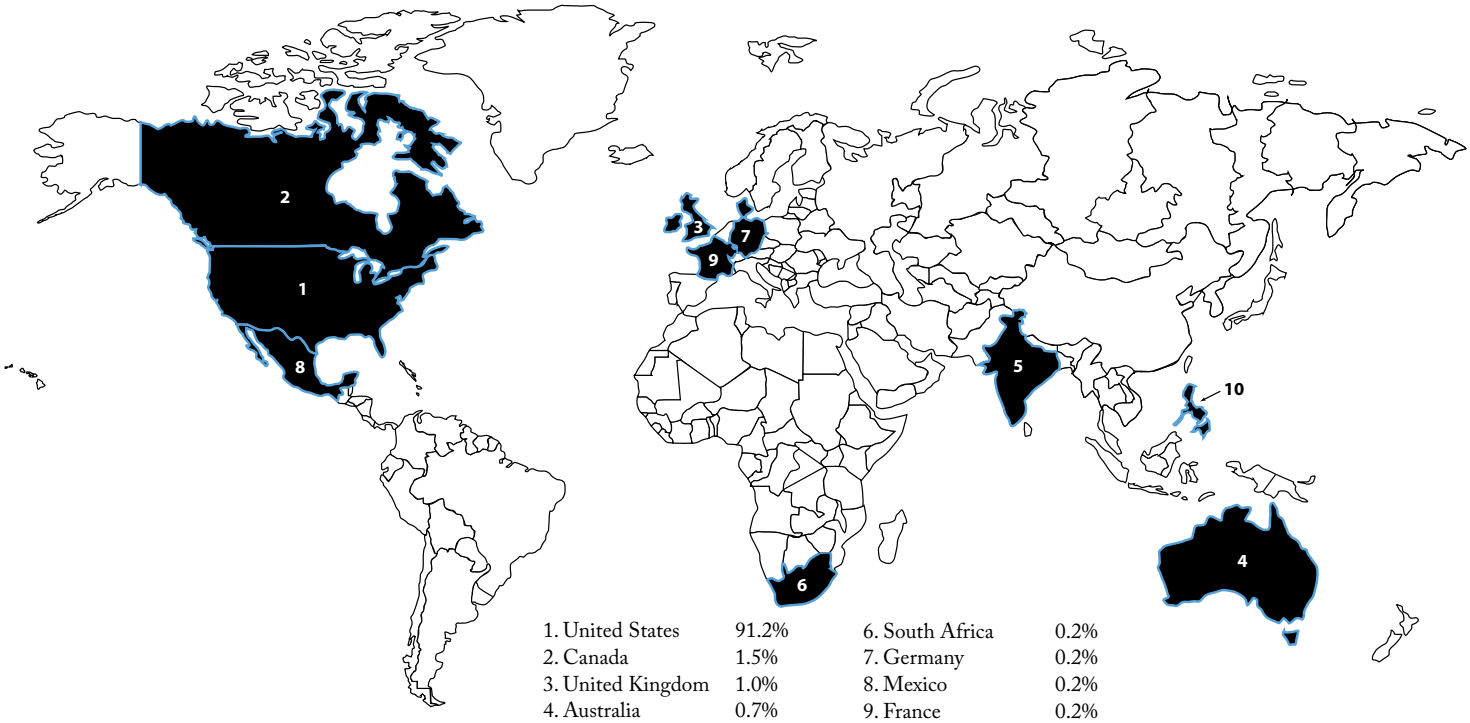
State	Per 100,000 Population
1. Alaska	566.57
2. Colorado	134.99
3. District of Columbia	129.29
4. New Jersey	122.86
5. Nevada	119.19
6. Maryland	117.29
7. Washington	108.06
8. Florida	105.72
9. Arizona	104.27
10. Virginia	93.76

Map 2: Top 10 States by Count: Individual Complainants (Numbered by Rank)



1. California	13.7%	6. Pennsylvania	3.6%
2. Florida	7.9%	7. Illinois	3.3%
3. Texas	7.3%	8. Virginia	3.0%
4. New York	5.8%	9. Ohio	2.9%
5. New Jersey	4.3%	10. Washington	2.9%

Map 3: Top 10 Countries by Count: Individual Complainants (Numbered by Rank)



