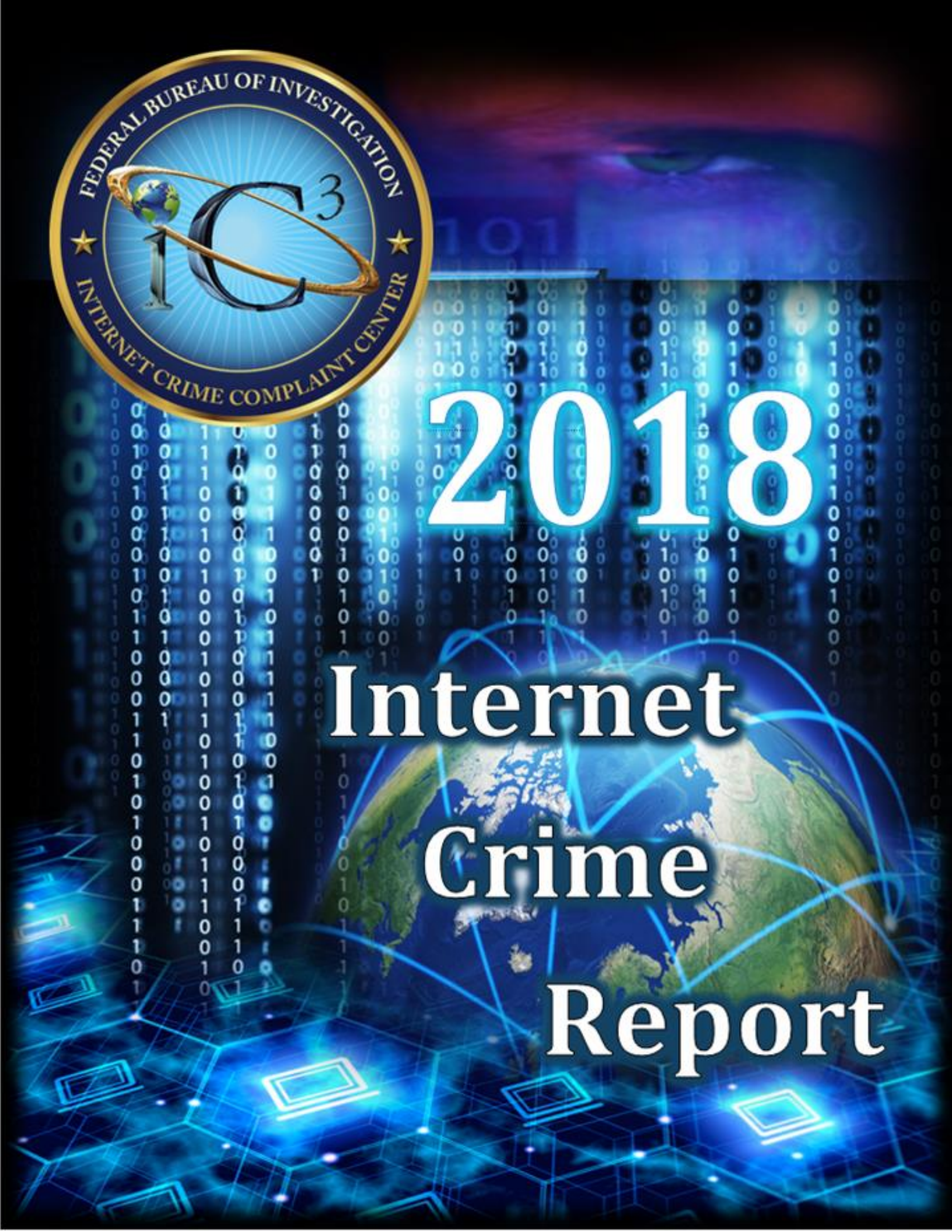

FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER
2018
Internet
Crime
Report

2018 INTERNET CRIME REPORT

TABLE OF CONTENTS

INTRODUCTION

Dear Reader,

The FBI is the lead federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists, and the FBI's IC3 provides the public with a trustworthy and convenient reporting mechanism to submit information concerning suspected Internet-facilitated criminal activity.

The 2018 Internet Crime Report emphasizes the IC3's efforts in monitoring trending scams such as Business Email Compromise (BEC), Extortion, Tech Support Fraud, and Payroll Diversion. In 2018, IC3 received a total of 351,937 complaints with losses exceeding $2.7 Billion.

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

In February 2018, the IC3 established the Recovery Asset Team (RAT) to assist in the recovery of funds for victims involved in BEC schemes by streamlining communications to financial Institutions. The RAT works within the Domestic Financial Fraud Kill Chain (DFFKC) to recover fraudulent funds wired by victims. The DFFKC is a partnership between law enforcement and financial entities. In 2018, the IC3 RAT notified 56 field offices and 12 Legal Attachés of 1,061 DFFKC's totaling $257,096,992, a recovery rate of 75%.

Another new asset of the IC3 was the creation of the Victim Specialists-Internet Crimes (VSIC) position. The VSIC contact victims of internet crimes, provide crisis intervention, conduct needs assessments, and refer victims to resources and referrals when appropriate. This new position is designed to ensure timely support and services are provided to victims to prevent further victimization and to engage the recovery process as quickly as possible. These positions also lead to a greater coordination of services with the victim's local field office Victim Specialist.

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

Matt Gorham

Matt Gorham
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.

