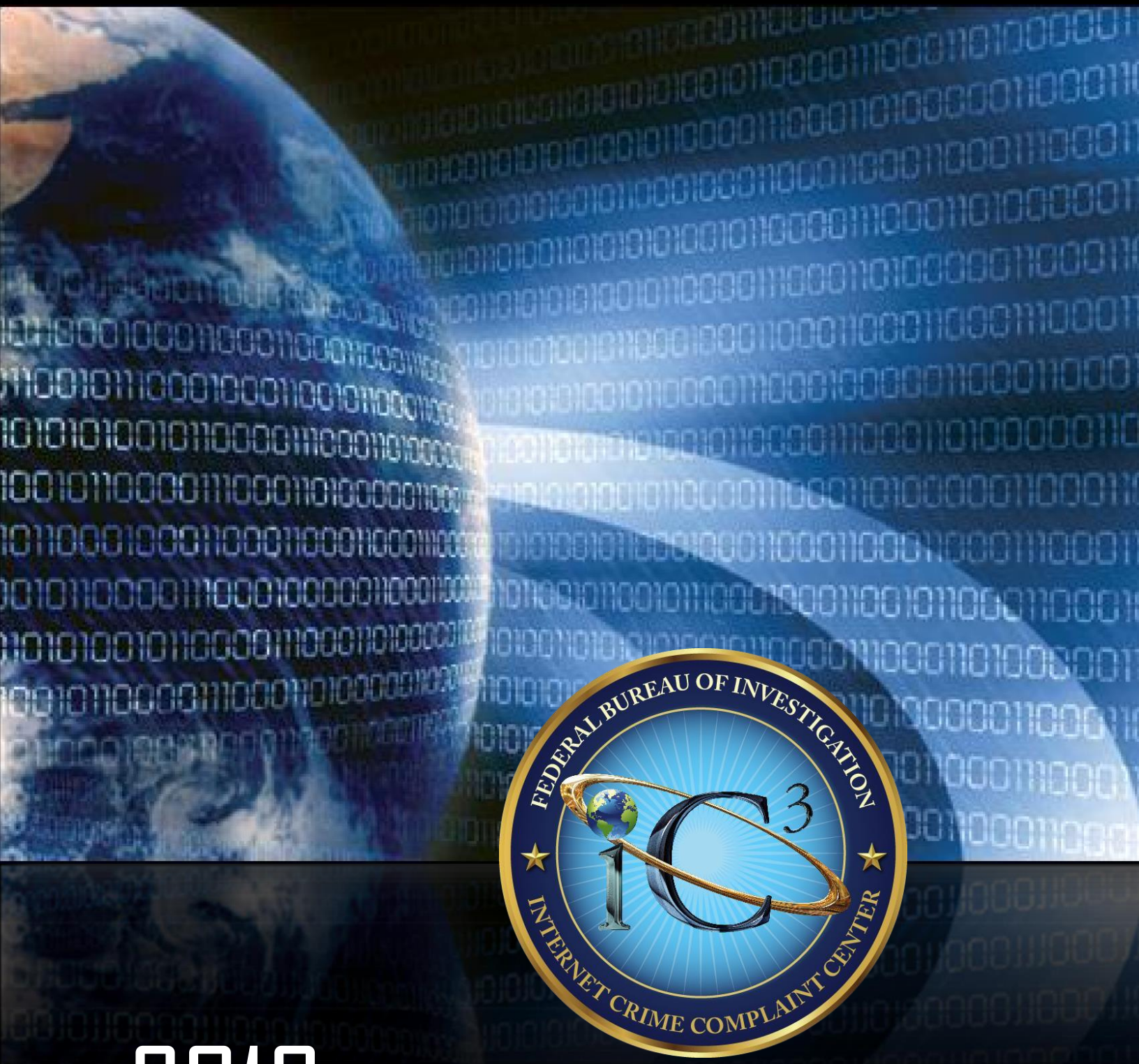


2016

Internet Crime Report

2016 Internet Crime Report

Table of Contents

Introduction 3
About the Internet Crime Complaint Center 2
IC3 History 2
The IC3 Role in Combating Cyber Crime 3
Collection 3
Analysis 4
Public Awareness 4
Referrals 4
Supporting Law Enforcement 5
IC3 Database Remote Access 5
Testimonials from Law Enforcement Database Users 5
Successes 7
Prosecutions 7
Operation Wellspring (OWS) Initiative 8
Hot Topics for 2016 9
Business Email Compromise (BEC) 9
Ransomware 10
Tech Support Fraud 11
Extortion 13
2016 Overall Statistics 14
2016 Victims by Age Group 14
Top 20 Foreign Countries by Victim 15
Top 10 States by Number of Reported Victims 16
Top 10 States by Reported Victim Loss 16
2016 Crime Types 17
2016 Overall State Statistics 19
Appendix A: Crime Type Definitions 23

Introduction

Dear Reader,

The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists. With each passing day, cyber intrusions are becoming more sophisticated, dangerous, and common. We continue to transform and develop in order to address the persistent and evolving cyber threats we face.

The FBI's Internet Crime Complaint Center (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 industry partners.

The 2016 Internet Crime Report highlights the IC3's efforts in monitoring trending scams such as Business Email Compromise (BEC), ransomware, tech support fraud, and extortion. In 2016, IC3 received a total of 298,728 complaints with reported losses in excess of $1.3 billion.

This past year, the top three crime types reported by victims were non-payment and non-delivery, personal data breach, and payment scams. The top three crime types by reported loss were BEC, romance and confidence fraud, and non-payment and non-delivery scams.

This year's report features a section on the importance of law enforcement collaboration and partnerships with the private sector and Intelligence Community. For example, the FBI continues to expand Operation Wellspring (OWS), an initiative through which state and local law enforcement officers are embedded in, and trained by, FBI cyber task forces and serve as the primary case agents on Internet-facilitated criminal investigations. Overall, OWS task forces opened 37 investigations in 2016 and have worked 73 total investigations since OWS was launched in August 2013.

We hope this report will assist you as we work in partnership to protect our nation and combat cyber threats.