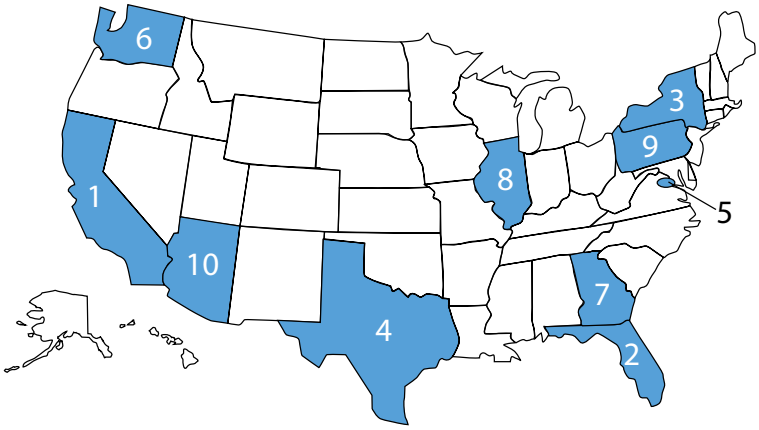
1. United States	91.2%	6. South Africa	0.2%
2. Canada	1.5%	7. Germany	0.2%
3. United Kingdom	1.0%	8. Mexico	0.2%
4. Australia	0.7%	9. France	0.2%
5. India	0.5%	10. Philippines	0.2%

Perpetrator Demographics

In instances where perpetrator information was provided, nearly 75 percent were men and more than half resided in California, Florida, New York, Texas, the District of Columbia or Washington (see Map 4).

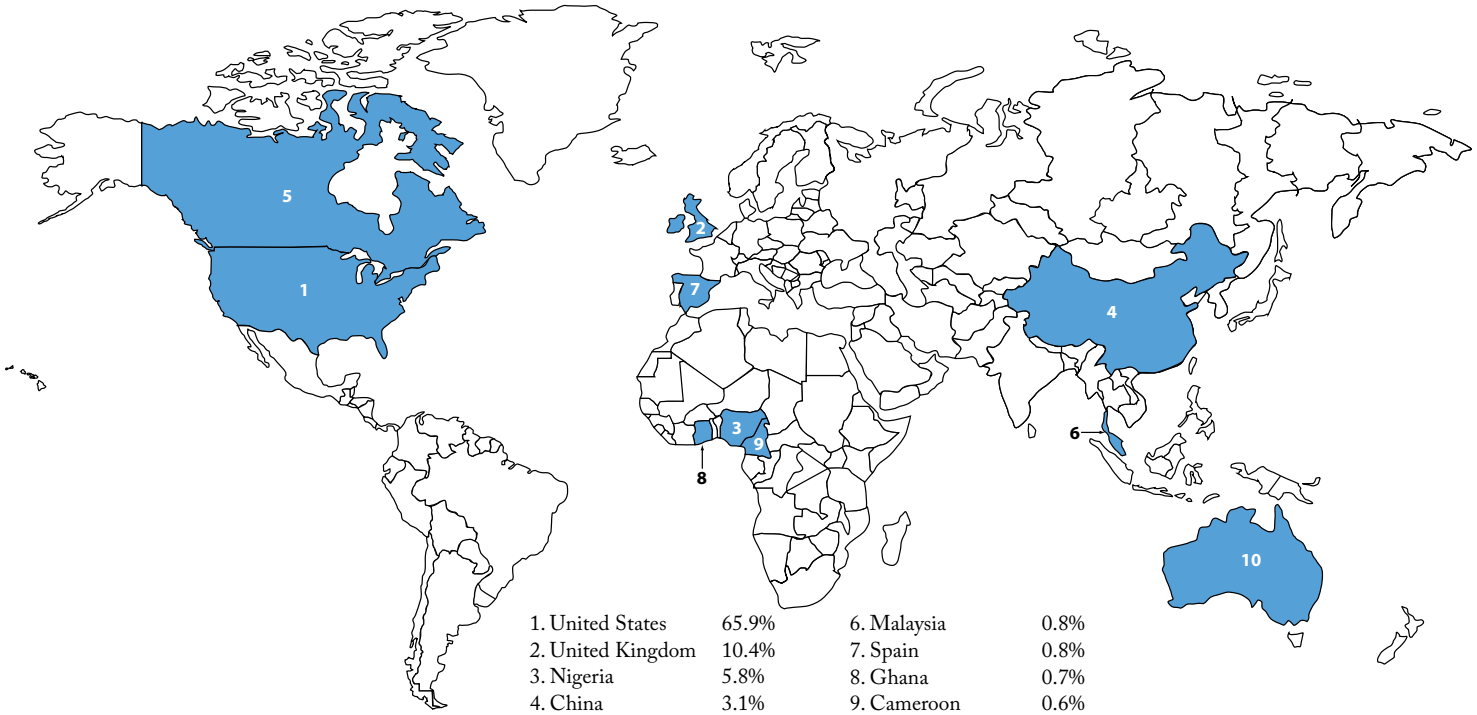
The highest numbers of perpetrators outside the U.S. were from the United Kingdom, Nigeria, and Canada (see Map 5). Refer to Appendix II for more information about perpetrator statistics by state.

