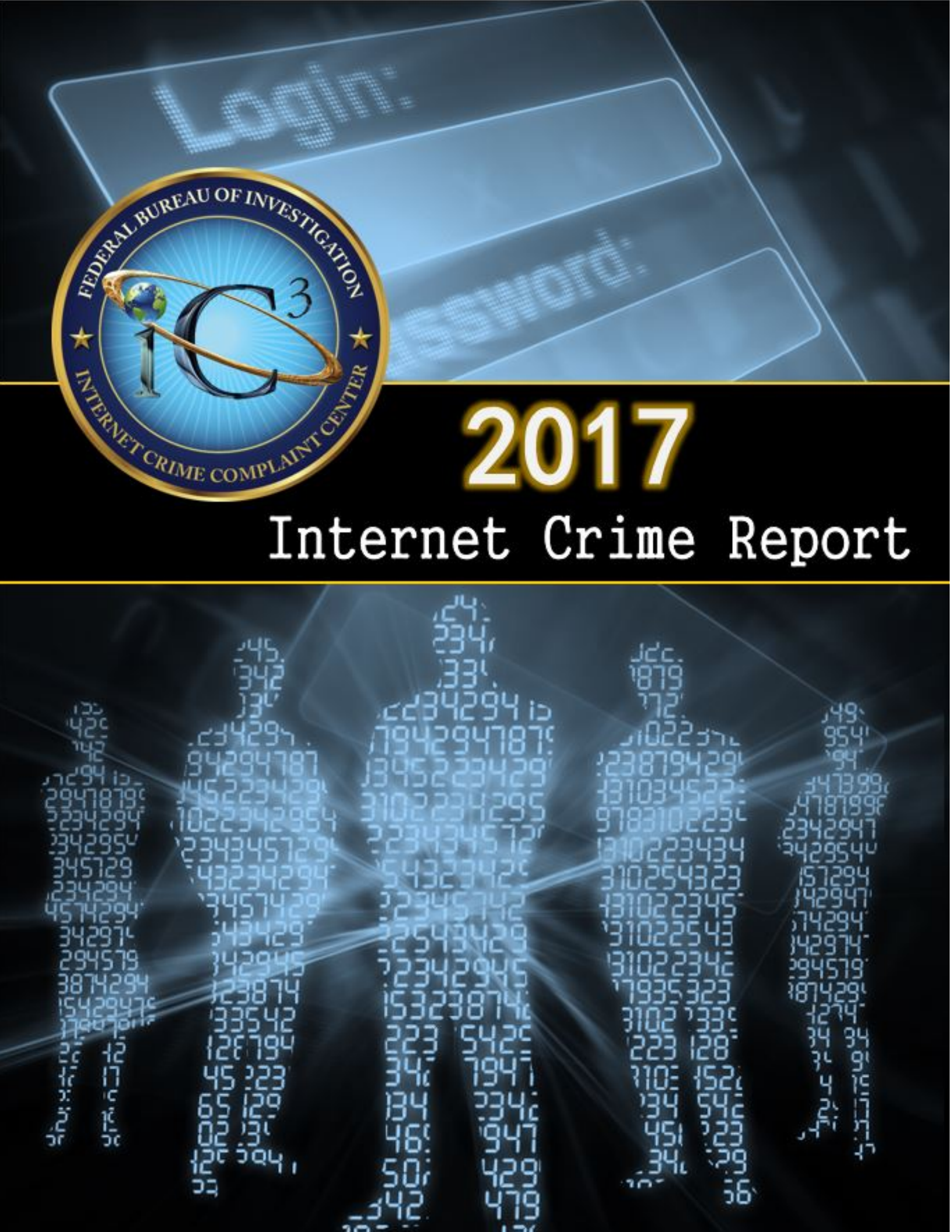


2017 Internet Crime Report

2017 Internet Crime Report

Table of Contents

Introduction **3**

About the Internet Crime Complaint Center **4**

IC3 History 4

The IC3 Role in Combating Cyber Crime 5

Collection 5

Analysis 6

Public Awareness 6

Referrals 6

Supporting Law Enforcement **7**

IC3 Database Remote Access 7

Successes 7

Operation Wellspring (OWS) Initiative 9

Hot Topics for 2017 ..... **12**

Business Email Compromise (BEC) 12

Ransomware 13

Tech Support Fraud 14

Elder Justice Initiative 15

Extortion 16

2017 Overall Statistics **17**

2017 Victims by Age Group **17**

Top 20 Foreign Countries by Victim **18**

Top 10 States by Number of Victims **19**

Top 10 States by Victim Loss **19**

2017 Crime Types **20**

2017 Overall State Statistics **22**

Appendix A: Crime Type Definitions **26**

Introduction

Dear Reader,

2017 was a milestone year for the FBI's Internet Crime Complaint Center (IC3). On October 12, 2017, at 4:10pm, the IC3 received its 4 millionth consumer internet crime complaint.

As the lead federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists, the FBI's IC3 provides the public with a trustworthy and convenient reporting mechanism to submit information concerning suspected Internet-facilitated criminal activity. The IC3 also strengthens the FBI's partnerships with our law enforcement and private industry partners. As cyber criminals become more sophisticated in their efforts to target victims, we must continue to transform and develop in order to address the persistent and evolving cyber threats we face.

The 2017 Internet Crime Report emphasizes the IC3's efforts in monitoring trending scams such as Business Email Compromise (BEC), Ransomware, Tech Support Fraud, and Extortion. The report also highlights the Elder Justice Initiative promoting justice for the nation's seniors. In 2017, IC3 received a total of 301,580 complaints with reported losses exceeding $1.4 Billion.

This past year, the most prevalent crime types reported by victims were Non-Payment/Non-Delivery, Personal Data Breach, and Phishing. The top three crime types with the highest reported loss were BEC, Confidence/Romance fraud, and Non-Payment/Non-Delivery.

This year's report features success stories from two different successful cases initiated from IC3 complaints. Additionally, the Operation Wellspring (OWS) Initiative continues to build the cyber investigative capability by utilizing Cyber Task Force officers, thus strengthening state and local law enforcement collaboration.

We hope this report provides additional information of value as we work together to protect our nation against cyber threats.

Scott S. Smith

Assistant Director

Cyber Division

Federal Bureau of Investigation

About the Internet Crime Complaint Center

The mission of the FBI is to protect the American people and uphold the Constitution of the United States.

The mission of the IC3 is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity, and to develop effective alliances with industry partners. Information is analyzed and disseminated for investigative and intelligence purposes, for law enforcement, and for public awareness.