Scott S. Smith
Assistant Director
Cyber Division
Federal Bureau of Investigation

About the Internet Crime Complaint Center

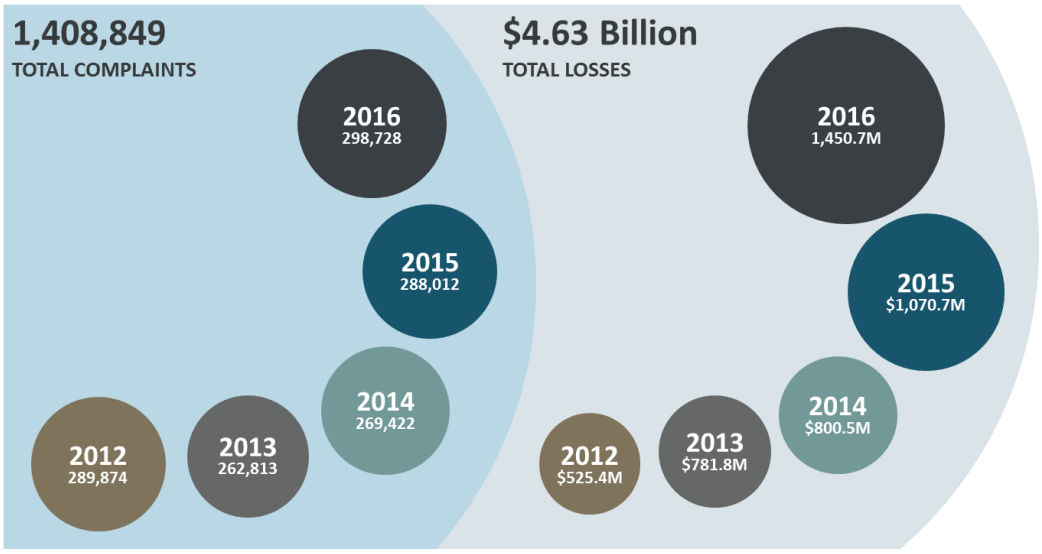
The mission of the FBI is to protect the American people and uphold the Constitution of the United States.

The mission of the Internet Crime Complaint Center (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 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, striving to identify trends relating to Internet-facilitated crimes and what those trends may represent in the coming year.

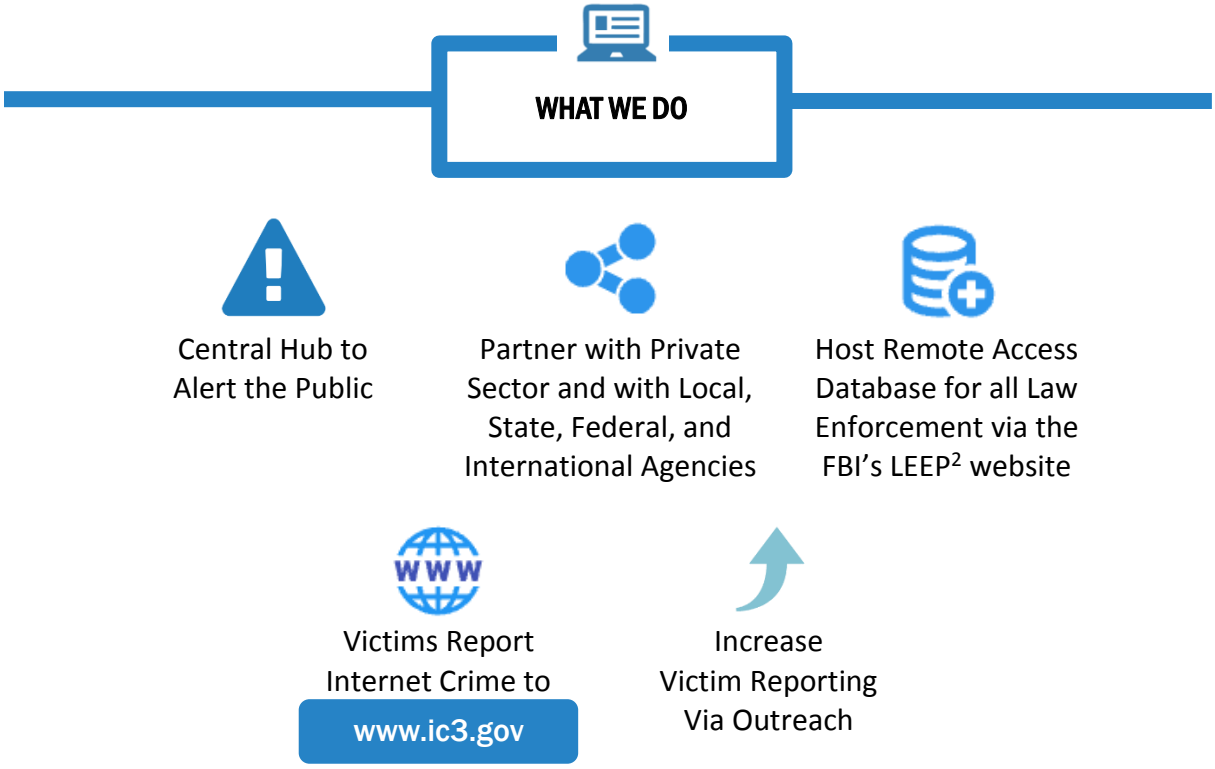
IC3 History

In May 2000, the IC3 was established as a center to receive complaints of Internet crime. There have been 3,762,348 complaints reported to the IC3 since its inception. Over the last five years, the IC3 received an average more than 280,000 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 2012 to 2016. Over that time period, IC3 received a total of 1,408,849 complaints, and a total reported loss of $4.63 billion.

The IC3 Role in Combating Cyber Crime



Collection

Millions of people in the United States are victims of Internet crimes each year. Detection is the cornerstone of determining the larger Internet crime picture. However, only an estimated 15 percent of the nation's fraud victims report their crimes to law enforcement.[3] This 15 percent figure is just a subset of the victims worldwide.

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

[2] Federal Bureau of Investigation. *Law Enforcement Enterprise Portal (LEEP)*. https://www.fbi.gov/services/cjis/leep

[3] The United States Attorney's Office, Western District of Washington. *Financial Crime Fraud Victims*. http://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud

related to the Internet crime, as well as any other relevant information necessary to support the complaint.