Map 4: Top 10 States by Count: Individual Perpetrators (Numbered by Rank)



1. California	15.8%	6. Washington	4.0%
2. Florida	9.8%	7. Georgia	3.9%
3. New York	8.5%	8. Illinois	3.1%
4. Texas	6.9%	9. Pennsylvania	2.6%
5. District of Columbia	5.1%	10. Arizona	2.6%

Map 5: Top 10 Countries by Count: Individual Perpetrators (Numbered by Rank)



1. United States	65.9%	6. Malaysia	0.8%
2. United Kingdom	10.4%	7. Spain	0.8%
3. Nigeria	5.8%	8. Ghana	0.7%
4. China	3.1%	9. Cameroon	0.6%
5. Canada	2.4%	10. Australia	0.5%

Success Stories

"This is excellent. We've already identified several good leads based on the information you were able to extract. Thanks so much for taking the time to help."
Special Agent W. Blake Cook, U.S. State Department, after receiving information on a case from an IC3 analyst.

IC3 does its part to ensure that victims of online crime are heard by giving their complaints to the proper authorities and providing law enforcement with valuable information related to the case. While analysts don't always see the outcome of their work, the evolution of IC3's complaint-handling process has resulted in analysts working more closely with law enforcement, which in turn produces better feedback.

Not So Free Samples

In the one case, a company offered free trial samples of products to victims who paid for the shipping and handling with a credit card. The company then made unauthorized purchases on the cards. A total of 372 complaints were lodged against the company, with reported losses totaling more than $53,000. An IC3 analyst noticed the high volume of complaints and used open-and closed-source analysis to build a case. From there, he referred it to relevant local law enforcement, which opened a joint investigation with the state Attorney General, who remains in constant contact with the IC3 analyst for assistance and updated complaint data.

Fraud on the Wire

A case involving wire transfer fraud involved more than 1,000 complaints, totaling nearly $3 million in reported losses. An IC3 analyst assisted state and local officials with the investigation. The state issued 15 subpoenas and reviewed more than 115 surveillance videos from one specific wire transfer company with offices throughout the state. This case could take several years to reach a full conclusion, but a state law enforcement official acknowledged that IC3 has been "a great resource" in producing needed information for his team. "IC3 is a terrific asset in our fight against major organized fraud schemes and an invaluable ally to law enforcement," the state official said.

False Advertisement

A marketing company promotes its customers' websites through television and online ads. However, the victims are often left empty-handed with no advertisement of their business, and the company stops any form of communication with them. IC3 originally sent this case to the federal officials of relevant jurisdiction with 15 complaints that reported losses of more than $130,000. Based on the conversation between the IC3 analyst and federal law enforcement, this case has exploded in scope. The number of victims reached the hundreds, and reported losses totaled more than $20 million. Federal law enforcement continues to investigate this case and regularly contacts IC3 for further complaints and information.

International Assistance

In April 2010, Romanian National Police charged 70 people for their roles in an organized crime group engaged in Internet fraud. In one of the country's largest-ever police actions, over 700 law enforcement officers conducted arrests and searches at 103 locations, while at the same time, police in the Czech Republic searched 10 locations and arrested 11 Romanian nationals.

In an 18-month period, Romanian police and prosecutors conducted more than 500 wiretaps and identified over 1,200 victims, approximately half of them Americans. The total loss was over $2 million.

The FBI Legal Attache in Bucharest and the Romanian Threat Focus Cell Cyber Task Force, including IC3, played a vital role in assisting the Romanian police in gathering evidence for their investigations of the subjects.

IC3 identified additional victims subjects. IC3 used victim-provided information such as subject addresses, email addresses, telephone numbers, and fax numbers to make initial investigative connections, which the Romanian National police developed further.

IC3 provided more than 600 victim complaints for a total of $2.7 million in reported losses, and assisted, along with multiple FBI Field Offices, in obtaining more than 100 signed Romanian police affidavits from victims.

IC3 Scam Alerts of 2010

Mystery/Secret Shopper Schemes

Source: IC3

Date: January 14, 2010

IC3 has been alerted to an increase in employment schemes pertaining to mystery/secret shopper positions. Many retail and service corporations hire evaluators to perform secret or random checks on themselves or their competitors, and fraudsters are capitalizing on this employment opportunity.