In 2018, the Victim Services Division (VSD) collaborated with the IC3 to develop a new position – Victim Specialists -Internet Crimes (VSIC). VSD secured approval and funding for three positions to be placed at the IC3. These VSIC positions are able to contact victims, provide crisis intervention, conduct needs assessments, and refer victims to resources and referrals when appropriate. In many circumstances, complaints involving cyberbullying, harassment, ID theft, and confidence scams may never rise to the level of a Federal investigation. Due to the nature of the system through which these complaints are vetted and then filtered down to local law enforcement officers, victims may not get the help they need in time. The FBI is obligated to try and triage these victims as their first line of defense. VSICs positioned at IC3 facilitate the necessary support services for victims that reach out. The key component in this process of assistance is to ensure timely support and services are provided to prevent further victimization and to engage the recovery process as quickly as possible.

The benefit from VSICs positioned at IC3 is that they are able to quickly reach out and call these victims to intervene and offer assistance. Many victims do not believe they have been compromised and genuinely want to help the perpetrator. Skilled VSICs can help navigate those feelings for the victim, allow them to come to terms with what has happened, and provide them the resources and steps necessary to get their life back together.

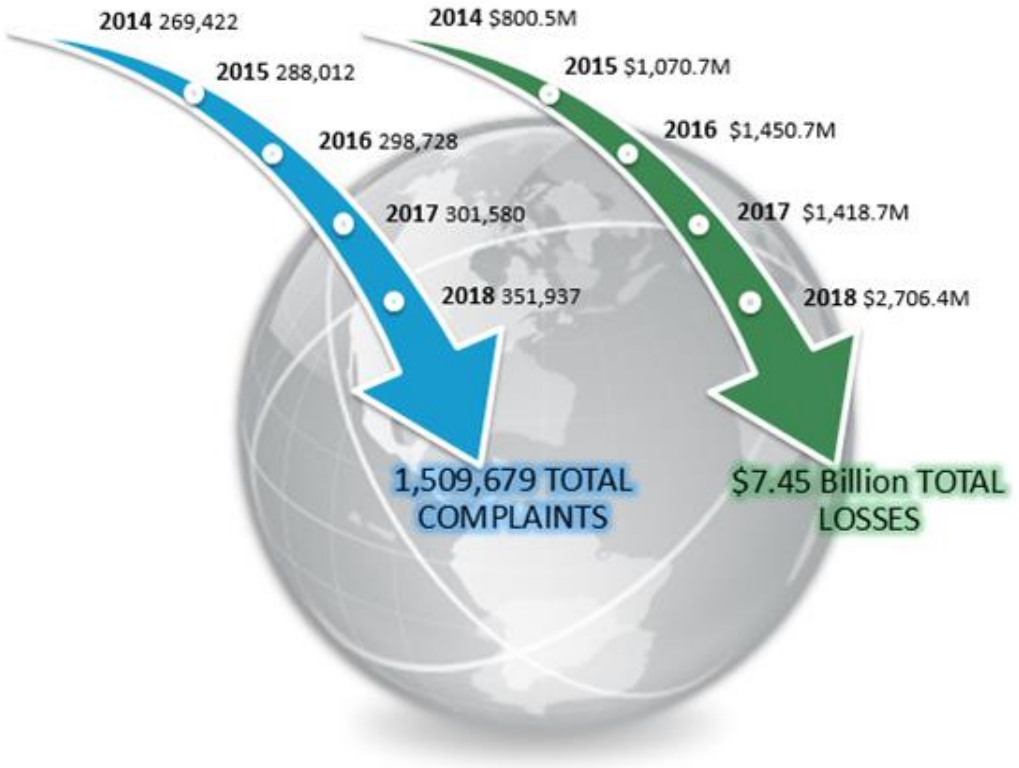
These positions also lead to a greater coordination of services. VSICs at IC3 work with the victim's local field office Victim Specialist (VS) to coordinate in-person services and support. VSICs at IC3 have the opportunity to liaison with their counterparts in the field and, should the situation warrant, they can work with the VS in the victim's area to facilitate a follow up meeting. This tremendously benefits VSs in the field in that the IC3 VSICs have developed much of the preliminary information the VS would try to assess in their first meeting with the victim. The field VS is able to work more efficiently with greater background information available prior to their first encounter. Timely victim assistance and support can further victimization and can start the victim instead on a path towards recovery.

IC3 HISTORY

In May 2000, the IC3 was established as a center to receive complaints of Internet crime. There have been 4,415,870 complaints reported to the IC3 since its inception. Over the last five years, the IC3 has received an average of almost 300,000 complaints per year. The complaints address a wide array of Internet scams affecting victims across the globe.[1]

IC3 Complaint Statistics

2014-2018



[1] Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2014 to 2018. Over that time period, IC3 received a total of 1,509,679 complaints, and a total loss of $7.45 billion.

THE IC3 ROLE IN COMBATING CYBER CRIME[2]

WHAT WE DO

Central Hub to Alert the Public

Victims Report Internet Crime Via

www.IC3.gov

Partner with Private Sector and with Local, State, Federal, and International Agencies

Increase Victim Reporting via Outreach

Host Remote Access Database for all Law Enforcement via the FBI's LEEP website

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

IC3 CORE FUNCTIONS

COLLECTION	ANALYSIS	PUBLIC AWARENESS	REFERRALS
The IC3 is the central point for Internet crime victims to report and alert the appropriate agencies to suspected criminal Internet activity. 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 Internet crime, as well as any other relevant information necessary to support the complaint.	The IC3 reviews and analyzes data submitted through its website and produces intelligence products to highlight emerging threats and new trends.	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 used 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.	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.

IC3 Core Functions[3]

[3] Accessibility description: image contains a table and wheel with the core functions. 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, as well as 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.