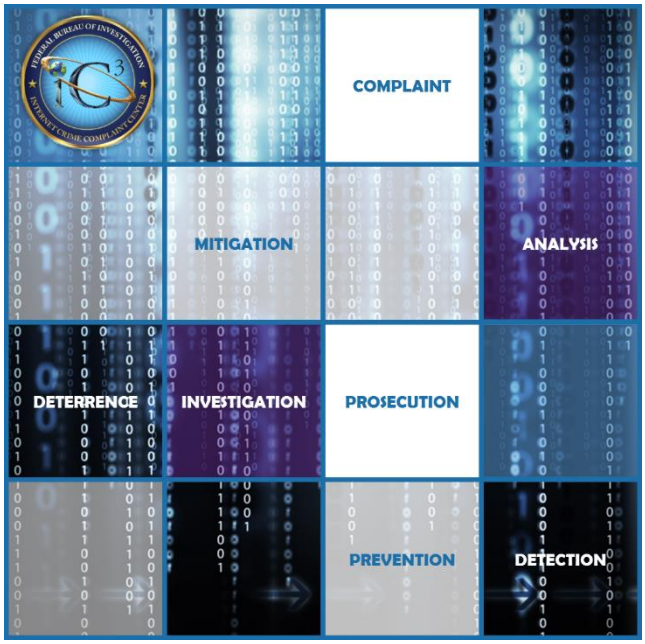
In addition to reporting the crime via www.ic3.gov, complainants should take steps to mitigate further loss. Victims can take actions such as contacting banks, credit card companies, and/or credit bureaus to block accounts, freeze accounts, dispute charges, or attempt recovery of lost funds. Victims should be diligent in reviewing credit reports to dispute any unauthorized transactions and should also consider credit monitoring services.

Analysis

The IC3 is well positioned to be the central point for Internet crime victims to report and to alert the appropriate agencies of 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

[4] Accessibility description: image contains the IC3 logo against a digital background. Core functions are listed in individual blocks: mitigation, complaint, analysis, deterrence, investigation, prosecution, prevention, and detection.

action may be brought against the perpetrator. Each and every step is necessary to assist law enforcement in stopping Internet crime.

Supporting Law Enforcement

IC3 Database Remote Access

A remote search capability of the IC3 database is available to all sworn law enforcement 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. These resources strengthen case development for investigators, enhance information sharing between agencies, and are accessible in one centralized location.

This web-based access provides users the ability to identify and aggregate victims and losses within a jurisdiction, and to substantiate investigations.

The IC3 expanded the remote search capabilities of the IC3 database by granting users the ability to gather IC3 complaint statistics. Users 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 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.

Testimonials from Law Enforcement Database Users

> *"I have published several reports based on trends that we were seeing since I was able to see the complaints. There were numerous instances of the quick reporting providing us with an opportunity to quickly mitigate circumstances or begin investigations before evidence was lost.*
>
> *Thanks for the great service …"*
>
> *FBI Portland*

> *"I had tremendous success using IC3. Without the availability and unlimited access to IC3 I would never have been able to identify the numerous suspects linked to a transnational criminal enterprise."*
>
> *Weld County, Colorado*

> *"The remote query is beneficial because it allows me to query potential leads and victim complaints outside of normal business hours.*

"Since February 2014, I have been investigating an ongoing romance scam investigation. Separate from following fraudulently obtained funds through subjects' bank accounts, IC3 data has enabled me to quickly determine if these funds are derived from a potential victim or possible co-conspirator. In a number of instances, victims making deposits into these accounts have filed complaints through IC3. The basic information provided by victims has given me general background information when conducting an interview. IC3 data has also corroborated information developed during the course of this investigation."

Department of Homeland Security, Wisconsin

"IC3 has served as a centralized intake for Business Email Compromises (BEC) across the United States. Boston Field Office reviews BEC complaints made to IC3 on a daily basis. IC3 has made this process easy through its modifications to the complaint form this year. The information is always up to the minute, which is important in these types of schemes. IC3 also proactively reaches out to the field when large BEC complaints involving recently wired funds are filed. In one instance, IC3 proactively reached out to the Boston Field Office to alert us to a $1.8 million wire. Based on the early notification, Boston was able to take the necessary steps to successfully recover the entire amount on behalf of the victim. Lastly, IC3 continues to be a steady source of intel on the BEC threat."

FBI Boston

Successes

Prosecutions

Real Estate/Rental Fraud: FBI San Diego

The IC3 provided multiple complaints with a monetary loss of $232,258.58 to FBI San Diego in March 2015. The complaints reported that Geoffrey Paul Moncrief was using properties listed on various vacation home rental websites to defraud victims of money, on an average of $8,000 per person. Subsequent investigation showed that Moncrief took full payment from multiple parties without delivering the real estate. Moncrief was ultimately charged in San Diego Superior Court with 28 Counts of violating California Penal Code section 487(a), Grand Theft. Moncrief entered a guilty plea to 26 counts of and was sentenced in San Diego Superior Court to 365 days corrective custody, three years of formal probation, and restitution in the amount of $232,258.58.

Wire Fraud: FBI San Diego

In February 2010, the IC3 provided multiple complaints to FBI San Diego reporting a monetary loss of $279,277. Complainants reported Christopher John Cozzie was selling pirated copies of infra-red imaging systems used in breast exams. Cozzie marketed these infra-red systems to include hardware, software, and training at a cost of approximately $35,000 per system but he either never delivered, or only partially delivered, on the orders.

Cozzie was indicted on ten counts of Wire Fraud, 18 U.S.C. 1343. He entered a guilty plea to one count of wire fraud and was sentenced to six months corrective custody, three years supervised release, and restitution in the amount of $279,277.

Operation Wellspring (OWS) Initiative

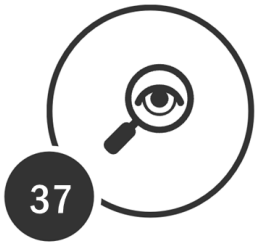
OWS builds the cyber investigative capability and capacity of the state and local law enforcement community. Through close collaboration with local field offices, IC3 helps state and local law enforcement partners identify and respond to malicious cyber activity.

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. OWS has expanded to 11 field offices: Albany, Buffalo, Kansas City, Knoxville, Las Vegas, New York City, New Orleans, Oklahoma City, Phoenix, 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. Thirty-seven investigations were opened in 2016. Accomplishments included arrests, disruptions, and convictions. Financial restitutions were made and criminals were sentenced.

Victim Complaints

The IC3 provided 174 referrals to 11 CTFs based on 2,719 complaints. The total victim loss associated with these complaints was approximately $14.4 million.