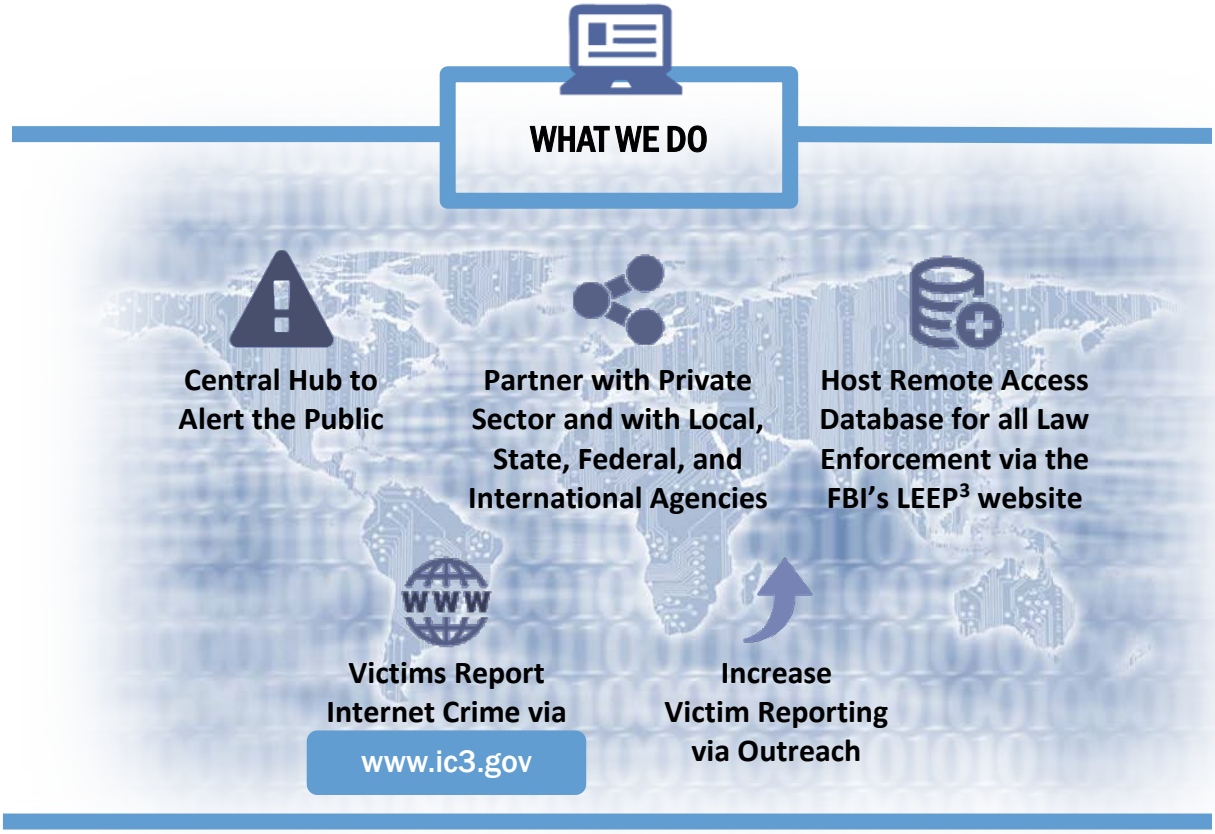
In an effort to promote public awareness, the IC3 produces this annual report to aggregate and highlight the data provided by the general public. The quality of the data is directly attributable to the information ingested via the public interface www.ic3.gov. The IC3 attempts to standardize the data by categorizing each complaint based on the information provided. The IC3 staff analyzes the data to identify trends in Internet-facilitated crimes and what those trends may represent in the coming year.

IC3 History

In May 2000, the IC3 was established as a center to receive complaints of Internet crime. There have been 4,063,933 complaints reported to the IC3 since its inception. Over the last five years, the IC3 has received an average of more than 284,000 complaints per year. The complaints address a wide array of Internet scams affecting victims across the globe.[1]

[1] Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2013 to 2017. Over that time period, IC3 received a total of 1,420,555 complaints, and a total reported loss of $5.52 billion.

The IC3 Role in Combating Cyber Crime[2]



Collection

Victims are encouraged and often directed by law enforcement to file a complaint online at www.ic3.gov. Complainants are asked to document accurate and complete information related to the Internet crime, as well as any other relevant information necessary to support the complaint. In addition to reporting the crime via www.ic3.gov, complainants should take steps to mitigate further loss. Victims can take actions such as contacting banks, credit card companies, and/or credit bureaus to block accounts, freeze accounts, dispute charges, or attempt recovery of lost funds. Victims should be diligent in reviewing credit reports to dispute any unauthorized transactions and should also consider credit monitoring services.

---

[2] Accessibility description - image depicts what IC3 does to include providing a central hub to alert the public: partner with private sector and with local, state, federal, and international agencies; host a remote access database for all law enforcement via the FBI's LEEP website; victim reporting at www.ic3.gov; and increase victim reporting via outreach.

[3] Federal Bureau of Investigation. Law Enforcement Enterprise Portal (LEEP)

Analysis

The IC3 is the central point for Internet crime victims to report and alert the appropriate agencies to suspected criminal Internet activity. The IC3 reviews and analyzes data submitted through its website, and produces intelligence products to highlight emerging threats and new trends.

Public Awareness

Public service announcements (PSAs), scam alerts, and other publications outlining specific scams are posted to the www.ic3.gov website. As more people become aware of Internet crimes and the methods utilized to carry them out, potential victims are equipped with a broader understanding of the dangers associated with Internet activity and are in a better position to avoid falling prey to schemes online.

IC3 Core Functions[4]

Referrals

The IC3 aggregates related complaints to build referrals, which are forwarded to local, state, federal, and international law enforcement agencies for potential investigation. If law enforcement conducts an investigation and determines a crime has been committed, legal action may be brought against the perpetrator.

[4] Accessibility description: image contains the IC3 logo against a digital background. Core functions are listed in individual blocks- Collection, Analysis, Public Awareness, and Referrals as components of an ongoing process.

Supporting Law Enforcement

IC3 Database Remote Access

All sworn law enforcement can remotely access and search the IC3 database through the FBI's Law Enforcement Enterprise Portal (LEEP).

LEEP is a gateway providing law enforcement agencies, intelligence groups, and criminal justice entities access to beneficial resources all in one centralized location. These resources can be used to strengthen case development for investigators and enhance information sharing between agencies. This web-based access additionally provides users the ability to identify and aggregate victims and losses within a jurisdiction.

The IC3 expanded the remote search capabilities of the IC3 database by allowing users to gather IC3 complaint statistics. Users now have the ability to run city, state, county, and country reports and sort by crime type, age, and transactional information. The user can also run overall crime type reports and sort by city, state, and country. The report results can be returned as a portable document format (PDF) or exported to Excel. This search capability allows users to better understand the scope of cyber crime in their area of jurisdiction and enhance cases.