The IC3 has received feedback indicating remote access to the IC3 database is indeed enhancing cases. For example, the Putnam County Sheriff's Office in Carmel, New York, searched the IC3 database as part of an investigation and identified three related IC3 complaints. They said, "We did one of these cases years ago and it took us months to make the connections that I was able to make with IC3 in less than an hour. I'm definitely a huge fan of the database and its power."

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.

The IC3 receives, on average, 900 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, **18** investigations were opened in 2018. Accomplishments included arrests, disruptions, convictions, indictments, and asset forfeitures. In addition, financial restitutions were obtained and criminals were sentenced.

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.

During 2018, the IC3 provided 123 referrals to 13 CTFs based on **1192** victim complaints. The total victim loss associated with these complaints was approximately $28.1 million.

OWS Statistics[4]

[4]Accessibility description: images containing the number of Field Offices (13) involved with the OWS initiative, the number of opened investigations (18), and the number of victims (1192).

HOT TOPICS FOR 2018

BUSINESS EMAIL COMPROMISE (BEC)

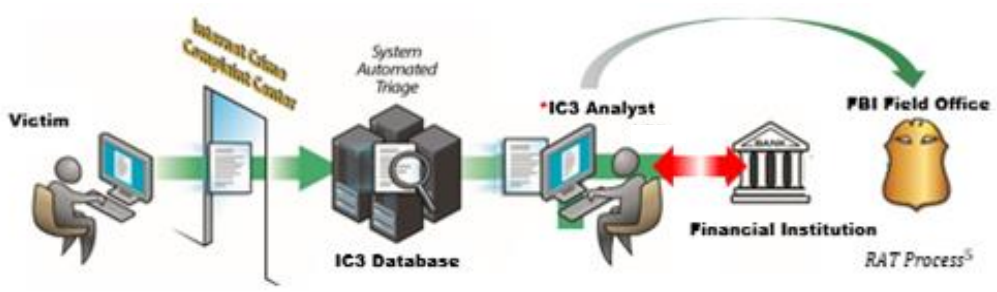
In 2018, the IC3 received 20,373 BEC/E-mail Account Compromise (EAC) complaints with adjusted losses of over $1.2 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing wire transfer payments. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

BEC and EAC are constantly evolving as scammers become more sophisticated. In 2013, BEC/EAC scams routinely began with the hacking or spoofing of the email accounts of chief executive officers or chief financial officers, and fraudulent emails were sent requesting wire payments be sent to fraudulent locations. Through the years, the scam has seen personal emails compromised, vendor emails compromised, spoofed lawyer email accounts, requests for W-2 information, and the targeting of the real estate sector.

In 2018, the IC3 received an increase in the number of BEC/EAC complaints requesting victims purchase gift cards. The victims received a spoofed email, a spoofed phone call or a spoofed text from a person in authority requesting the victim purchase multiple gift cards for either personal or business reasons.

IC3 RECOVERY ASSET TEAM

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the recovery of funds for victims who made transfers to domestic accounts under fraudulent pretenses.



*If criteria is met, transaction details are forwarded to the identified point of contact at recipient bank to notify of fraudulent activity and request freezing of account. Once response is received from the recipient bank, RAT contacts the appropriate field office(s).

The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis.

Recovery to Date:
02/02/2018 to 12/31/2018

Incidents: 1,061

Losses: $257,096,991.65

Recovery: $192,699,195.72

Recovery Rate: 75%

Goals of RAT-Financial Institution Partnership

- Assist in the identification of potentially fraudulent accounts across the sector.
- Remain at the forefront of emerging trends among financial fraud schemes.
- Foster a symbiotic relationship in which information is appropriately shared.

Guidance for BEC Victims

- Contact the originating Financial Institution as soon as fraud is recognized to request a recall or reversal as well as a Hold Harmless Letter or Letter of Indemnity.
- File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.
- Visit www.ic3.gov for updated PSAs regarding BEC trends as well as other fraud schemes targeting specific populations (real estate, pre-paid cards, W-2, etc.).
- Never make any payment changes without verifying with the intended recipient; verify email addresses are accurate when checking mail on a cell phone or other mobile device.

[5] Accessibility description: complaint flow with fraudulent account information through the RAT process.

RAT SUCCESSES

In its first year, the IC3 RAT has already been proven instrumental. The following are four examples of the RAT's successful contributions in investigative efforts.

New York

In February 2018, the IC3 RAT received a complaint filed by a BEC victim located in New York, who, after receiving a compromised email from their closing agent during a real estate transaction, initiated a wire transfer of $50,000.00 to a fraudulent bank account located in New York. The IC3 RAT contacted the bank's fraud department to identify the bank's procedures for fraudulent wire transfer notification. The bank then worked with the IC3 and the victim to recover the funds. In April 2018, the bank reported to the IC3 that the victim would receive a full recovery of the funds.

Denver

In September 2018, the IC3 RAT received a complaint filed by a BEC victim located in Colorado. The victim reported that they initiated a fraudulent wire transfer of $56,179.27 after receiving a spoofed email from a lending agent during a real estate transaction. The IC3 RAT, working in coordination with the Denver Field Office, contacted the victim's bank and worked with the fraud department to freeze the funds. Because of the IC3 RAT's communication with the bank, the victim was able to recover $54,000.00 of the funds, and purchase their new home.

Newark

In August 2018, the IC3 RAT received a complaint filed on behalf of a town located in New Jersey. The town was the victim of a BEC scam in which they transferred over $1M to a fraudulent account. The IC3 RAT, in coordination with the Newark Field Office, worked with the financial institution partners to successfully freeze the funds and return the money to the town.