Victims have reported to IC3 they were contacted via e-mail and U.S. mail to apply to be a mystery shopper. Applicants are asked to send a resume and are purportedly subject to an extensive background check before being accepted as a mystery shopper. The employees are sent a check with instructions to shop at a specified retailer for a specific length of time and spend a specific amount on merchandise from the store. The employees receive instructions to take note of the store's environment, color, payment procedures, gift items, and shopping/carrier bags and report back to the employer. The second evaluation is the ease and accuracy of wiring money from the retail location. The money to be wired is also included in the check sent to the employee. The remaining balance is the employee's payment for the completion of the assignment. After merchandise is purchased and money is wired, the employees are advised by the bank the check cashed was counterfeit, and they are responsible for the money lost in addition to bank fees incurred.

In other versions of the scheme, applicants are requested to provide bank account information to have money directly deposited into their accounts. The fraudster then has acquired access to these victims' accounts and can withdraw money, which makes the applicant a victim of Identity Theft.

Tips

Here are some tips you can use to avoid becoming a victim of employment schemes associated with mystery/secret shopping:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Virus scan all attachments, if possible.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link you are actually directed to and determine if they match and will lead you to a legitimate site.
- There are legitimate mystery/secret shopper programs available. Research the legitimacy on companies hiring mystery shoppers. Legitimate companies will not charge an application fee and will accept applications on-line.
- No legitimate mystery/secret shopper program will send payment in advance and ask the employee to send a portion of it back.

Individuals who believe they have information pertaining to mystery/secret shopper schemes are encouraged to file a complaint at www.ic3.gov.

New Twist on Counterfeit Check Schemes Targeting U.S. Law Firms

Source: IC3

Date: January 21, 2010

The FBI continues to receive reports of counterfeit check scheme targeting U.S. law firms. As previously reported, scammers send e-mails to lawyers, claiming to be overseas and seeking legal representation to collect delinquent payments from third parties in the U.S. The law firm receives a retainer agreement, invoices reflecting the amount owed, and a check payable to the law firm. The firm is instructed to extract the retainer fee, including any other fees associated with the transaction, and wire the remaining funds to banks in Korea, China, Ireland, or Canada. By the time the check is determined to be counterfeit, the funds have already been wired overseas.

In a new twist, the fraudulent client seeking legal representation is an ex-wife "on assignment" in an Asian country, and she claims to be pursuing a collection of divorce settlement monies from her ex-husband in the U.S. The law firm agrees to represent the ex-wife, sends an e-mail to the ex-husband, and receives a "certified" check for the settlement via delivery service. The ex-wife instructs the firm to wire the funds, less the retainer fee, to an overseas bank account. When the scam is executed successfully, the law firm wires the money before discovering the check is counterfeit.

All Internet users need to be cautious when they receive unsolicited e-mails. Law firms are advised to conduct as much due diligence as possible before engaging in transactions with parties who are handling their

business solely via e-mail, particularly those parties claiming to reside overseas.

Please view an additional public service announcement posted to the IC3 Web site regarding a similar Asian Extortion Scheme located at the following link, http://www.ic3.gov/media/2009/090610.aspx. Individuals who receive information pertaining to counterfeit check schemes are encouraged to file a complaint at www.ic3.gov.

National Center for Disaster Fraud to Coordinate Haitian and Chilean Fraud Complaints

Source: U.S. Department of Justice
FBI
Date: March 10, 2010

Shortly after the earthquake in Haiti last January, the FBI and the National Center for Disaster Fraud (NCDF) established a telephone hotline to report suspected fraud associated with relief efforts. That number, (866) 720-5721, was initially staffed for the purpose of reporting suspected scams being perpetrated by criminals in the aftermath of the Haitian earthquake. Since then with the recent earthquake in Chile our efforts have expanded to identify similar fraud activity coming out of that disaster. Therefore the public is encouraged to call this same number (866) 720-5721 to report suspected fraud from either disaster. The telephone line is staffed by a live operator 24 hours a day, seven days a week. Additionally, e-mail information can be directly sent to disaster@leo.gov.

The National Center for Disaster Fraud was originally established by the Department of Justice to investigate, prosecute, and deter fraud in the wake of Hurricane Katrina, when billions of dollars in federal disaster relief poured into the Gulf Coast Region. Now, its mission has expanded to include suspected fraud from any natural or manmade disaster. More than 20 federal agencies, including the FBI, participate in the NCDF, allowing the center to act as a centralized clearinghouse of information related to Haitian or Chilean Relief Fraud.

The FBI continues to remind the public to apply a critical eye and do their due diligence before giving contributions to anyone soliciting donations on behalf of Haitian or Chilean victims. Solicitations can originate from e-mails, websites, door-to-door collections, mailings and telephone calls, and similar methods.