Hot Topics for 2016

Business Email Compromise (BEC)

Business Email Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses who regularly perform wire transfer payments. The Email Account Compromise (EAC) component of BEC targets individuals who perform wire transfer payments. The techniques used in both the BEC and EAC scams have become increasingly similar, prompting the IC3 to begin tracking these scams as a single crime type in 2017. The scam is carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

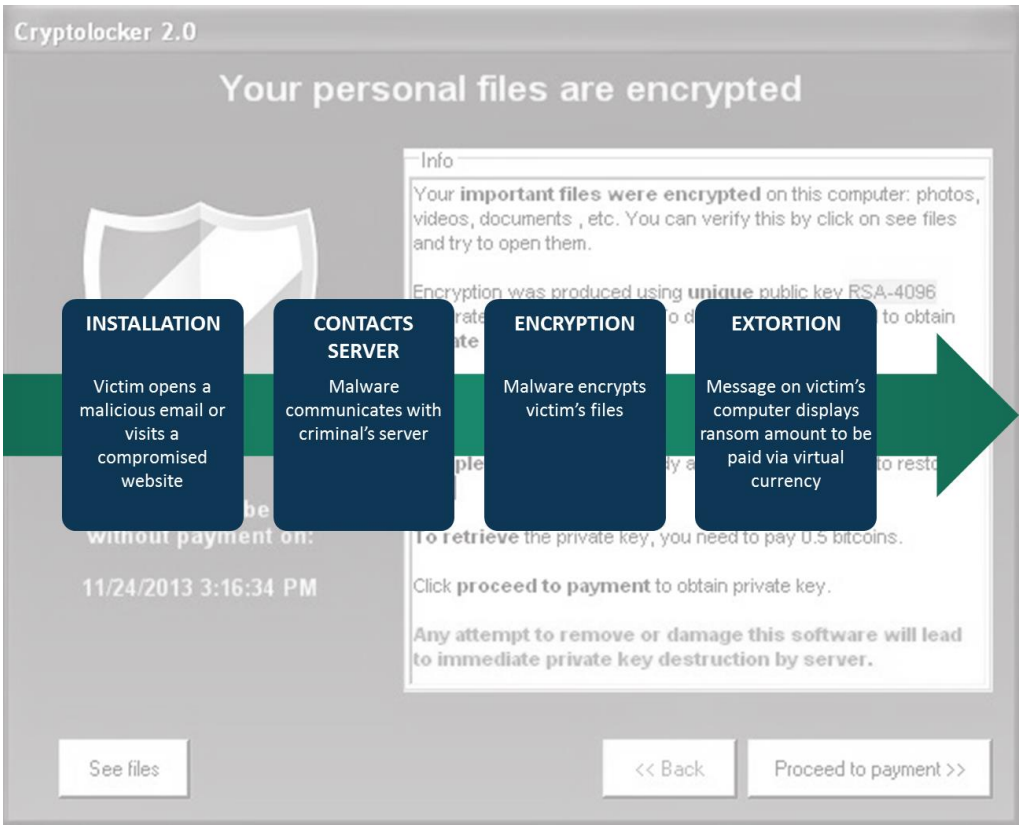
Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices.

Fraudulent transfers have gone through accounts in many countries, with a large majority traveling through Asia. The scam began to evolve in 2013 when victims indicated the email accounts of Chief Executive Officers or Chief Financial Officers of targeted businesses were hacked or spoofed, and wire payments were requested to be sent to fraudulent locations. BEC/EAC continued to evolve, and in 2014 victim businesses reported having personal emails compromised and multiple fraudulent requests for payment sent to vendors identified from their contact list. 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 requests for Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees.

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 2016, the IC3 received 12,005 BEC/EAC complaints with losses of over $360 million.

Ransomware

Ransomware is a form of malware targeting both human and technical weaknesses in an effort to deny the availability of critical data and/or systems. Ransomware is frequently delivered through various vectors, including phishing and Remote Desktop Protocol (RDP). RDP allows computers to connect to each other across a network. 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. Recent iterations target specific organizations and their employees, making awareness and training a critical preventative measure. In 2016, the IC3 received 2,673 complaints identified as ransomware with losses of over $2.4 million.



See footnote for accessibility description of image.[5]

[5] Image depicts typical ransomware process: Step One – Installation: victim opens a malicious email or visits a compromised website. Step Two – Contacts Server: malware communicates with criminal's server. Step Three – Encryption: malware encrypts victim's files. Step Four – Extortion: Message on victim's computer displays ransom amount, to be paid via virtual currency.

Tech Support Fraud

Tech support fraud occurs when the subject claims to be associated with a computer software or security company, or even a cable or Internet company, offering technical support to the victim. Phony tech support companies utilize several different methods to contact or lure their victims. This list is not all inclusive, as the subjects are always varying their schemes.

1. Cold call
2. Pop-up or locked screen
3. Search Engine Optimization: The subject pays to have their company websites appear in the top of search results when a victim searches for technical support.
4. URL Hijacking / Typosquatting: The subject relies on mistakes made by the victim when entering a URL, which either causes an "error" or redirects to the subject's website.

Once the phony tech support company or representative makes verbal contact with the victim, the subject tries to convince the victim to provide remote access to their device. Once the subject has control, additional criminal activity occurs. For example:

- The subject takes control of the victim's device and/or bank account, and will not release control until the victim pays a ransom.
- The subject accesses computer files containing financial accounts, passwords, or personal data (health records, social security numbers, etc.).
- The subject intentionally installs viruses on the device.
- The subject threatens to destroy the victim's computer or continues to call in a harassing manner.

A variation of the fraud, where the subject contacts the victim offering a refund for tech support services previously rendered, has increased. The victim is convinced to allow the subject access to their device and to log onto their online bank account to process the refund. The subject then has control of the victim's device and bank account. With this access, the subject claims to have "mistakenly" refunded too much money to the victim's accounts, and requests the victim wire the difference back to the subject company. In reality, the subject transferred funds among the victim's own accounts (checking, savings, retirement, etc.) to make it appear as though funds were deposited. The victim wires money to the subject, thereby suffering a loss, and does not find out until later the "overpayment" was simply a shift of funds between the victim's own accounts. The refund and wiring process can occur multiple times, thereby exacerbating the losses.

The IC3 has received thousands of tech support related fraud complaints. Victims have lost millions of dollars to the perpetrators. In 2016, the IC3 received 10,850 tech support fraud complaints with losses in excess of $7.8 million. While the majority of tech support fraud

victims are from the U.S., the fraud was reported by victims in 78 different countries. The fraud affects victims of all ages; however, older victims are often the most vulnerable.

Extortion

Extortion is defined as an incident when a cyber criminal demands something of value from a victim by threatening physical or financial harm or the release of sensitive data. Extortion is often used in various schemes reported to the IC3, including Denial of Service attacks, hitman schemes[6], sextortion[7], Government impersonation schemes, loan schemes[8], and high-profile data breaches[9]. Another tactic exploited in extortion schemes is the use of virtual currency as a payment mechanism. Virtual currency provides the cyber criminal an additional layer of anonymity when perpetrating these schemes. The IC3 continues to receive complaints regarding various extortion techniques. In 2016, the IC3 received 17,146 extortion-related complaints with adjusted losses of over $15 million.