New York

In August 2018, the IC3 RAT received a complaint filed by a BEC victim located in Florida reporting a fraudulent wire fraud of $50,000 to a bank located in Bronx, New York. The IC3 RAT contacted the bank's chief of security to identify their procedures for fraudulent wire transfer notification. The bank chief of security then alerted the IC3 RAT when the criminal financial recipient entered the bank and was attempting to request funds from the fraudulent account. The IC3 RAT contacted the New York Field Office, which immediately responded to the bank to arrest the criminal recipient.

PAYROLL DIVERSION

In 2018, the IC3 received approximately 100 complaints with a combined reported loss of $100M. In the Payroll Diversion scam, cybercriminals target employees through phishing emails designed to capture an employee's login credentials. Once the cybercriminal has obtained an employee's credentials, the credentials are used to access the employee's payroll account. The cybercriminal will typically add rules to the employee's account preventing the employee from receiving alerts regarding direct deposit changes. The cybercriminal will then change the direct deposit information, redirecting the payroll funds to an account controlled by the cybercriminal, which is often a prepaid card. Institutions most affected by this scam have been education, healthcare, and commercial airway transportation.

Example of IC3 success:

The IC3 has maintained a working relationship with a major charity since 2005 to address charity fraud when it arises. As a result of the established relationship, the charity contacted the IC3 regarding a Payroll Diversion incident that resulted in the loss of $140,000. The IC3 immediately contacted the Washington Field Office and provided the complaint information, which resulted in the FBI opening a case.

TECH SUPPORT FRAUD

Tech support fraud continues to be a growing problem. In 2018, the IC3 received 14,408 complaints related to tech support fraud from victims in 48 countries. The losses amounted to nearly $39 million, which represents a 161% increase in losses from 2017. The majority of victims reported to be over 60 years of age.

Additional information, explanations, and suggestions for protection regarding tech support fraud is available in a recently published Tech Support Fraud Public Service Announcement on the IC3 website: https://www.ic3.gov/media/2018/180328.aspx

Investigative efforts have yielded many successes. The following are two examples.

Tampa

The IC3 has provided ongoing assistance to the Tampa Field Office, by identifying multiple victims and losses associated with the subject's actions. As a result, a Florida man was charged for serving as a runner and a domestic manager of a call center that engaged in several types of telemarketing fraud, including technical-support fraud. The indictment charged the subject with conspiracy to commit mail and wire fraud, wire fraud, mail fraud, and money laundering. According to the indictment, the subject received checks and cash mailed from victims to his home office, deposited the checks, and sent payments (less a fee for his services) to his India-based co-conspirators. The case is being prosecuted by the U.S. Attorney's Office for the Middle District of Florida. The charges carry a maximum penalty of 20 years in prison. The government has also sought forfeiture of unlawful proceeds.

Los Angeles

The IC3 received a search request from Los Angeles Field Office. Over $388,000 in losses were identified via IC3 victims. As a result, a California man was arrested and charged for serving as a payment gateway for a tech support call center located in India. The subject received and processed payments back to individuals in India running the call center. Many victims lost hundreds of dollars, while some elderly victims lost hundreds of thousands of dollars. In October 2018, the subject entered a guilty plea to one count of Title 18 US Code 371, Conspiracy to Commit Wire Fraud and Mail Fraud. The subject's arrest led to wire fraud charges of two additional Indian citizens for recruiting U.S. co-conspirators in connection with a tech support fraud center in India. This case is being prosecuted by the Consumer Protection Branch, the Antitrust Division, and the U.S. Attorney's Office for the Central District of California. The wire fraud charge carries a maximum penalty of 20 years in prison.

EXTORTION

In 2018, the IC3 received 51,146 extortion-related complaints with adjusted losses of over $83 million which represents a 242% increase in extortion related complaints from 2017. 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 [6] attacks, hitman schemes,[7] sextortion,[8] government impersonation schemes[9], loan schemes,[10] and high-profile data breaches.[11] Virtual currency is commonly demanded as the payment mechanism because it provides the criminal an additional layer of anonymity when perpetrating these schemes. The majority of extortion complaints received in 2018 were part of a sextortion campaign in which victims received an email threatening to send a pornographic video of them or other compromising information to family, friends, coworkers, or social network contacts if a ransom was not paid.

Example of IC3 success:

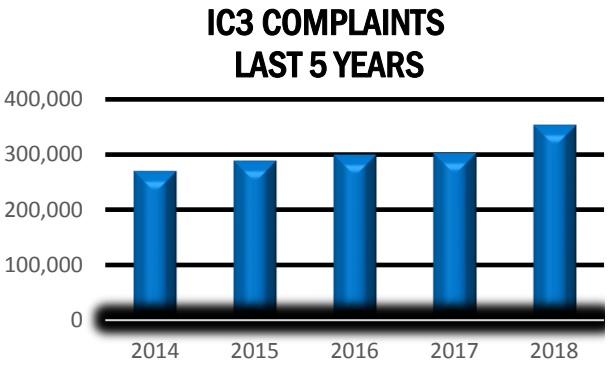
On February 7, 2018, the IC3 referred an intrusion and Distributed Denial of Service (DDoS)[12] extortion complaint to the Los Angeles Field Office for case consideration. A company in the Los Angeles area reported receiving an extortion email claiming to have their customer data and requesting a ransom be paid to stop a DDoS attack. The Los Angeles Field Office opened a case as a result of the IC3 referral. The investigation revealed the email was affiliated with the Apophis Squad, a group that has been reported for multiple bomb threats to schools, and DDoS extortion threats to companies. The IC3 provided the Los Angeles Field Office additional complaints about the Apophis Squad received throughout the year for case enhancement. On February 8, 2019, subjects Timothy Dalton Vaughn and George Duke-Cohan were federally indicted and on February 12, 2019, the FBI arrested Vaughn.

---

[6] A Denial of Service attack typically uses one computer and one Internet connection to flood a network/system.
[7] A *hitman scheme* is an email extortion in which a perpetrator sends a disturbing email threatening to kill the recipient and/or their family. The email instructs the recipient to pay a fee to remain safe and avoid having the hit carried out.
[8] *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.
[9] Government impersonation occurs when a government official is impersonated in an attempt to collect money.
[10] 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.
[11] 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.
[12] A Distributed Denial of Service (DDoS) attack uses multiple computers and Internet connections to flood a network/system.

2018 Overall Statistics[13]

IMPORTANT STATS



 # Of Complaints Reported Since Inception ('00)
4,415,870

Approximately 300,000
Complaints Received Per Year On Average

$2.71 Billion
Victim Losses in **2018**

Over 900
Complaints Received Per Day On Average

2018 VICTIMS BY AGE GROUP

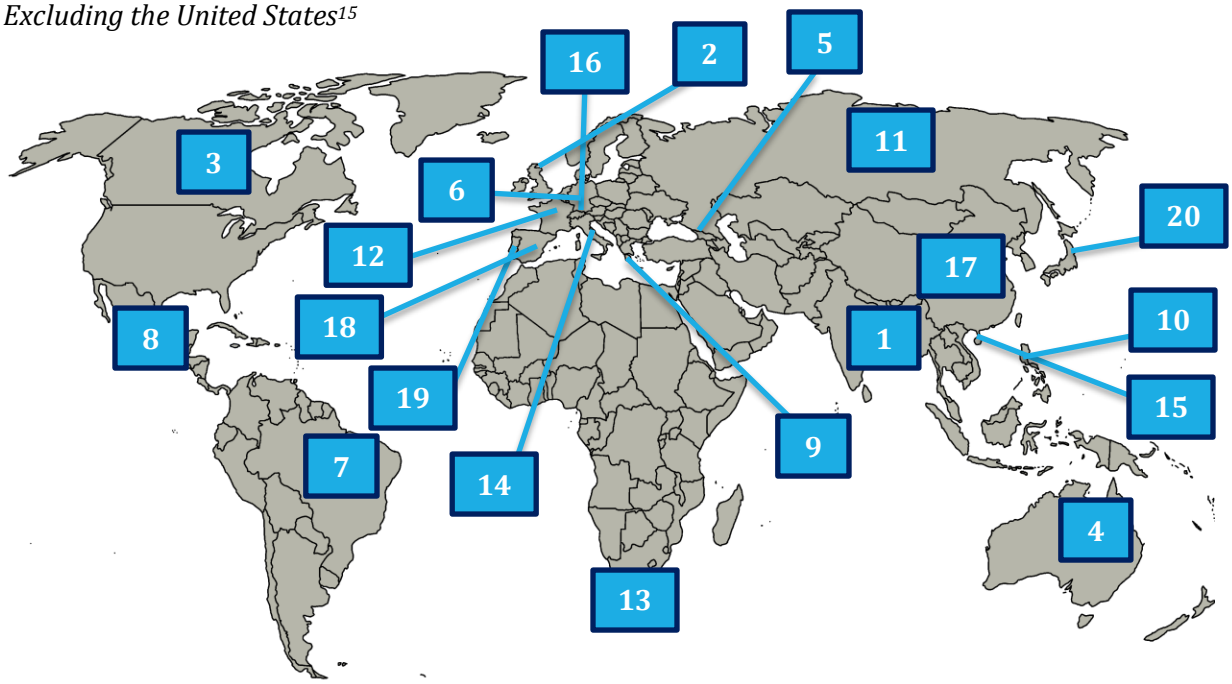
Victims		
Age Range[14]	Total Count	Total Loss
Under 20	9,129	$12,553,082
20 - 29	40,924	$134,485,965
30 - 39	46,342	$305,699,977
40 - 49	50,545	$405,612,455
50 - 59	48,642	$494,926,300
Over 60	62,085	$649,227,724

[13] Accessibility description: image depicts several key statistics regarding complaints and victim loss. A bar chart shows total number of complaints for the years 2014 to 2018. The total number of complaints received since the year 2000 is 4,415,870. IC3 receives approximately 300,000 complaints each year, or more than 900 per day.