Therefore, before making a donation of any kind, consumers should adhere to certain guidelines, including the following:

- Do not respond to any unsolicited (spam) incoming e-mails, including clicking links contained within those messages because they may contain computer viruses.
- Be skeptical of individuals representing themselves as surviving victims or officials asking for donations via e-mail or social networking sites.
- Beware of organizations with copy-cat names similar to but not exactly the same as those of reputable charities.
- Rather than following a purported link to a website, verify the legitimacy of non-profit organizations by utilizing various Internet-based resources that may assist in confirming the group's existence and its non-profit status.
- Be cautious of e-mails that claim to show pictures of the disaster areas in attached files, because the files may contain viruses. Only open attachments from known senders.
- To ensure contributions are received and used for intended purposes, make contributions directly to known organizations rather than relying on others to make the donation on your behalf.
- Do not be pressured into making contributions, as reputable charities do not use such tactics.
- Do not give your personal or financial information to anyone who solicits contributions. Providing such information may compromise your identity and make you vulnerable to identity theft.
- Avoid cash donations if possible. Pay by debit or credit card, or write a check directly to the charity. Do not make checks payable to individuals.
- Legitimate charities do not normally solicit donations via money transfer services.
- Most legitimate charities websites end in .org rather than .com.
- There are scams targeting Haitian immigrants and their families offering assistance in getting family members and friends out of Haiti. These individuals charge a fee and then claim they will provide the necessary immigration paperwork or an airline ticket for disaster victims to leave Haiti. For official information pertaining to immigration from Haiti to the U.S., visit the U.S. Citizenship and Immigration Services (USCIS) website at www.USCIS.gov.

If you believe you have been a victim of fraud from a person or an organization soliciting relief funds on behalf of Haitian or Chilean earthquake victims, contact the National Center for Disaster Fraud at (866) 720-5721. You can also fax information to (225) 334-4707 or e-mail it to disaster@leo.gov.

You can also report suspicious e-mail solicitations or fraudulent websites to the FBI's Internet Crime Complaint Center at www.ic3.gov.

Rental and Real Estate Scams

Source: IC3
Date: March 11, 2010

Individuals need to be cautious when posting rental properties and real estate on-line. IC3 continues to receive numerous complaints from individuals who have fallen victim to scams involving rentals of apartments and houses, as well as postings of real estate on-line.

Rental scams occur when the victim has rental property advertised and is contacted by an interested party. Once the rental price is agreed-upon, the scammer forwards a check for the deposit on the rental property to the victim. The check is to cover housing expenses and is, either written in excess of the amount required, with the scammer asking for the remainder to be remitted back, or the check is written for the correct amount, but the scammer backs out of the rental agreement and asks for a refund. Since the banks do not usually place a hold on the funds, the victim has immediate access to them and believes the check has cleared. In the end, the check is found to be counterfeit and the victim is held responsible by the bank for all losses.

Another type of scam involves real estate that is posted via classified advertisement websites. The scammer duplicates postings from legitimate real estate websites and reposts these ads, after altering them. Often, the scammers use the broker's real name to create a fake email, which gives the fraud more legitimacy. When the victim sends an email through the classified advertisement website inquiring about the home, they receive a response from someone claiming to be the owner. The "owner" claims he and his wife are currently on missionary work in a foreign country. Therefore, he needs someone to rent their home while they are away. If the victim is interested in renting the home, they are asked to send money to the owner in the foreign country.

If you have been a victim of Internet crime, please file a complaint at http://www.ic3.gov/.

Fraudulent Telephone Calls Allowing Fraudsters Access to Consumer Financial and Brokerage Accounts

Source: IC3
Date: June 21, 2010

The FBI Newark Division released a warning to consumers concerning a new scheme using telecommunications denial-of-service (TDoS) attacks. The FBI determined fraudsters compromised victim accounts and contacted financial institutions to change the victim profile information (i.e., email addresses, telephone numbers and bank account numbers).

The TDoS attacks used automated dialing programs and multiple accounts to overwhelm victims' cell phones and land lines with thousands of calls. When victims answered the calls they heard dead air (nothing on the other end), an innocuous recorded message, advertisement, or a telephone sex menu. Calls were typically short in duration but so numerous that victims changed their phone numbers to terminate the attack.

These TDoS attacks were used as a diversion to prevent financial and brokerage institutions from verifying victim account changes and transactions. Fraudsters were afforded adequate time to transfer funds from victim brokerage and financial online accounts.

Protection from TDoS attacks and other types of fraud requires consumers to be vigilant and proactive. In Newark's Public Service Announcement (PSA), they recommend consumers protect themselves by:

- Implement security measures for all financial accounts by placing fraud alerts with the major credit bureaus if you believe they were targeted by a TDOS attack or other forms of fraud.
- Use strong passwords for all financial accounts and change them regularly.
- Obtain and review your annual credit report for fraudulent activity.