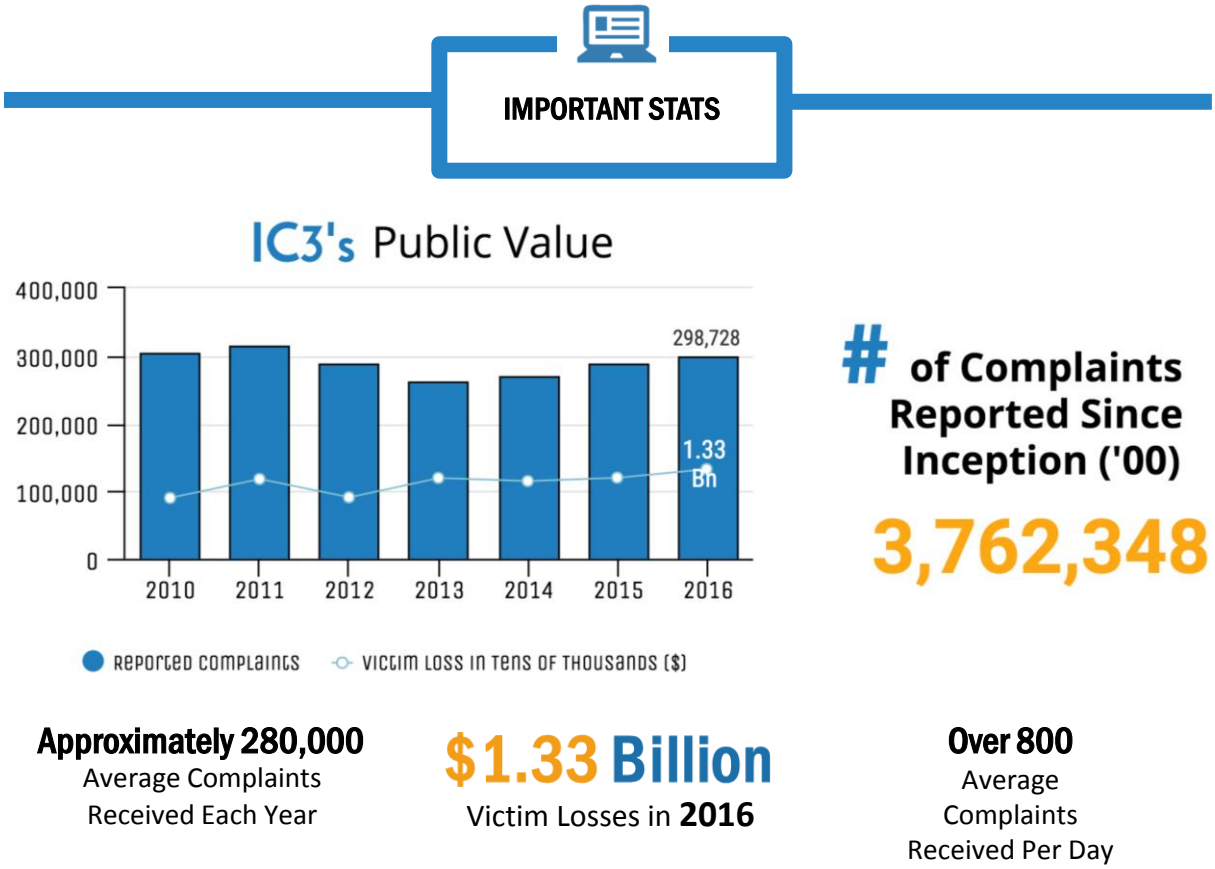
[6] *Hitman Scheme*: Described as an email extortion in which a perpetrator sends a disturbing email threatening to kill a victim and/or their family. The email instructs the recipient to pay a fee to remain safe and avoid having the hit carried out.

[7] *Sextortion*: Described as a situation in which someone threatens to distribute your private and sensitive material if you don't provide them images of a sexual nature, sexual favors, or money.

[8] *Loan Scheme*: Described as a situation in which perpetrators contact victims claiming to be a debt collector from a legitimate company instructing victims to pay fees in order to avoid legal consequences.

[9] *High Profile Data Breach*: 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.

2016 Overall Statistics



See footnote for accessibility description of image.[10]

2016 Victims by Age Group

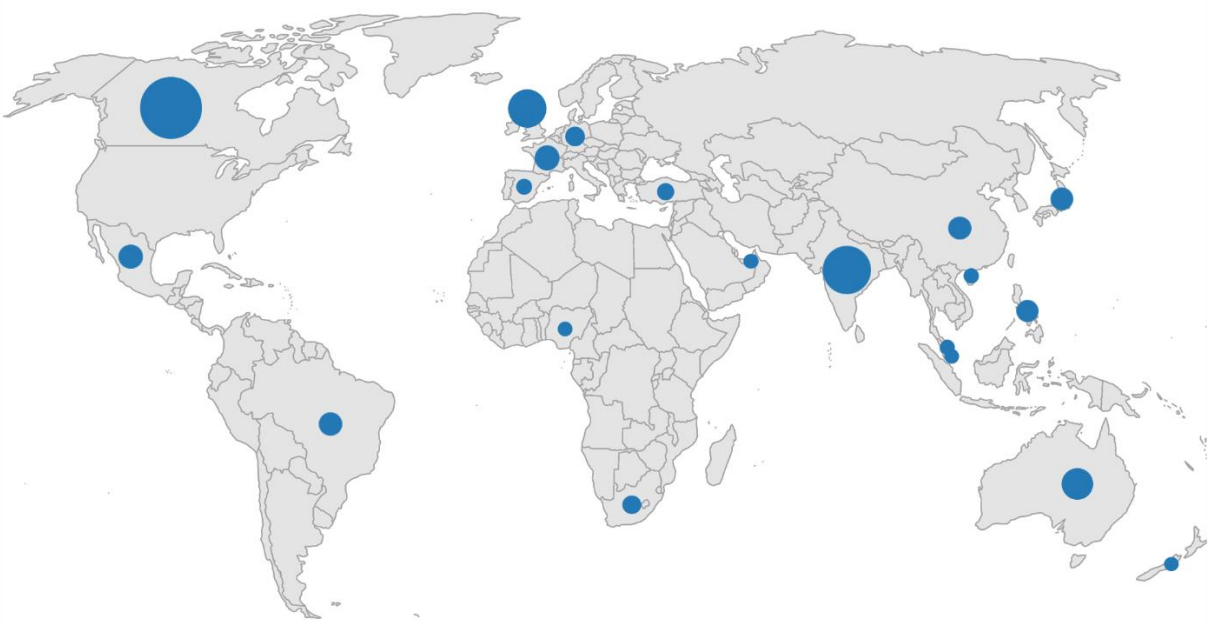
Victims		
Age Range[11]	Total Count	Total Loss
Under 20	10,004	$6,698,742
20 - 29	46,266	$68,015,095
30 - 39	54,670	$190,095,752
40 - 49	51,394	$224,322,960
50 - 59	49,208	$298,145,628
Over 60	55,043	$339,474,918