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

TOP 20 FOREIGN COUNTRIES BY VICTIM

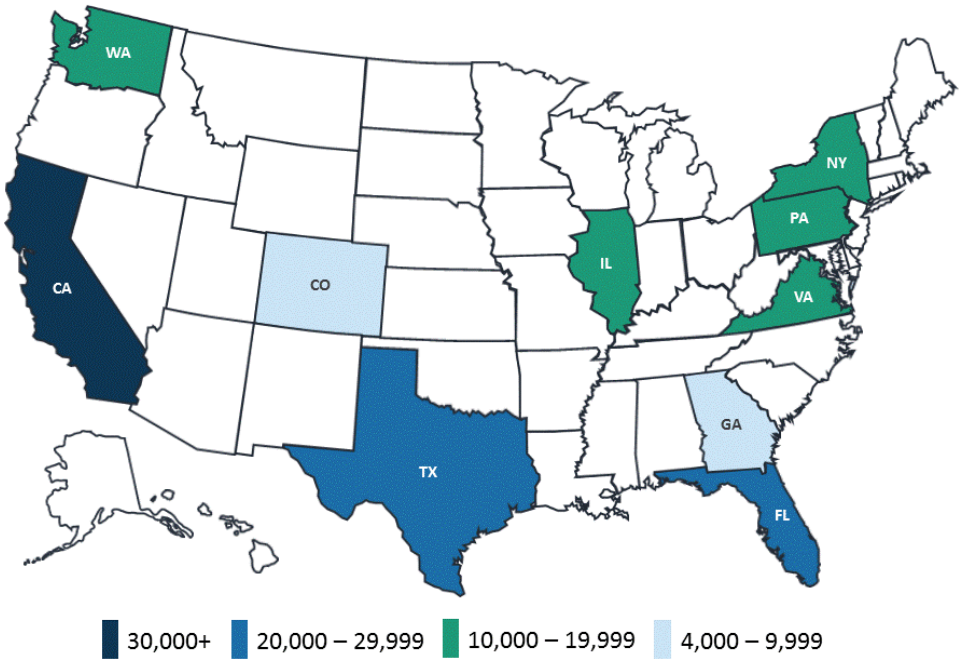
Excluding the United States[15]



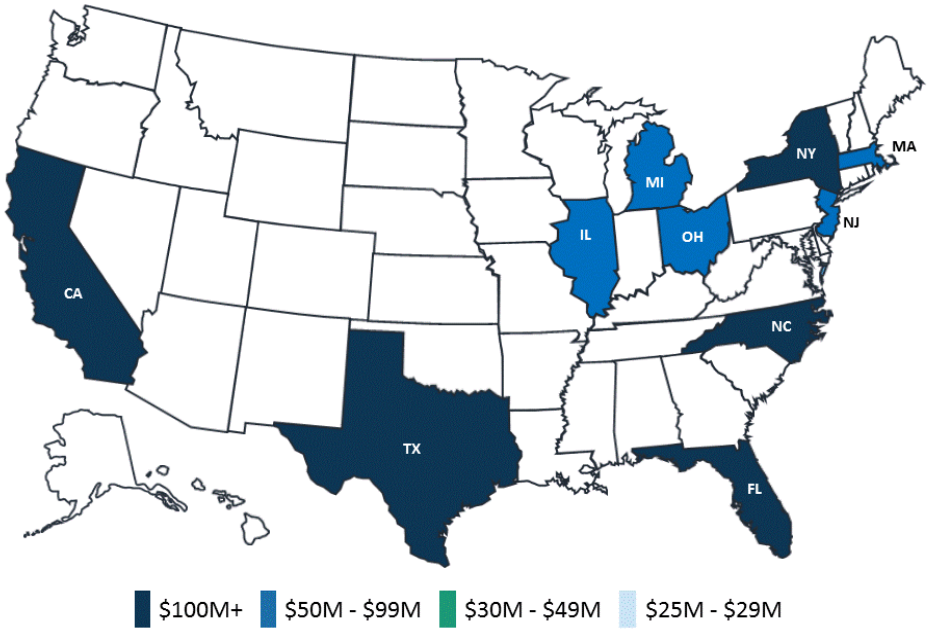
1. India	**4,556**	**6. Germany**	**622**	**11. Russian Federation**	**471**	**16. Switzerland**	**371**
2. United Kingdom	**3,970**	**7. Brazil**	**605**	**12. France**	**428**	**17. China**	**367**
3. Canada	**2,880**	**8. Mexico**	**591**	**13. South Africa**	**409**	**18. Spain**	**331**
4. Australia	**1,227**	**9. Greece**	**514**	**14. Italy**	**384**	**19. Portugal**	**316**
5. Georgia	**1,144**	**10. Philippines**	**511**	**15. Hong Kong**	**371**	**20. Japan**	**311**

[15] Accessibility description: image includes a world map with numbered squares providing total number of complaints 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[16]



TOP 10 STATES BY VICTIM LOSS[17]



[16] Accessibility description: image depicts the United States, with the top ten states (based on number of reporting victims). These include California, Texas, Florida, Washington, Illinois, Pennsylvania, New York, Colorado, Virginia, and Georgia.

[17] Accessibility description: image depicts the United States, with the top ten states (based on reported victim loss). These include California, Texas, Florida, New York, North Carolina, Ohio, Illinois, Michigan, New Jersey, and Massachusetts.

2018 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Non-Payment/Non-Delivery	65,116	Other	10,826
Extortion	51,146	Lottery/Sweepstakes	7,146
Personal Data Breach	50,642	Misrepresentation	5,959
No Lead Value	36,936	Investment	3,693
Phishing/Vishing/Smishing/Pharming	26,379	Malware/Scareware/Virus	2,811
BEC/EAC	20,373	Corporate Data Breach	2,480
Confidence Fraud/Romance	18,493	IPR/Copyright and Counterfeit	2,249
Harassment/Threats of Violence	18,415	Denial of Service/TDoS	1,799
Advanced Fee	16,362	Ransomware	1,493
Identity Theft	16,128	Crimes Against Children	1,394
Spoofing	15,569	Re-shipping	907
Overpayment	15,512	Civil Matter	768
Credit Card Fraud	15,210	Charity	493
Employment	14,979	Health Care Related	337
Tech Support	14,408	Gambling	181
Real Estate/Rental	11,300	Terrorism	120
Government Impersonation	10,978	Hacktivist	77

Descriptors*

Social Media	40,198
Virtual Currency	36,477

*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.