If you were a target of a TDoS attack, immediately contact your financial institutions, notify your telephone provider, and promptly report it to IC3 website at: www.ic3.gov. The IC3 complaint database links complaints to assist in referrals to the appropriate law enforcement agency for case consideration. The complaint information is also used to identity emerging trends and patterns.

To learn more about the FBI's role in addressing these attacks please refer to the FBI Newark Division, PSA dated May 11, 2010, located at: http://newark.fbi.gov/press.htm.

Claims of Being Stranded Swindle Consumers Out of Thousands of Dollars

Source: IC3
Date: July 2, 2010

IC3 continues to receive reports of individuals' e-mail or social networking accounts being compromised and used in a social engineering scam to swindle consumers

out of thousands of dollars. Portraying to be the victim, the hacker uses the victim's account to send a notice to their contacts. The notice claims the victim is in immediate need of money due to being robbed of their credit cards, passport, money, and cell phone; leaving them stranded in London or some other location. Some claim they only have a few days to pay their hotel bill and promise to reimburse upon their return home. A sense of urgency to help their friend/contact may cause the recipient to fail to validate the claim, increasing the likelihood of them falling for this scam.

If you receive a similar notice and are not sure it is a scam, you should always verify the information before sending any money.

If you have been a victim of this type of scam or any other Cyber crime, you can report it to the IC3 website at: www.ic3.gov. The IC3 complaint database links complaints for potential referral to the appropriate law enforcement agency for case consideration. Complaint information is also used to identity emerging trends and patterns.

Fraudulent Notifications Deceive Consumers Out of Thousands of Dollars

Source: IC3

Date: November 8, 2010

IC3 continues to receive reports of letters and emails being distributed as part of a prize sweepstakes or lottery scheme. The scheme uses fraudulent checks bearing the logos of various financial institutions.

Individuals are informed they won a sweepstakes or lottery and will receive a lump sum payout if they pay taxes and processing fees upfront. The communication directs individuals to call a telephone number to secure their unclaimed prize, and receive instructions for paying the upfront taxes and fees. A fraudulent check is enclosed with the letter, or sent after the initial call, in the amount of the supposed taxes. The instructions inform the individual to cash the check and wire the proceeds, in order to receive the payout. Following these instructions leaves the victim liable for the amount of the counterfeit check, plus any additional fees charged by their bank. Recipients of the communication may fall victim to the scheme due to the allure of easy money and the apparent legitimacy of the check. The alleged cash prizes and locations of the financial institutions vary.

If you receive a similar notice you should always verify the information before sending any money.

Tips to avoid being scammed:

- A federal statute prohibits mailing lottery tickets, advertisements, or payments to purchase tickets in a foreign lottery.
- Be leery if you do not remember entering a lottery or sweepstakes.
- Beware of lotteries or sweepstakes that charge a fee prior to delivery of your prize.
- Be wary of demands to send additional money to be eligible for future winnings.

If you have been a victim of this type of scam or any other cyber crime, you can report it to the IC3 website at: www.ic3.gov. The IC3 complaint database links complaints for potential referral to law enforcement for case consideration. Complaint information is also used to identify emerging trends and patterns to alert the public to new criminal schemes.

Telephone Collection Scams Related to Delinquent Payday Loans

Source: IC3

Date: December 1, 2010

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 companies such as United Cash Advance, U.S. Cash Advance, U.S. Cash Net, and other internet check cashing services.

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, 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 victim's home, cell phone, and place of employment. They refuse to provide to 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 victim's relatives, friends, and employers.

Some fraudsters instruct victims to fax a statement agreeing to pay a certain dollar amount, on a specific date, via prepaid visa card. The statement further declares that the victim would never dispute the debt.

THESE TELEPHONE CALLS ARE AN ATTEMPT TO OBTAIN PAYMENT BY INSTILLING FEAR IN THE VICTIMS. DO NOT FOLLOW THE INSTUCTIONS OF THE CALLER.

If you receive telephone calls such as these, you should:

- Contact your banking institutions;
- Contact the three major credit bureaus and request an alert be put on your file;
- Contact your local law enforcement agencies if you feel you are in immediate danger;
- File a complaint at www.ic3.gov.

Conclusion

As the 2010 Internet Crime Report shows, the effects of online crime cut across all demographic groups and span the globe. IC3 has demonstrated its ability to adapt to the ever-changing landscape of Internet crime by providing the latest technological tools to assist law enforcement in bringing perpetrators to justice.

The combined power of IC3's CMS, ICSIS and Automatch streamlines the way complaints are processed and referred.

The expert analysis IC3 provides to law enforcement fosters greater collaboration between investigators in multiple jurisdictions.