[10] Image depicts several key statistics regarding complaints and victim loss. A bar chart shows total number of complaints and overall victim loss for the years 2010 to 2016. For 2016, 298,728 complaints were received, with a total victim loss of $1.33 billion. The total number of complaints received since the year 2000 is 3,762,348. IC3 receives approximately 280,000 complaints each year, or more than 800 per day.

[11] Not all complaints include an associated age range—those without this info are excluded from this table.

Top 20 Foreign Countries by Victim

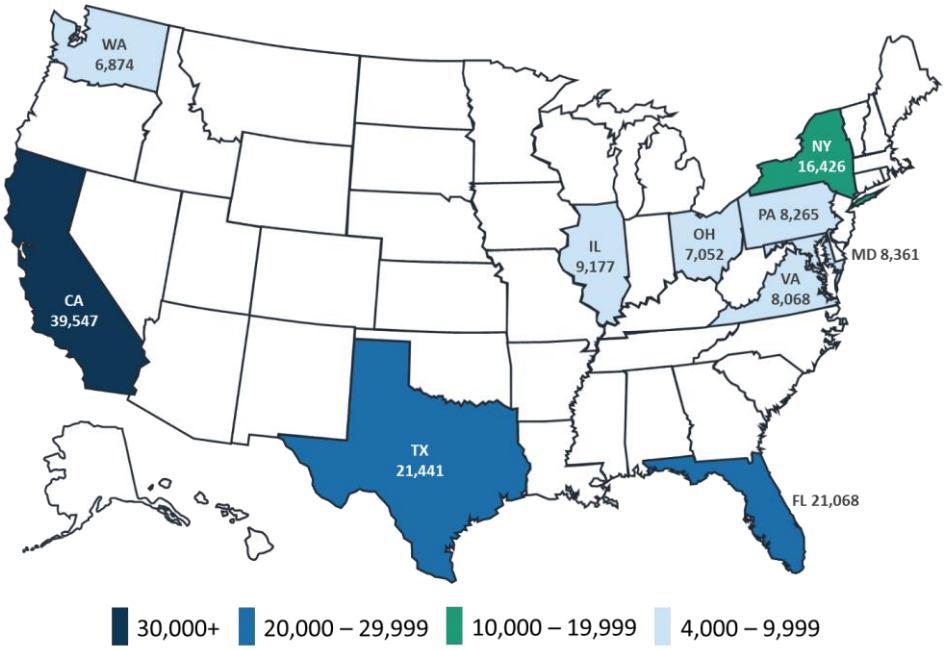
Excluding the United States[12]



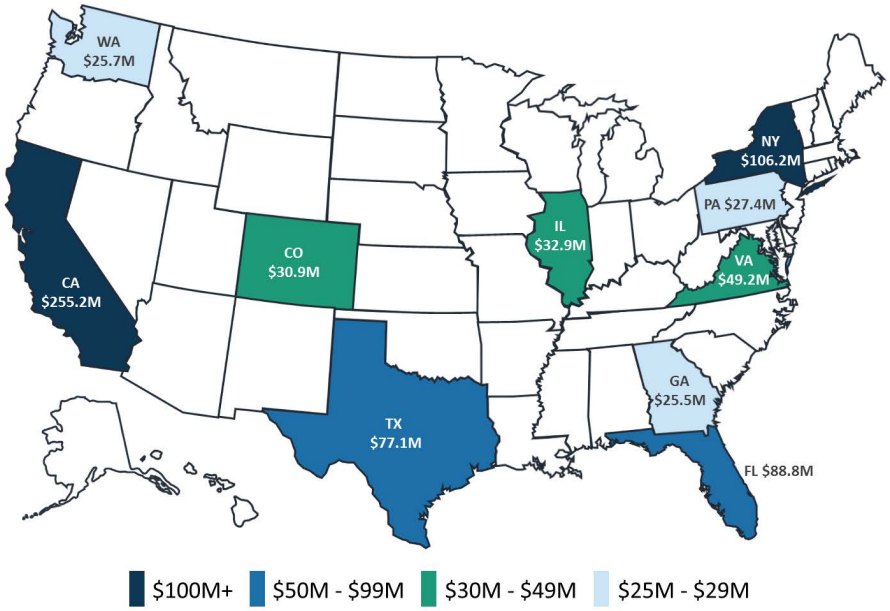
1. Canada	3,772	6. Brazil	533	11. Germany	350	16.United Arab Emirates	202
2. India	2,188	7. Mexico	521	12. South Africa	337	17. Malaysia	193
3. United Kingdom	1,509	8. China	473	13. Turkey	286	18. Singapore	192
4. Australia	936	9. Japan	447	14. Spain	229	19. Nigeria	188
5. France	568	10. Philippines	439	15. Hong Kong	223	20. New Zealand	187

[12] 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 included. Specific stats for each country can be found in the text table immediately below the image.

Top 10 States by Number of Reported Victims [13]



Top 10 States by Reported Victim Loss [14]



[13] Accessibility description: image depicts the United States, with the top ten states (based on reported victims) highlighted. These include California (39,547), Texas (21,441), New York (16,426), Florida (21,068), Illinois (9,177), Pennsylvania (8,265), Maryland (8,361), Virginia (8,068), Ohio (7,052), and Washington (6,874).

[14] Accessibility description: image depicts the United States, with the top ten states (based on reported victim loss). These include California ($255.2M), New York ($106.2M), Florida ($88.8M), Texas ($77.1M), Virginia ($49.2M), Illinois ($32.9M), Colorado ($30.9M), Pennsylvania ($27.4M), Washington ($25.7M), and Georgia ($25.5M).