2018 Crime Types *Continued*

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,297,803,489	Tech Support	$38,697,026
Confidence Fraud/Romance	$362,500,761	Harassment/Threats of Violence	$21,903,829
Investment	$252,955,320	Misrepresentation	$20,000,713
Non-Payment/Non-Delivery	$183,826,809	IPR/Copyright and Counterfeit	$15,802,011
Real Estate/Rental	$149,458,114	Civil Matter	$15,172,692
Personal Data Breach	$148,892,403	Malware/Scareware/ Virus	$7,411,651
Corporate Data Breach	$117,711,989	Health Care Related	$4,474,792
Identity Theft	$100,429,691	Ransomware	*$3,621,857
Advanced Fee	$92,271,682	Denial of Service/TDos	$2,052,340
Credit Card Fraud	$88,991,436	Re-Shipping	$1,684,179
Extortion	$83,357,901	Charity	$1,006,379
Spoofing	$70,000,248	Gambling	$926,953
Government Impersonation	$64,211,765	Crimes Against Children	$265,996
Other	$63,126,929	Hacktivist	$77,612
Lottery/Sweepstakes	$60,214,814	Terrorism	$10,193
Overpayment	$53,225,507	No Lead Value	$0.00
Phishing/Vishing/Smishing/Pharming	$48,241,748		
Employment	$45,487,120		

Descriptors*

Social Media	$101,045,973	*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	$182,106,976	

***Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, equipment, or any third party remediation services acquired by a victim. In some cases victims do not report any loss amount to the FBI, thereby creating an artificially low ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.**

2018 OVERALL STATE STATISTICS

Count by Victim per State*

Rank	State	Victims	Rank	State	Victims
1	California	49,031	30	Kentucky	2,813
2	Texas	25,589	31	Oklahoma	2,644
3	Florida	23,984	32	New Mexico	2,127
4	New York	18,124	33	Kansas	2,098
5	Virginia	14,800	34	Iowa	1,983
6	Washington	10,775	35	Mississippi	1,882
7	Pennsylvania	10,554	36	Arkansas	1,849
8	Illinois	10,087	37	Alaska	1,603
9	Colorado	9,328	38	Idaho	1,513
10	Georgia	9,095	39	District of Columbia	1,364
11	Maryland	8,777	40	Nebraska	1,205
12	New Jersey	8,440	41	West Virginia	1,109
13	Arizona	8,027	42	Hawaii	1,100
14	Ohio	7,812	43	New Hampshire	1,056
15	Michigan	7,533	44	Rhode Island	1,028
16	North Carolina	7,523	45	Delaware	897
17	Wisconsin	6,621	46	Maine	832
18	Massachusetts	6,173	47	Montana	787
19	Tennessee	5,584	48	Puerto Rico	704
20	Missouri	5,508	49	Vermont	525
21	Nevada	5,228	50	Wyoming	497
22	Indiana	4,676	51	South Dakota	465
23	Alabama	4,585	52	North Dakota	459
24	Oregon	4,511	53	U.S. Virgin Islands	65
25	Minnesota	4,304	54	Guam	52
26	South Carolina	3,575	55	U.S. Minor Outlying Islands	47
27	Louisiana	3,469	56	American Samoa	16
28	Connecticut	3,134	57	Northern Marina Islands	15
29	Utah	3,041			

***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.**

2018 Overall State Statistics *Continued*

Total Losses by Victim per State*

Rank	State	Loss	Rank	State	Loss
1	California	$450,482,128	30	Louisiana	$16,396,262
2	New York	$201,090,065	31	Iowa	$15,337,975
3	Texas	$195,611,047	32	Oklahoma	$11,587,907
4	Florida	$178,141,470	33	Nebraska	$9,426,684
5	North Carolina	$137,230,988	34	Kentucky	$9,352,781
6	Ohio	$97,730,046	35	District of Columbia	$8,899,830
7	Illinois	$82,849,726	36	New Mexico	$8,617,772
8	Michigan	$80,929,815	37	West Virginia	$8,298,753
9	New Jersey	$79,711,752	38	Arkansas	$6,971,524
10	Massachusetts	$68,242,216	39	Rhode Island	$6,929,001
11	Pennsylvania	$62,692,761	40	Idaho	$6,853,195
12	Georgia	$61,466,974	41	Montana	$6,612,063
13	Washington	$60,513,117	42	Hawaii	$6,460,785
14	Minnesota	$48,814,059	43	New Hampshire	$6,084,633
15	Maryland	$47,180,259	44	Mississippi	$5,725,032
16	Arizona	$45,166,115	45	Puerto Rico	$5,219,087
17	Virginia	$43,792,436	46	Wyoming	$4,517,128
18	Connecticut	$37,859,918	47	Alaska	$3,616,856
19	Colorado	$34,082,849	48	Delaware	$3,141,393
20	Indiana	$29,577,716	49	U.S. Virgin Islands	$2,723,790
21	Nevada	$28,920,936	50	Maine	$2,699,746
22	Oregon	$28,599,963	51	North Dakota	$2,296,789
23	Tennessee	$28,590,404	52	Vermont	$2,127,317
24	Missouri	$25,577,740	53	South Dakota	$1,733,826
25	Wisconsin	$24,649,284	54	Guam	$155,055
26	Utah	$20,617,421	55	U.S. Minor Outlying Islands	$96,346
27	South Carolina	$19,567,920	56	American Samoa	$18,537
28	Kansas	$17,474,768	57	Northern Mariana Islands	$13,865
29	Alabama	$16,911,098			