Successes

International Investment Scam: FBI Houston

Beginning in 2015, the IC3 provided multiple complaints to FBI Houston regarding an elaborate investment scheme. The scheme involved the impersonation of Branch Banking & Trust (BB&T) and JPMorgan Chase (Chase) executives, the fabrication of U.S. government documents, the creation of fraudulent investment agreements in the name of BB&T and Chase, and the purchase of luxury vehicles to launder the proceeds of the scheme. It was perpetrated by individuals primarily living in West Africa, who impersonated U.S. bank officials and financial consultants, and made fraudulent offers of investment funding to victims all over the world via the Internet and phone. Victims were deceived into believing they would receive millions of dollars of investment funding as part of joint ventures with U.S. banks, usually BB&T or Chase. The perpetrators utilized false domain names to make it appear their emails were affiliated with BB&T or Chase. To convince victims the opportunities were authentic, the perpetrators recruited U.S. citizens to pose as bank "representatives" at in-person meetings with the victims. If the victims lived outside the U.S., the perpetrators orchestrated bogus visits to the local U.S. embassy or consulate and fabricated U.S. government documents to convince the victims the U.S. government was sponsoring the investment agreements. The victims were then induced to pay tens of thousands, and often hundreds of thousands, of dollars to U.S.-based bank accounts on the belief that such payments were necessary to effectuate their investment agreements.

Once the funds hit the U.S.-based accounts, money movers controlling the accounts used various means to liquidate the proceeds and move the funds to West Africa, including outgoing wire transfers to exporters, cash withdrawals, and the purchase of luxury vehicles which were shipped to West Africa.

The scheme allegedly resulted in losses of more than $7 million from victims in more than 20 countries. To date, a house in Richmond, vehicles and approximately $200,000 in cash, all directly traceable to victims' payments, have been seized[5].

Harassment/Extortion: FBI Los Angeles

Since October 2017, FBI Los Angeles has been investigating a reported intrusion of a company's network that also involved harassment and extortion by an unknown subject. This individual continuously harassed the company with emails and phone calls that greatly impacted the victim company's business. The harassment continued until the company agreed to make payments for the attacks to stop.

The case was initiated by an IC3 complaint sent to FBI Los Angeles. During the course of the investigation, IC3 linked another complaint to the victim company and provided that information to FBI Los Angeles as well. The information contained within the linked IC3 complaint was instrumental in providing probable cause for a search warrant and then used in the interview of a subject, which ultimately led to a full confession.

[5] International Investment Scam Details

Operation Wellspring (OWS) Initiative

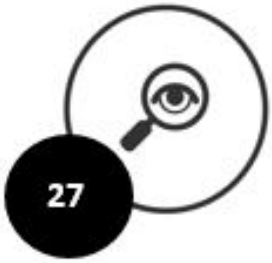
Operation Wellspring builds the cyber investigative capability and capacity of the state and local law enforcement community. Through close collaboration with FBI field offices, IC3 helps state and local law enforcement partners identify and respond to malicious cyber activity.

Key Components

- Serves as a national platform to receive, develop, and refer Internet-facilitated fraud complaints.
- Coordinates with FBI Cyber and Criminal components.
- Trains state and local law enforcement officers on cyber crime investigations.
- Addresses Internet-facilitated criminal cases not meeting most federal investigative thresholds by utilizing Cyber Task Force (CTF) state and local officers.

CTFs

The OWS Initiative was launched in August 2013 with the Salt Lake City CTF, in partnership with the Utah Department of Public Safety. Since then, OWS has expanded to 13 field offices: Albany, Buffalo, Kansas City, Knoxville, Las Vegas, New York City, New Orleans, Oklahoma City, Omaha–Des Moines, Phoenix, Richmond, Salt Lake City, and San Diego.



Total OWS Opened Investigations

The IC3 receives, on average, 800 complaints per day, and OWS offers CTFs a consistent resource to identify Internet fraud subjects and victims located throughout the world. As a result of OWS, 27 investigations were opened in 2017. Accomplishments included arrests, disruptions, convictions, indictments, and asset forfeitures. In addition, financial restitutions were obtained and criminals were sentenced.

Victim Complaints

The IC3 provided 289 referrals to 13 CTFs based on 1,867 victim complaints. The total victim loss associated with these complaints was approximately $15.7 million.

OWS Statistics[6]

[6]Accessibility description: images containing the number of Field Offices (13) involved with the OWS initiative, the number of opened investigations (27), and the number of victims (1,867).

OWS Success Stories

SAN DIEGO

Multiple victims reported on www.IC3.gov that they had been defrauded by the same subject over the internet. The victims shipped high end clothing and jewelry to the subject without receiving the agreed compensation. The subject broke off all communication after receiving the products. The Deputy District Attorney from the San Diego County District Attorney's Computer and Technology Crime High-Tech Response Team (CATCH) agreed to handle the case at the state level. The investigation included the execution of a physical search warrant and arrest at the suspect's home by members of the FBI San Diego CTF and members of the San Diego District Attorney's CATCH team. As a result of the search and arrest, investigators recovered stolen property and obtained a recorded interview in which the suspect admitted to the theft. The San Diego Regional Computer Forensics Laboratory (RCFL) was also used to analyze devices seized during the search warrant providing additional evidence for the case. The cooperative effort between IC3, the San Diego District Attorney's CATCH team, the San Diego RCFL and FBI San Diego CTF resulted in a theft conviction and the return of stolen property.

SAN DIEGO

This case involved the employee theft of approximately $25,000 worth of merchandise from a San Diego-based electronics internet retailer and the coordinated sale of the stolen items on a co-conspirator's auction website. A component of this case included an internet return fraud scheme in which the subjects purchased items from an online seller and later returned less valuable products for a refund. Working with the OWS Task Force, the Deputy District Attorney from the San Diego County District Attorney's CATCH agreed to handle the case at the state level. Analysis of search warrant returns showed the sale of the stolen items and the division of the proceeds between the two subjects. Both subjects admitted to the crimes during recorded interviews and were later arrested. Both subjects pled guilty to felony charges and were required to pay restitution to the victim.

KNOXVILLE

In the spring of 2016, Brandon Douglas Shanahan began impersonating a former, well-known University of Tennessee football player to extort and threaten multiple female victims. Utilizing a username posing as the player, Shanahan would threaten bodily harm and demand inappropriate photographs. Multiple victims were identified with similar reports of harassment during the investigation and through IC3 complaints. In June 2016, Shanahan was arrested and activities disrupted. Shanahan knowingly transmitted in interstate and foreign commerce with intent to extort money and other things of value. In December 2016, Shanahan entered a guilty plea on the count of interstate communications with the intent to extort. Shanahan broke his bond agreement, was re-arrested, and pled guilty to an additional count. Shanahan was sentenced to 30 months in a Federal Bureau of Prisons (BOP) Facility, followed by a one-year probation.