As this report demonstrates, cyber criminals have become more creative in devising ways to separate Internet users from their money. IC3 has evolved to keep pace with emerging trends and technology, becoming an indispensible asset to victims of online crime and to law enforcement.

Law enforcement officers in Indiana attend ICSIS training.

Appendix I

Definitions of Complaint Types

- **Non-Delivery Payment/Merchandise (non-auction)** – Purchaser did not receive items purchased, or seller did not receive payment for items sold.
- **FBI-Related Scams** – Scams in which a criminal poses as the FBI to defraud victims.
- **Identity Theft** – Unauthorized use of victim's personally identifying information to commit fraud or other crimes.
- **Computer Crimes** –1) Crimes that target computer networks or devices directly or 2) crimes facilitated by computer networks or devices.
- **Miscellaneous Fraud** – Variety of scams meant to defraud the public, such as work-at-home scams, fraudulent sweepstakes and contests, and other fraudulent schemes.
- **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.
- **Spam** – Mass-produced, unsolicited bulk messages.
- **Auction Fraud** – Fraudulent transactions that occur in the context of an online auction site.
- **Credit Card Fraud** – Fraudulent, unauthorized charging of goods and services to a victim's credit card.
- **Overpayment Fraud** – An incident in which the complainant receives an invalid monetary instrument with instructions to deposit it in a bank account and to send excess funds or a percentage of the deposited money back to the sender.

Table 7 - Complaint Categories and Subcategories

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

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

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

Appendix II
Complainant/Perpetrator Statistics

Table 8: Complainant Statistics by State*

Rank	State	Percent	Rank	State	Percent
1	California	13.7%	**27**	South Carolina	1.2%
2	Florida	7.9%	**28**	Louisiana	1.1%
3	Texas	7.3%	**29**	Connecticut	1.0%
4	New York	5.8%	**30**	Kentucky	1.0%
5	New Jersey	4.3%	**31**	Oklahoma	0.9%
6	Pennsylvania	3.6%	**32**	Utah	0.9%
7	Illinois	3.3%	**33**	Kansas	0.8%
8	Virginia	3.0%	**34**	Arkansas	0.7%
9	Ohio	2.9%	**35**	New Mexico	0.7%
10	Washington	2.9%	**36**	Iowa	0.6%
11	Michigan	2.7%	**37**	Mississippi	0.5%
12	Colorado	2.7%	**38**	West Virginia	0.5%
13	Maryland	2.7%	**39**	Idaho	0.5%
14	Arizona	2.6%	**40**	New Hampshire	0.5%
15	Georgia	2.6%	**41**	Hawaii	0.4%
16	North Carolina	2.5%	**42**	Maine	0.4%
17	Tennessee	1.9%	**43**	Nebraska	0.4%
18	Massachusetts	1.9%	**44**	Montana	0.3%
19	Indiana	1.8%	**45**	District of Columbia	0.3%
20	Missouri	1.6%	**46**	Rhode Island	0.3%
21	Alaska	1.6%	**47**	Delaware	0.3%
22	Oregon	1.4%	**48**	Vermont	0.2%
23	Wisconsin	1.4%	**49**	Wyoming	0.2%
24	Minnesota	1.4%	**50**	South Dakota	0.2%
25	Alabama	1.3%	**51**	North Dakota	0.1%
26	Nevada	1.3%			

**Numbers shown are the percentage of total individual complainants within the United States, in which the state is known.*

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

Table 9: Perpetrator Statistics by State*

Rank	State	Percent	Rank	State	Percent
1	California	15.8%	**27**	South Carolina	0.9%
2	Florida	9.8%	**28**	Montana	0.9%
3	New York	8.5%	**29**	Alabama	0.9%
4	Texas	6.9%	**30**	Wisconsin	0.8%
5	District of Columbia	5.1%	**31**	Louisiana	0.8%
6	Washington	4.0%	**32**	Kentucky	0.7%
7	Georgia	3.9%	**33**	Oklahoma	0.7%
8	Illinois	3.1%	**34**	Nebraska	0.6%
9	Pennsylvania	2.6%	**35**	Kansas	0.6%
10	Arizona	2.6%	**36**	Maine	0.5%
11	New Jersey	2.4%	**37**	Delaware	0.5%
12	Ohio	2.3%	**38**	Alaska	0.5%
13	Michigan	2.2%	**39**	Arkansas	0.4%
14	Nevada	2.2%	**40**	Iowa	0.4%
15	North Carolina	2.1%	**41**	Mississippi	0.3%
16	Virginia	1.9%	**42**	New Mexico	0.3%
17	Colorado	1.8%	**43**	Hawaii	0.3%
18	Maryland	1.7%	**44**	Idaho	0.3%
19	Massachusetts	1.6%	**45**	Rhode Island	0.3%
20	Tennessee	1.4%	**46**	West Virginia	0.3%
21	Indiana	1.4%	**47**	New Hampshire	0.3%
22	Minnesota	1.1%	**48**	North Dakota	0.2%
23	Missouri	1.0%	**49**	Wyoming	0.2%
24	Utah	1.0%	**50**	South Dakota	0.1%
25	Oregon	1.0%	**51**	Vermont	0.1%
26	Connecticut	0.9%			