***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.**

2018 Overall State Statistics *Continued*

Count by Subject per State*

Rank	State	Subjects	Rank	State	Subjects
1	California	15,975	30	Wisconsin	858
2	Texas	10,252	31	District of Columbia	845
3	Florida	9,141	32	Utah	843
4	Virginia	7,569	33	Delaware	825
5	New York	7,352	34	Kentucky	783
6	Maryland	4,279	35	Montana	739
7	Illinois	3,919	36	Mississippi	710
8	New Jersey	3,645	37	Connecticut	624
9	Georgia	3,081	38	Iowa	600
10	Washington	2,819	39	Arkansas	498
11	Pennsylvania	2,601	40	New Mexico	428
12	Michigan	2,309	41	North Dakota	352
13	Ohio	2,258	42	Idaho	348
14	Nevada	2,251	43	Hawaii	300
15	Arizona	2,089	44	Rhode Island	297
16	Tennessee	2,016	45	Alaska	268
17	North Carolina	1,997	46	West Virginia	261
18	Colorado	1,707	47	New Hampshire	242
19	Nebraska	1,653	48	Maine	240
20	Massachusetts	1,485	49	South Dakota	166
21	Missouri	1,375	50	Vermont	140
22	Oregon	1,257	51	Wyoming	140
23	Indiana	1,209	52	Puerto Rico	115
24	South Carolina	1,124	53	U.S. Minor Outlying Islands	16
25	Alabama	1,059	54	U.S. Virgin Islands	15
26	Minnesota	969	55	Guam	4
27	Louisiana	935	56	American Samoa	3
28	Oklahoma	872	57	Northern Mariana Islands	3
29	Kansas	866			

***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.**

2018 Overall State Statistics *Continued*

Subject Earnings per Destination State*

Rank	State	Loss	Rank	State	Loss
1	California	$181,698,326	30	Louisiana	$5,395,827
2	Florida	$93,294,872	31	Hawaii	$4,997,730
3	Maryland	$85,984,642	32	Utah	$4,953,576
4	New York	$84,538,779	33	Alabama	$4,411,596
5	Texas	$79,616,314	34	Wisconsin	$4,171,769
6	Georgia	$45,325,413	35	Iowa	$4,133,227
7	Illinois	$23,843,582	36	Kentucky	$3,995,141
8	New Jersey	$23,499,992	37	Arkansas	$3,687,941
9	Nevada	$23,398,329	38	Puerto Rico	$3,617,864
10	Michigan	$20,486,316	39	Mississippi	$3,562,790
11	Pennsylvania	$19,479,628	40	New Mexico	$3,477,718
12	North Carolina	$17,481,764	41	Delaware	$3,241,823
13	Colorado	$16,371,194	42	Idaho	$3,235,557
14	Virginia	$15,427,366	43	Kansas	$2,489,295
15	Missouri	$14,273,141	44	Montana	$2,090,337
16	Arizona	$13,737,455	45	Wyoming	$2,052,206
17	Washington	$13,587,420	46	Alaska	$1,936,162
18	Tennessee	$11,485,660	47	Rhode Island	$1,668,834
19	Massachusetts	$9,787,562	48	North Dakota	$920,577
20	Indiana	$9,317,973	49	Maine	$772,482
21	Oklahoma	$8,579,862	50	West Virginia	$731,691
22	Ohio	$8,413,509	51	South Dakota	$482,016
23	South Carolina	$7,294,220	52	Vermont	$244,045
24	Connecticut	$7,030,105	53	U.S. Minor Outlying Islands	$23,402
25	District of Columbia	$6,877,801	54	U.S. Virgin Islands	$12,597
26	Minnesota	$6,604,137	55	Guam	$10,613
27	New Hampshire	$5,612,713	56	American Samoa	$7,000
28	Nebraska	$5,475,575	57	Northern Mariana Islands	$0.00
29	Oregon	$5,472,776			

***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

Overpayment: An individual is sent a payment/commission and is instructed to keep a portion of the payment and send the remainder 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.

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 Fraud: 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.

Denial of Service/TDoS: Denial of Service (DoS) Attack floods a network/system or Telephony Denial of Service (TDoS) floods a service with multiple requests, slowing down or interrupting service.

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/Inheritance: An individual is contacted about winning a lottery or sweepstakes they never entered, or to collect on an inheritance from an unknown relative and are asked to pay a tax or fee in order to receive their award.

Malware/Scareware/Virus: Software or code 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.

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.

Spoofing: Contact information (phone number, email, and website) is deliberately falsified to mislead and appear to be from a legitimate source. For example, spoofed phone numbers making mass robo-calls; spoofed emails sending mass spam; forged websites used to mislead and gather personal information. Spoofing is often used in connection with other crime types.

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 cleanup viruses or malware or to facilitate a refund for prior support services.

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

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

APPENDIX B: ADDITIONAL INFORMATION ABOUT IC3 DATA

- Adjusted Losses: each complaint is reviewed by an IC3 analyst. The analyst categorizes the complaint according to the Crime Type(s) that are appropriate. Additionally, the analyst will adjust the loss amount if the complaint data does not support the loss amount reported.
- One complaint may have multiple crime types.
- Some complainants may have filed more than once, creating a possible duplicate.
- All location-based reports are generated from information entered when known/provided by the complainant.
- Losses reported in foreign currencies were converted to U.S. dollars when possible.
- Complaint counts represent the number of individual complaints received from each state and do not represent the number of individuals filing a complaint.