KNOXVILLE

Multiple victims reported to the IC3 that they had not received vehicles purchased and paid for via the internet. The IC3 aggregated the complaints, conducted independent research, and provided the information to the FBI Knoxville CTF. The resulting investigation determined Irvin Cachu-Melo and Luis Javier Martinez-Melo were operating as "money mules" in an on-going wire fraud scam involving the fraudulent sales of automobiles. Cachu-Melo and Martinez-Melo used stolen identities acquired by Martinez-Melo, to conduct wire transfers of the funds.

In 2017, The investigation determined Cachu-Melo was arrested and pled guilty to Conspiracy to Commit Money Laundering. Cachu-Melo was sentenced to 25 months in a BOP Facility along with three years of supervised release. Martinez-Melo was also arrested and pled guilty to Conspiracy to Commit Bank Fraud, Aggravated Identity Theft, and Conspiracy to Commit Wire Fraud. Martinez-Melo was sentenced to serve 57 months in a BOP Facility and is subject to 5 years of supervised release.

Hot Topics for 2017

Business Email Compromise

BEC is a sophisticated scam targeting businesses that often work with foreign suppliers and/or businesses and regularly perform wire transfer payments. The Email Account Compromise (EAC) variation of BEC targets individuals who regularly perform wire transfer payments. It should be noted while most BEC and EAC victims reported using wire transfers as their regular method of transferring business funds, some victims reported using checks. The fraudsters used the method most commonly associated with their victims' normal business practices. Both scams typically involve one or more fraudsters, who compromise legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. Because the techniques used in the BEC and EAC scams have become increasingly similar, the IC3 began tracking these scams as a single crime type in 2017.

Fraudulent transfers conducted as a result of BEC and EAC have been routed through accounts in many countries with a large majority traveling through Asia.

BEC and EAC are constantly evolving as scammers become more sophisticated. In 2013, victims indicated the email accounts of Chief Executive Officers or Chief Financial Officers were hacked or spoofed, and fraudulent emails were sent requesting wire payments be sent to fraudulent locations. In 2014, victims reported personal email accounts were being compromised, and fraudulent requests for payment were sent to vendors identified out of their personal contact lists. In 2015, victims reported being contacted by subjects posing as lawyers or law firms instructing them to make secret or time sensitive wire transfers.

BECs may not always be associated with a request for transfer of funds. In 2016, the scam evolved to include the compromise of legitimate business email accounts and fraudulent requests for Personally Identifiable Information or Wage and Tax Statements commonly known as W-2 forms for employees. In 2017, the real estate sector was heavily targeted with many victims reporting losses during real estate transactions.

The BEC/EAC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and rental scams. The victims of these scams are usually U.S.-based and may be recruited to illegally transfer money on behalf of others.

In 2017, the IC3 received 15,690 BEC/EAC complaints with adjusted losses of over $675 million.

Ransomware

Ransomware is a form of malware targeting both human and technical weaknesses in an effort to make critical data and/or systems inaccessible. Ransomware is delivered through various vectors, including Remote Desktop Protocol, which allows computers to connect to each other across a network, and phishing.

In one scenario, spear phishing emails are sent to end users resulting in the rapid encryption of sensitive files on a corporate network. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, typically in virtual currency such as Bitcoin. The actor will purportedly provide an avenue to the victim to regain access to their data once the ransom is paid.

Recent iterations target specific organizations and their employees, making awareness and training a critical preventative measure.

The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom. Paying a ransom emboldens the adversary to target other organizations for profit, and provides for a lucrative environment for other criminals to become involved. While the FBI does not support paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

In all cases the FBI encourages organizations to contact a local FBI field office immediately to report a ransomware event and request assistance.

In 2017, the IC3 received 1,783 complaints identified as ransomware with adjusted losses of over $2.3 million.

Tech Support Fraud

Tech Support Fraud is a widespread scam in which criminals claim to provide customer, security, or technical support in an effort to defraud unwitting individuals and gain access to the individuals' devices. There are many variations of this scam, and criminals are constantly changing their tactics to continue the fraud. For example, in addition to telephone calls, pop-up and locked screens, search engine advertising, and URL hijacking/typosquatting, criminals now use phishing emails with malicious links or fraudulent account charges to lure their victims. Criminals also pose as a variety of different security, customer, or technical support representatives and offer to resolve any number of issues, including compromised email, bank accounts, computer viruses, or offer to assist with software license renewal. Some recent complaints involve criminals posing as technical support representatives for income tax assistance, GPS, printer, or cable companies, or support for virtual currency exchanges. In some variations, criminals pose as government agents, who offer to recover losses related to tech support fraud schemes or request financial assistance with "apprehending" criminals.

The "fake refund" variation of tech support fraud is increasing in reports and losses. In this scheme, the criminal contacts the victim offering a refund for tech support services previously rendered. The criminal pretends to refund too much money to the victim's account and requests the victim return the difference. The "refund and return" process can occur multiple times, resulting in the victim potentially losing thousands of dollars.

During this scheme, if the criminal can connect to the victim's devices, the criminal will download the victim's personal files containing financial accounts, passwords, and personal data, like health records, social security numbers, and tax information. The information is used to request bank transfers or open new accounts to accept and process unauthorized payments. Criminals will also send phishing emails to the victim's personal contacts from the victim's computer.

Additional information, explanations, and suggestions for protection regarding tech support fraud is available in a recently published Tech Support Fraud Public Service Announcement[7] on the IC3 website.

In 2017, the IC3 received 10,949 complaints related to tech support fraud. The claimed losses amounted to nearly $15 million, which represented a 90% increase in losses from 2016. While a majority of tech support fraud involves victims in the U.S., IC3 has received complaints from victims in 85 different countries.

[7] Federal Bureau of Investigation. Internet Crime Complaint Center. Tech Support Fraud Public Service Announcement

Elder Justice Initiative

On February 22, 2018, in response to a coordinated sweep of elder fraud cases, Attorney General Jeff Sessions stated "The Justice Department and its partners are taking unprecedented, coordinated action to protect elderly Americans from financial threats, both foreign and domestic … When criminals steal the hard-earned life savings of older Americans, we will respond with all the tools at the Department's disposal – criminal prosecutions to punish offenders, civil injunctions to shut the schemes down, and asset forfeiture to take back ill-gotten gains … I have directed Department prosecutors to coordinate with both domestic law enforcement partners and foreign counterparts to stop these criminals from exploiting our seniors."[8] The mission of the Elder Justice Initiative is to support and coordinate the Department's enforcement and programmatic efforts to combat elder abuse, neglect and financial fraud and scams that target our nation's seniors. We engage in this work by focusing on the following mission areas:

Building local, state, and federal capacity to fight elder abuse: Providing targeted training and resources to elder justice professionals including: prosecutors, law enforcement, judges, victim specialists, first responders, civil legal aid employees and multi-disciplinary teams to enhance their ability to respond to elder abuse efficiently and effectively.