**Numbers shown are the percentage of total individual perpetrators within the United States, in which the state is known.*

(Please note that percentages contained in the table above do not total 100 percent. The table above only represents statistics from 50 states and the District of Columbia. The table above does not represent statistics from other U.S. territories or Canada. The District of Columbia's numbers may be inflated by the number of FBI-related scams, in which complainants believe the incident has taken place in D.C., even though often the perpetrator is not based there.)

Table 10: Complainants per 100,000 Population*

Rank	State	Per 1,000	Rank	State	Per 1,000
1	Alaska	566.57	**27**	Texas	73.01
2	Colorado	134.99	**28**	Indiana	71.94
3	District of Columbia	129.29	**29**	Pennsylvania	71.64
4	New Jersey	122.86	**30**	Connecticut	71.37
5	Nevada	119.19	**31**	Alabama	70.54
6	Maryland	117.29	**32**	Missouri	69.42
7	Washington	108.06	**33**	Michigan	68.69
8	Florida	105.72	**34**	West Virginia	67.99
9	Arizona	104.27	**35**	Georgia	67.74
10	Virginia	93.76	**36**	Rhode Island	67.64
11	California	92.89	**37**	North Carolina	67.15
12	Oregon	92.63	**38**	Illinois	65.70
13	New Hampshire	87.96	**39**	South Carolina	65.31
14	Utah	86.14	**40**	Minnesota	65.31
15	Montana	85.20	**41**	Oklahoma	63.81
16	Wyoming	84.45	**42**	Ohio	63.31
17	Vermont	84.37	**43**	Arkansas	62.45
18	Hawaii	82.77	**44**	Wisconsin	61 .29
19	New Mexico	81.24	**45**	Louisiana	59.24
20	Idaho	79.48	**46**	Kentucky	57.49
21	Delaware	78.29	**47**	Nebraska	52.56
22	Tennessee	76.83	**48**	Iowa	50.71
23	New York	75.80	**49**	North Dakota	48.76
24	Massachusetts	74.16	**50**	South Dakota	47.28
25	Maine	73.39	**51**	Mississippi	44.24
26	Kansas	73.14			

**Based on 2010 Census figures*

Table 11: Perpetrators per 100,000 Population*

Rank	State	Per 1,000	Rank	State	Per 1,000
1	District of Columbia	833.43	**27**	Virginia	22.88
2	Montana	87.62	**28**	Vermont	22.21
3	Nevada	79.28	**29**	North Carolina	21.83
4	Alaska	68.42	**30**	Michigan	21.70
5	Washington	58.71	**31**	Tennessee	21.43
6	Delaware	54.45	**32**	Minnesota	21.30
7	Florida	51.25	**33**	Indiana	20.60
8	New York	43.51	**34**	Pennsylvania	20.37
9	California	41.86	**35**	Ohio	19.42
10	Arizona	40.15	**36**	Idaho	19.39
11	Georgia	39.32	**37**	Kansas	19.17
12	Maine	38.54	**38**	South Carolina	18.96
13	Utah	36.65	**39**	New Hampshire	18.99
14	Colorado	35.73	**40**	Alabama	18.01
15	North Dakota	34.49	**41**	Louisiana	17.93
16	Nebraska	30.77	**42**	South Dakota	17.56
17	Wyoming	29.09	**43**	Oklahoma	17.16
18	Maryland	28.56	**44**	Missouri	17.04
19	Rhode Island	27.93	**45**	New Mexico	16.02
20	Texas	27.16	**46**	Kentucky	15.73
21	New Jersey	26.42	**47**	West Virginia	15.43
22	Oregon	25.84	**48**	Arkansas	14.84
23	Connecticut	24.56	**49**	Wisconsin	14.29
24	Massachusetts	24.08	**50**	Iowa	12.53
25	Illinois	23.64	**51**	Mississippi	11.18
26	Hawaii	23.52			

**Based on 2010 Census figures*

(The District of Columbia's numbers may be inflated by the number of FBI-related scams, in which complainants believe the incident has taken place in D.C., even though often the perpetrator is not based there.)

www.ic3.gov