2016 Crime Types

By Victim Count			
Crime Type	**Victims**	**Crime Type**	**Victims**
Non-Payment/Non-Delivery	81,029	Lottery/Sweepstakes	4,231
Personal Data Breach	27,573	Corporate Data Breach	3,403
419/Overpayment	25,716	Malware/Scareware	2,783
Phishing/Vishing/Smishing/Pharming	19,465	Ransomware	2,673
Employment	17,387	IPR/Copyright and Counterfeit	2,572
Extortion	17,146	Investment	2,197
Identity Theft	16,878	Virus	1,498
Harassment/Threats of Violence	16,385	Crimes Against Children	1,230
Credit Card Fraud	15,895	Civil Matter	1,070
Advanced Fee	15,075	Denial of Service	979
Confidence Fraud/Romance	14,546	Re-shipping	893
No Lead Value	13,794	Charity	437
Other	12,619	Health Care Related	369
Real Estate/Rental	12,574	Terrorism	295
Government Impersonation	12,344	Gambling	137
BEC/EAC	12,005	Hacktivist	113
Tech Support	10,850		
Misrepresentation	5,436		

Descriptors*		
Social Media	18,712	*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	1,904	

2016 Crime Types *Continued*

By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	$360,513,961	Misrepresentation	$13,725,233
Confidence Fraud/Romance	$219,807,760	Government Impersonation	$12,278,714
Non-payment/Non-Delivery	$138,228,282	Denial of Service	$11,213,566
Investment	$123,407,997	Tech Support	$7,806,416
Corporate Data Breach	$95,869,990	IPR/Copyright and Counterfeit	$6,829,467
Other	$73,092,101	Malware/Scareware	$3,853,351
Advanced Fee	$60,484,573	Ransomware	$2,431,261
Personal Data Breach	$59,139,152	Re-shipping	$1,932,021
Identity Theft	$58,917,398	Charity	$1,660,452
Civil Matter	$57,688,555	Virus	$1,635,321
419/Overpayment	$56,004,836	Health Care Related	$995,659
Credit Card Fraud	$48,187,993	Gambling	$290,693
Real Estate/Rental	$47,875,765	Terrorism	$219,935
Employment	$40,517,605	Crimes Against Children	$79,173
Phishing/Vishing/Smishing/Pharming	$31,679,451	Hacktivist	$55,500
Harassment/Threats of Violence	$22,005,655	No Lead Value	$0
Lottery/Sweepstakes	$21,283,769		
Extortion	$15,811,837		

Descriptors*		
Social Media	$66,401,318	*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	$28,302,365	

2016 Overall State Statistics

Count by Victim per State*					
Rank	State	Victims	Rank	State	Victims
1	California	39,547	30	Oklahoma	2,455
2	Texas	21,441	31	Utah	2,295
3	Florida	21,068	32	Kansas	1,963
4	New York	16,426	33	Arkansas	1,853
5	Illinois	9,177	34	New Mexico	1,702
6	Maryland	8,361	35	Iowa	1,560
7	Pennsylvania	8,265	36	Mississippi	1,467
8	Virginia	8,068	37	Alaska	1,259
9	Ohio	7,052	38	West Virginia	1,153
10	Washington	6,874	39	New Hampshire	1,126
11	Colorado	6,847	40	Idaho	1,120
12	Georgia	6,697	41	Hawaii	1,055
13	New Jersey	6,690	42	Nebraska	1,028
14	North Carolina	6,492	43	District of Columbia	938
15	Michigan	6,384	44	Maine	770
16	Arizona	6,349	45	Montana	744
17	Massachusetts	4,888	46	Puerto Rico	709
18	Tennessee	4,693	47	Delaware	703
19	Indiana	4,658	48	Rhode Island	663
20	Missouri	4,096	49	Vermont	440
21	Oregon	3,947	50	Wyoming	432
22	Nevada	3,775	51	South Dakota	376
23	Alabama	3,726	52	North Dakota	350
24	Wisconsin	3,662	53	Guam	50
25	South Carolina	3,500	54	U.S. Minor Outlying Islands	42
26	Minnesota	3,390	55	Virgin Islands, U.S.	42
27	Louisiana	3,002	56	Northern Mariana Islands	15
28	Kentucky	2,621	57	American Samoa	10
29	Connecticut	2,545			

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

2016 Overall State Statistics *Continued*

Loss by Victim per State*					
Rank	**State**	**Loss**	**Rank**	**State**	**Loss**
1	California	$255,181,657	30	Arkansas	$7,917,870
2	New York	$106,225,695	31	Utah	$7,304,226
3	Florida	$88,841,178	32	Alabama	$7,178,091
4	Texas	$77,135,765	33	Kansas	$7,011,898
5	Virginia	$49,175,677	34	Connecticut	$6,960,531
6	Illinois	$32,938,414	35	Iowa	$5,013,079
7	Colorado	$30,893,224	36	Nebraska	$4,289,411
8	Pennsylvania	$27,432,303	37	Idaho	$4,174,839
9	Washington	$25,728,634	38	Mississippi	$3,473,575
10	Georgia	$25,477,413	39	New Hampshire	$3,171,083
11	New Jersey	$24,500,833	40	Montana	$3,052,401
12	North Carolina	$24,194,018	41	Hawaii	$2,924,323
13	Michigan	$24,174,754	42	West Virginia	$2,576,787
14	Maryland	$23,145,424	43	Alaska	$2,276,799
15	Arizona	$20,567,423	44	Puerto Rico	$2,084,360
16	Ohio	$20,410,854	45	District of Columbia	$1,921,649
17	Massachusetts	$20,324,110	46	Delaware	$1,675,255
18	Missouri	$15,886,334	47	Rhode Island	$1,570,612
19	Oklahoma	$15,412,650	48	Maine	$1,192,677
20	Nevada	$15,246,405	49	South Dakota	$933,723
21	Oregon	$13,767,261	50	Wyoming	$913,941
22	Louisiana	$13,290,356	51	North Dakota	$859,856
23	Minnesota	$12,634,057	52	Vermont	$855,007
24	Tennessee	$12,557,922	53	Guam	$676,443
25	South Carolina	$10,860,131	54	Virgin Islands, U.S.	$155,114
26	Wisconsin	$10,309,552	55	U.S. Minor Outlying Islands	$59,066
27	Kentucky	$9,381,342	56	Northern Mariana Islands	$55,917
28	Indiana	$9,266,381	57	American Samoa	$300
29	New Mexico	$8,701,654			