Promoting justice for older Americans: Investigating and prosecuting financial scams targeting older adults. Promoting greater local, state, and federal coordination to resolve cases where long-term care entities provide grossly substandard care to their residents or patients.

Supporting research to improve elder abuse policy and practice: Promoting foundational research into elder abuse and financial exploitation in order to transform the practice of professionals in ways that positively impact the lives of older adults.

Helping older victims and their families: Connecting older adults and their families or caregivers with appropriate investigative agencies, as well as empowering them with information about abuse and recovering from its effects.

Further information is available at the DOJ Elder Justice Initiative website.[9] The US Senate Special Committee on Aging provides additional information in their publication, "Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors".[10]

In 2017, the IC3 received 49,523 complaints from victims over the age of 60 with adjusted losses in excess of $342 million.

[8]U.S. Department of Justice. Protecting Elderly Americans From Financial Threats
[9]Elder Justice Initiative. DOJ Elder Justice Initiative Website
[10] U.S. Senate Special Committee on Aging. Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors

Extortion

Extortion occurs when a criminal demands something of value from a victim by threatening physical or financial harm or the release of sensitive data. Extortion is used in various schemes reported to the IC3, including Denial of Service attacks, hitman schemes,[11] sextortion,[12] government impersonation schemes, loan schemes,[13] and high-profile data breaches.[14] Virtual currency is commonly demanded as the payment mechanism because it provides the criminal an additional layer of anonymity when perpetrating these schemes.

In 2017, the IC3 received 14,938 extortion-related complaints with adjusted losses of over $15 million.

[11] A *hitman scheme* involves an email extortion in which a perpetrator sends a disturbing email threatening to kill a victim and/or their family. The email instructs the recipient to pay a fee to remain safe and avoid having the hit carried out.

[12] *Sextortion* occurs when a perpetrator threatens to distribute an individual's private and sensitive material unless the individual provides the perpetrator images of a sexual nature, sexual favors, or money.

[13] A *loan scheme* involves perpetrators contacting victims claiming to be debt collectors from a legitimate company and instructing victims to pay fees in order to avoid legal consequences.

[14] A *high profile data breach* is when sensitive, protected or confidential data belonging to a well-known or established organization is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

2017 Overall Statistics [15]

Important Stats

 # Of Complaints Reported Since Inception ('00)
4,063,933

Approximately 284,000
Average Complaints Received Each Year

$1.42 Billion
Victim Losses in 2017

Over 800
Average Complaints Received Per Day

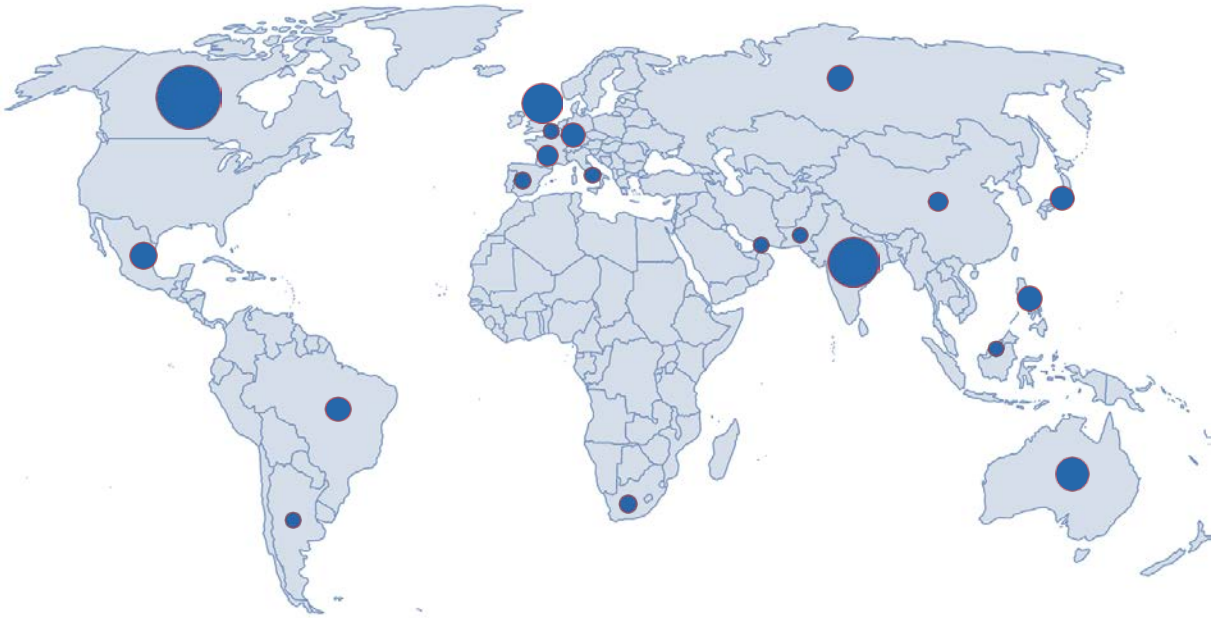
2017 Victims by Age Group

Victims		
Age Range[16]	Total Count	Total Loss
Under 20	9,053	$8,271,311
20 - 29	41,132	$67,981,630
30 - 39	45,458	$156,287,698
40 - 49	44,878	$244,561,364
50 - 59	43,764	$275,621,946
Over 60	49,523	$342,531,972

[15] Accessibility description: image depicts several key statistics regarding complaints and victim loss. A bar chart shows total number of complaints for the years 2013 to 2017. The total number of complaints received since the year 2000 is 4,063,933. IC3 receives approximately 284,000 complaints each year, or more than 800 per day.
[16] Not all complaints include an associated age range—those without this information are excluded from this table.

Top 20 Foreign Countries by Victim

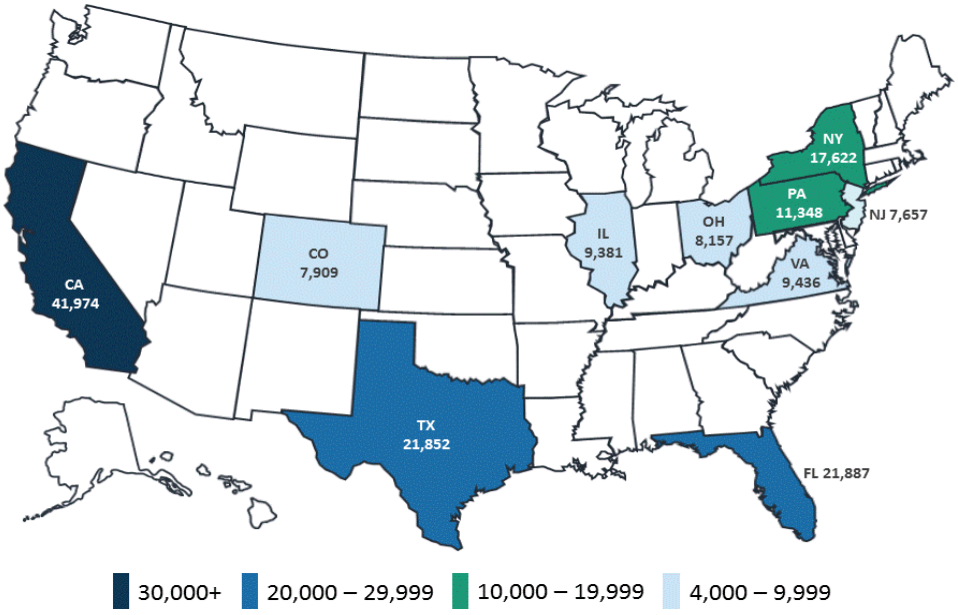
Excluding the United States[17]



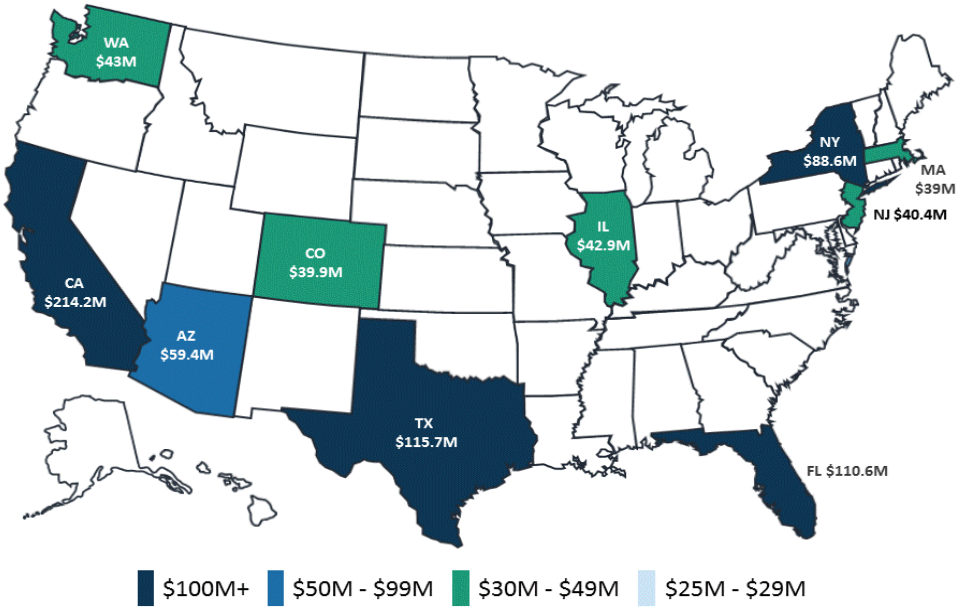
1. Canada	3,164	6. Russian Federation	594	11. France	368	16. Netherlands	266
2. India	2,819	7. Brazil	558	12. China	366	17. Malaysia	265
3. United Kingdom	1,383	8. Germany	466	13. South Africa	349	18. United Arab Emirates	259
4. Australia	989	9. Philippines	453	14. Italy	291	19. Spain	248
5. Mexico	632	10. Japan	413	15. Pakistan	276	20. Argentina	238

[17] Accessibility description: image includes a world map with circles corresponding in size to the total number of reports received from specific countries. The top twenty countries are indicated. Specific statistics for each country ranked in descending order of victim figures can be found in the text table immediately below the image.

Top 10 States by Number of Victims [18]



Top 10 States by Victim Loss [19]



[18] Accessibility description: image depicts the United States, with the top ten states (based on reported victims) highlighted. These include California (41,974), Florida (21,887), Texas (21,852), New York (17,622), Pennsylvania (11,348), Virginia (9,436), Illinois (9,381), Ohio (8,157), Colorado (7,909), and New Jersey (7,657).

[19] Accessibility description: image depicts the United States, with the top ten states (based on reported victim loss). These include California ($214.2M), Texas (115.7M) Florida ($110.6M), New York ($88.6M), Arizona ($59.4M), Washington ($43M), Illinois ($42.9M), New Jersey ($40.4M), Colorado ($39.9M), and Massachusetts ($39M).

2017 Crime Types

By Victim Count			
Crime Type	**Victims**	**Crime Type**	**Victims**
Non-Payment/Non-Delivery	84,079	Misrepresentation	5,437
Personal Data Breach	30,904	Corporate Data Breach	3,785
Phishing/Vishing/Smishing/Pharming	25,344	Investment	3,089
Overpayment	23,135	Malware/Scareware/Virus	3,089
No Lead Value	20,241	Lottery/Sweepstakes	3,012
Identity Theft	17,636	IPR/Copyright and Counterfeit	2,644
Advanced Fee	16,368	Ransomware	1,783
Harassment/Threats of Violence	16,194	Crimes Against Children	1,300
Employment	15,784	Denial of Service/TDoS	1,201
BEC/EAC	15,690	Civil Matter	1,057
Confidence Fraud/Romance	15,372	Re-shipping	1,025
Credit Card Fraud	15,220	Charity	436
Extortion	14,938	Health Care Related	406
Other	14,023	Gambling	203
Tech Support	10,949	Terrorism	177
Real Estate/Rental	9,645	Hacktivist	158
Government Impersonation	9,149		

Descriptors*		
Social Media	19,986	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	4,139	

2017 Crime Types *Continued*

By Victim Loss			
Crime Type	**Loss**	**Crime Type**	**Loss**
BEC/EAC	$676,151,185	Misrepresentation	$14,580,907
Confidence Fraud/Romance	$211,382,989	Harassment/Threats of Violence	$12,569,185
Non-Payment/Non-Delivery	$141,110,441	Government Impersonation	$12,467,380
Investment	$96,844,144	Civil Matter	$5,766,550
Personal Data Breach	$77,134,865	IPR/Copyright and Counterfeit	$5,536,912
Identity Theft	$66,815,298	Malware/Scareware/ Virus	$5,003,434
Corporate Data Breach	$60,942,306	Ransomware	$2,344,365
Advanced Fee	$57,861,324	Denial of Service/TDoS	$1,466,195
Credit Card Fraud	$57,207,248	Charity	$1,405,460
Real Estate/Rental	$56,231,333	Health Care Related	$925,849
Overpayment	$53,450,830	Re-Shipping	$809,746
Employment	$38,883,616	Gambling	$598,853
Phishing/Vishing/Smishing/ Pharming	$29,703,421	Crimes Against Children	$46,411
Other	$23,853,704	Hacktivist	$20,147
Lottery/Sweepstakes	$16,835,001	Terrorism	$18,926
Extortion	$15,302,792	No Lead Value	$0
Tech Support	$14,810,080		

		Descriptors*
Social Media	$56,478,483	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	$58,391,810	

2017 Overall State Statistics

Count by Victim per State*					
Rank	State	Victims	Rank	State	Victims
1	California	41,974	30	Connecticut	2,662
2	Florida	21,887	31	Utah	2,260
3	Texas	21,852	32	Hawaii	1,923
4	New York	17,622	33	Mississippi	1,799
5	Pennsylvania	11,348	34	Kansas	1,767
6	Virginia	9,436	35	Arkansas	1,753
7	Illinois	9,381	36	Iowa	1,533
8	Ohio	8,157	37	Alaska	1,418
9	Colorado	7,909	38	New Mexico	1,415
10	New Jersey	7,657	39	Idaho	1,186
11	Washington	7,505	40	District of Columbia	1,143
12	North Carolina	7,316	41	Nebraska	1,140
13	Georgia	7,007	42	New Hampshire	1,106
14	Maryland	6,789	43	West Virginia	1,085
15	Arizona	6,417	44	Delaware	759
16	Michigan	6,400	45	Maine	740
17	Wisconsin	5,245	46	Montana	737
18	Massachusetts	5,221	47	Rhode Island	704
19	Tennessee	4,779	48	Puerto Rico	605
20	Nevada	4,675	49	Vermont	451
21	Missouri	4,187	50	Wyoming	434
22	Indiana	4,067	51	South Dakota	404
23	Alabama	3,865	52	North Dakota	355
24	South Carolina	3,687	53	Guam	66
25	Minnesota	3,619	54	U.S. Minor Outlying Islands	51
26	Oregon	3,455	55	U.S. Virgin Islands	48
27	Louisiana	3,319	56	American Samoa	17
28	Oklahoma	2,809	57	Northern Marina Islands	13
29	Kentucky	2,740			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information.

2017 Overall State Statistics *Continued*

Loss by Victim per State*					
Rank	**State**	**Loss**	**Rank**	**State**	**Loss**
1	California	$214,217,307	**30**	Alabama	$9,949,873
2	Texas	$115,680,902	**31**	Idaho	$7,657,726
3	Florida	$110,620,330	**32**	Kentucky	$7,220,342
4	New York	$88,633,788	**33**	Mississippi	$6,786,910
5	Arizona	$59,366,635	**34**	Kansas	$5,045,755
6	Washington	$42,991,213	**35**	Arkansas	$4,823,489
7	Illinois	$42,894,106	**36**	New Mexico	$4,716,033
8	New Jersey	$40,441,739	**37**	Nebraska	$4,286,773
9	Colorado	$39,935,041	**38**	Iowa	$4,013,395
10	Massachusetts	$38,962,867	**39**	New Hampshire	$3,725,739
11	Georgia	$38,353,746	**40**	Rhode Island	$3,390,078
12	Pennsylvania	$36,319,408	**41**	Hawaii	$3,368,323
13	Virginia	$35,438,537	**42**	District of Columbia	$2,707,684
14	Ohio	$30,672,149	**43**	Montana	$2,553,804
15	Maryland	$30,045,488	**44**	South Dakota	$2,472,062
16	Michigan	$25,362,646	**45**	West Virginia	$2,435,608
17	North Carolina	$22,203,108	**46**	Delaware	$2,376,718
18	Nevada	$19,578,132	**47**	Wyoming	$2,331,692
19	Missouri	$19,475,647	**48**	North Dakota	$2,006,821
20	Minnesota	$19,126,165	**49**	Alaska	$1,709,126
21	Wisconsin	$15,787,242	**50**	Puerto Rico	$1,590,979
22	Tennessee	$13,561,295	**51**	Maine	$1,310,506
23	Indiana	$13,228,744	**52**	Vermont	$1,291,941
24	South Carolina	$13,048,133	**53**	Guam	$819,163
25	Connecticut	$12,465,243	**54**	U.S. Virgin Islands	$625,169
26	Oklahoma	$11,671,198	**55**	U.S. Minor Outlying Islands	$61,445
27	Oregon	$11,165,342	**56**	Northern Mariana Islands	$21,320
28	Louisiana	$10,696,284	**57**	American Samoa	$2,200
29	Utah	$10,302,892			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information.

2017 Overall State Statistics *Continued*

Count by Subject per State*					
Rank	State	Subjects	Rank	State	Subjects
1	California	14,786	30	District of Columbia	873
2	Texas	8,785	31	Delaware	821
3	Florida	8,709	32	Utah	785
4	New York	7,162	33	Wisconsin	716
5	Virginia	3,795	34	Kentucky	701
6	Illinois	3,627	35	Connecticut	677
7	Georgia	3,228	36	Mississippi	677
8	Maryland	3,161	37	Montana	673
9	New Jersey	2,876	38	Iowa	621
10	Washington	2,514	39	Arkansas	510
11	Ohio	2,384	40	West Virginia	372
12	Pennsylvania	2,361	41	North Dakota	318
13	Nebraska	2,153	42	New Mexico	304
14	Nevada	2,082	43	Idaho	280
15	Arizona	1,874	44	Maine	264
16	Michigan	1,868	45	Alaska	252
17	North Carolina	1,817	46	Hawaii	234
18	Louisiana	1,717	47	Rhode Island	212
19	Tennessee	1,473	48	New Hampshire	186
20	Colorado	1,400	49	Wyoming	154
21	Massachusetts	1,392	50	South Dakota	139
22	Missouri	1,355	51	Puerto Rico	115
23	South Carolina	1,193	52	Vermont	77
24	Oregon	1,192	53	U.S. Minor Outlying Islands	18
25	Indiana	1,148	54	U.S. Virgin Islands	15
26	Oklahoma	1,101	55	Guam	9
27	Minnesota	1,030	56	American Samoa	5
28	Alabama	1,022	57	Northern Mariana Islands	5
29	Kansas	953			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information.

2017 Overall State Statistics *Continued*

Subject Earnings per Destination State*					
Rank	State	Loss	Rank	State	Loss
1	California	$83,676,865	30	Kansas	$3,185,500
2	Texas	$70,647,821	31	District of Columbia	$2,931,263
3	Florida	$47,274,025	32	Utah	$2,634,496
4	New York	$39,107,593	33	Arkansas	$2,631,804
5	Georgia	$22,691,044	34	Iowa	$2,367,889
6	Illinois	$17,081,877	35	Wisconsin	$2,254,829
7	Ohio	$16,646,002	36	Mississippi	$2,253,167
8	New Jersey	$11,424,449	37	New Hampshire	$1,989,281
9	Maryland	$11,309,325	38	Kentucky	$1,957,108
10	Nevada	$11,077,774	39	Montana	$1,924,196
11	Washington	$9,654,732	40	Delaware	$1,616,234
12	Pennsylvania	$9,516,714	41	New Mexico	$1,464,315
13	Virginia	$9,457,095	42	Maine	$1,298,749
14	Michigan	$8,437,965	43	Idaho	$1,237,269
15	North Carolina	$8,357,577	44	Rhode Island	$1,119,321
16	Colorado	$8,052,578	45	Hawaii	$947,310
17	Arizona	$6,792,467	46	North Dakota	$865,639
18	Oklahoma	$6,636,529	47	West Virginia	$770,919
19	Massachusetts	$6,588,675	48	South Dakota	$756,336
20	Oregon	$5,866,936	49	Wyoming	$711,958
21	Nebraska	$5,150,696	50	Vermont	$536,348
22	Connecticut	$4,674,297	51	Alaska	$446,294
23	Louisiana	$4,585,139	52	Puerto Rico	$340,309
24	Indiana	$4,539,775	53	North Mariana Islands	$181,180
25	Minnesota	$4,314,856	54	U.S. Minor Outlying Islands	$131,727
26	South Carolina	$3,985,279	55	American Samoa	$8,370
27	Tennessee	$3,764,353	56	U.S. Virgin Islands	$5,854
28	Missouri	$3,522,518	57	Guam	$4,977
29	Alabama	$3,429,023			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information.

Appendix A: Crime Type Definitions

419/Overpayment: "419" refers to the section in Nigerian law regarding con artistry and fraud and is associated with requests for help facilitating the transfer of money. The sender of the "419" letter or email offers the recipient a commission or share in the profits of a transfer of money, but will first request the recipient send money to pay for some of the costs associated with the transfer. The recipient may be sent a payment and instructed to keep a portion of the payment, but send the rest on to another individual or business.

Advanced Fee: In advance fee schemes, the perpetrator informs a victim that the victim has qualified for a large financial loan or has won a large financial award, but must first pay the perpetrator taxes or fees in order to access the loan or award. The victim pays the advance fee, but never receives the promised money.

Auction: A fraudulent transaction or exchange that occurs in the context of an online auction site.

Business Email Compromise/Email Account Compromise: BEC is a scam targeting businesses working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam that targets individuals. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Charity: Perpetrators set up false charities, usually following natural disasters, and profit from individuals who believe they are making donations to legitimate charitable organizations.

Civil Matter: Civil lawsuits are any disputes formally submitted to a court that is not criminal.

Confidence/Romance Fraud: A perpetrator deceives a victim into believing the perpetrator and the victim have a trust relationship, whether family, friendly or romantic. As a result of that belief, the victim is persuaded to send money, personal and financial information, or items of value to the perpetrator or to launder money on behalf of the perpetrator. Some variations of this scheme are romance/dating scams or the grandparent's scam.

Corporate Data Breach: A leak or spill of business data that is released from a secure location to an untrusted environment. It may also refer to a data breach within a corporation or business where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

Credit Card: Credit card fraud is a wide-ranging term for fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction.

Crimes Against Children: Anything related to the exploitation of children, including child abuse.

Criminal Forums: A medium where criminals exchange ideas and protocols relating to intrusion.

Denial of Service: An interruption of an authorized user's access to any system or network, typically caused with malicious intent.

Employment: An individual believes they are legitimately employed, and loses money or launders money/items during the course of their employment.

Extortion: Unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.

Gambling: Online gambling, also known as Internet gambling and iGambling, is a general term for gambling using the Internet.

Government Impersonation: A government official is impersonated in an attempt to collect money.

Hacktivist: A computer hacker whose activity is aimed at promoting a social or political cause.

Harassment/Threats of Violence: Harassment occurs when a perpetrator uses false accusations or statements of fact to intimidate a victim. Threats of Violence refers to an expression of an intention to inflict pain, injury, or punishment, which does not refer to the requirement of payment.

Health Care Related: A scheme attempting to defraud private or government health care programs, usually involving health care providers, companies, or individuals. Schemes may include offers for fake insurance cards, health insurance marketplace assistance, stolen health information, or may involve medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums or social media, and fraudulent websites.

IPR/Copyright and Counterfeit: The theft and illegal use of others' ideas, inventions, and creative expressions, to include everything from trade secrets and proprietary products to parts to movies, music, and software.

Identity Theft/Account Takeover: Identify theft involves a perpetrator stealing another person's personal identifying information, such as name or Social Security number, without permission to commit fraud. Account Takeover is when a perpetrator obtains account information to perpetrate fraud on existing accounts.

Investment: Deceptive practice that induces investors to make purchases on the basis of false information. These scams usually offer the victims large returns with minimal risk. Variations of this scam include retirement schemes, Ponzi schemes and pyramid schemes.

Lottery/Sweepstakes: An individual is contacted about winning a lottery or sweepstakes they never entered and are asked to pay a tax or fee in order to receive their winnings.

Malware/Scareware: Software intended to damage or disable computers and computer systems. Sometimes scare tactics are used by the perpetrators to solicit funds.

Misrepresentation: Merchandise or services were purchased or contracted by individuals online for which the purchasers provided payment. The goods or services received were of a measurably lesser quality or quantity than was described by the seller.

No Lead Value: Incomplete complaints which do not allow a crime type to be determined.

Non-Payment/Non-Delivery: In non-payment situations, goods and services are shipped, but payment is never rendered. In non-delivery situations, payment is sent, but goods and services are never received.

Other: Other types of fraud not listed.

Personal Data Breach: A leak or spill of personal data that is released from a secure location to an untrusted environment. It may also refer to a security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual.

Phishing/Vishing/Smishing/Pharming: Unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

Ransomware: A type of malicious software designed to block access to a computer system until money is paid.

Re-shipping: Individuals receive packages purchased through fraudulent means and subsequently repackage the merchandise for shipment, usually abroad.

Real Estate/Rental: Fraud involving real estate, rental or timeshare property.

Social Media: A complaint alleging the use of social networking or social media (Facebook, Twitter, Instagram, chat rooms, etc.) as a vector for fraud. Social Media does not include dating sites.

Tech Support: Attempts to gain access to a victim's electronic device by falsely claiming to offer tech support, usually for a well-known company. Scammer asks for remote access to the victim's device to clean-up viruses or malware or to facilitate a refund for prior support services.

Terrorism: Violent acts intended to create fear that is perpetrated for a religious, political, or ideological goal and deliberately target or disregard the safety of non-combatants.

Virus: Code capable of copying itself and having a detrimental effect, such as corrupting the system or destroying data.

Virtual Currency: A complaint mentioning a form of virtual cryptocurrency, such as Bitcoin, Litecoin, or Potcoin.