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

2016 Overall State Statistics *Continued*

Count by Subject per State*					
Rank	**State**	**Subjects**	**Rank**	**State**	**Subjects**
1	California	15,240	30	Minnesota	1,084
2	Texas	11,309	31	Kansas	1,079
3	Florida	8,528	32	Mississippi	1,021
4	New York	7,636	33	Louisiana	919
5	Illinois	3,841	34	Connecticut	794
6	Georgia	3,614	35	Kentucky	777
7	Maryland	3,241	36	Wisconsin	774
8	Washington	2,779	37	Iowa	565
9	Virginia	2,603	38	Montana	547
10	Nebraska	2,444	39	Arkansas	532
11	New Jersey	2,439	40	New Mexico	406
12	Pennsylvania	2,433	41	Idaho	346
13	Ohio	2,414	42	West Virginia	312
14	Arizona	2,226	43	Hawaii	296
15	Michigan	2,178	44	North Dakota	287
16	North Carolina	2,074	45	New Hampshire	250
17	Tennessee	1,814	46	Maine	240
18	Nevada	1,748	47	Alaska	215
19	Colorado	1,628	48	Rhode Island	200
20	Massachusetts	1,443	49	Vermont	186
21	Missouri	1,384	50	Puerto Rico	163
22	South Carolina	1,374	51	South Dakota	146
23	District of Columbia	1,360	52	Wyoming	138
24	Oklahoma	1,283	53	U.S. Minor Outlying Islands	18
25	Utah	1,262	54	Guam	14
26	Indiana	1,246	55	Virgin Islands, U.S.	10
27	Alabama	1,226	56	Northern Mariana Islands	3
28	Delaware	1,149	57	American Samoa	2
29	Oregon	1,109			

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

2016 Overall State Statistics *Continued*

Subject Earnings per Destination State*					
Rank	State	Loss	Rank	State	Loss
1	California	$74,917,042	30	Alabama	$4,258,587
2	Texas	$57,602,715	31	Connecticut	$3,507,155
3	Hawaii	$50,893,790	32	Utah	$3,322,074
4	New York	$46,039,475	33	Louisiana	$3,278,684
5	Florida	$38,158,286	34	Iowa	$2,681,761
6	Georgia	$24,821,761	35	Kentucky	$2,660,183
7	Colorado	$17,735,623	36	Kansas	$2,616,821
8	Illinois	$12,867,132	37	Delaware	$2,560,784
9	Pennsylvania	$12,557,106	38	Mississippi	$2,428,942
10	New Jersey	$11,834,991	39	Arkansas	$1,969,540
11	Wisconsin	$10,726,136	40	New Mexico	$1,850,003
12	Oregon	$10,660,242	41	Montana	$1,517,688
13	Arizona	$10,440,842	42	Idaho	$1,347,658
14	Washington	$10,215,859	43	Rhode Island	$960,607
15	Virginia	$9,940,731	44	West Virginia	$793,537
16	Oklahoma	$7,819,581	45	North Dakota	$791,530
17	Ohio	$7,651,776	46	Maine	$518,573
18	Missouri	$7,581,974	47	Alaska	$517,609
19	Maryland	$7,442,627	48	New Hampshire	$484,082
20	Michigan	$6,703,012	49	South Dakota	$418,626
21	North Carolina	$6,314,756	50	Vermont	$263,594
22	Nevada	$6,272,081	51	Wyoming	$261,875
23	Massachusetts	$6,119,164	52	Puerto Rico	$227,168
24	Nebraska	$6,049,631	53	Guam	$210,000
25	Minnesota	$6,018,709	54	U.S. Minor Outlying Islands	$65,723
26	Indiana	$5,188,886	55	Northern Mariana Islands	$29,832
27	District of Columbia	$5,143,770	56	Virgin Islands, U.S.	$18,181
28	Tennessee	$4,860,522	57	American Samoa	$0
29	South Carolina	$4,589,415			

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

Appendix A: Crime Type Definitions

419/Overpayment: "419" is a term that refers to the section in Nigerian law associated with con artistry and fraud, associated with solicitation from individuals requesting help in facilitating the transfer of money. The sender offers a commission or share in the profits, but will first ask that money be sent to pay for some of the costs associated with the transfer. (Overpayment) An individual is sent a payment and instructed to keep a portion of the payment, but send the rest on to another individual or business.

Advanced Fee: An individual pays money to someone in anticipation of receiving something of greater in return, but instead, receives significantly less than expected or nothing.

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 (not individuals) working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam which 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: Using deception to get money from individuals believing they are making donations to legitimate charities and/or charities representing victims of natural disasters shortly after the incident occurs.

Civil Matter: Civil litigation generally includes all disputes formally submitted to a court, about any subject in which one party is claimed to have committed a wrong, but not a crime. In general, this is the legal process most people think of when the word "lawsuit" is used.

Confidence Fraud/Romance: An individual believes they are in a relationship (family, friendly, or romantic) and are tricked into sending money, personal and financial information, or items of value to the perpetrator or to launder money or items to assist the perpetrator. This is basically the Grandparent's Scheme and any scheme in which the perpetrator preys on the complainant's "heartstrings."

Corporate Data Breach: A leak/spill of business data which is released from a secure location to an untrusted environment. 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 theft and fraud committed using a credit card or any similar payment mechanism (ACH, EFT, recurring charge, etc.) 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 one 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) Utilizing false accusations or statements of fact (as in defamation) to intimidate. (Threats of Violence) 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 which usually involve health care providers, companies, or individuals. Schemes may include offers for (fake) insurance cards, health insurance market place assistance, stolen health information, or various other scams and/or any scheme involving medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums/social media, and fraudulent websites.

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

Identity Theft/Account Takeover: (Identity Theft) Someone steals and uses personal identifying information, like a name or Social Security number, without permission to commit fraud or other crimes, or a fraudster obtains account information to perpetrate fraud on existing accounts (Account Takeover).

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 (Retirement, 401K, Ponzi, Pyramid, etc.).

Lottery/Sweepstakes: An individual is contacted about winning a lottery/sweepstakes they never entered.

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: Goods and services are shipped, and payment is never rendered (non-payment). Payment is sent, and goods and services are never received (non-delivery).

Other: Other types of Internet/Non-Internet fraud not listed.

Personal Data Breach: A leak/spill of personal data which is released from a secure location to an untrusted environment. Also, 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: The use of 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 at their residence and subsequently repackage the merchandise for shipment, usually abroad.

Real Estate/Rental: Loss of funds from a real estate investment or fraud involving 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 (terror); are 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/crypto currency (Bitcoin, Litecoin, Potcoin, etc.).

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu