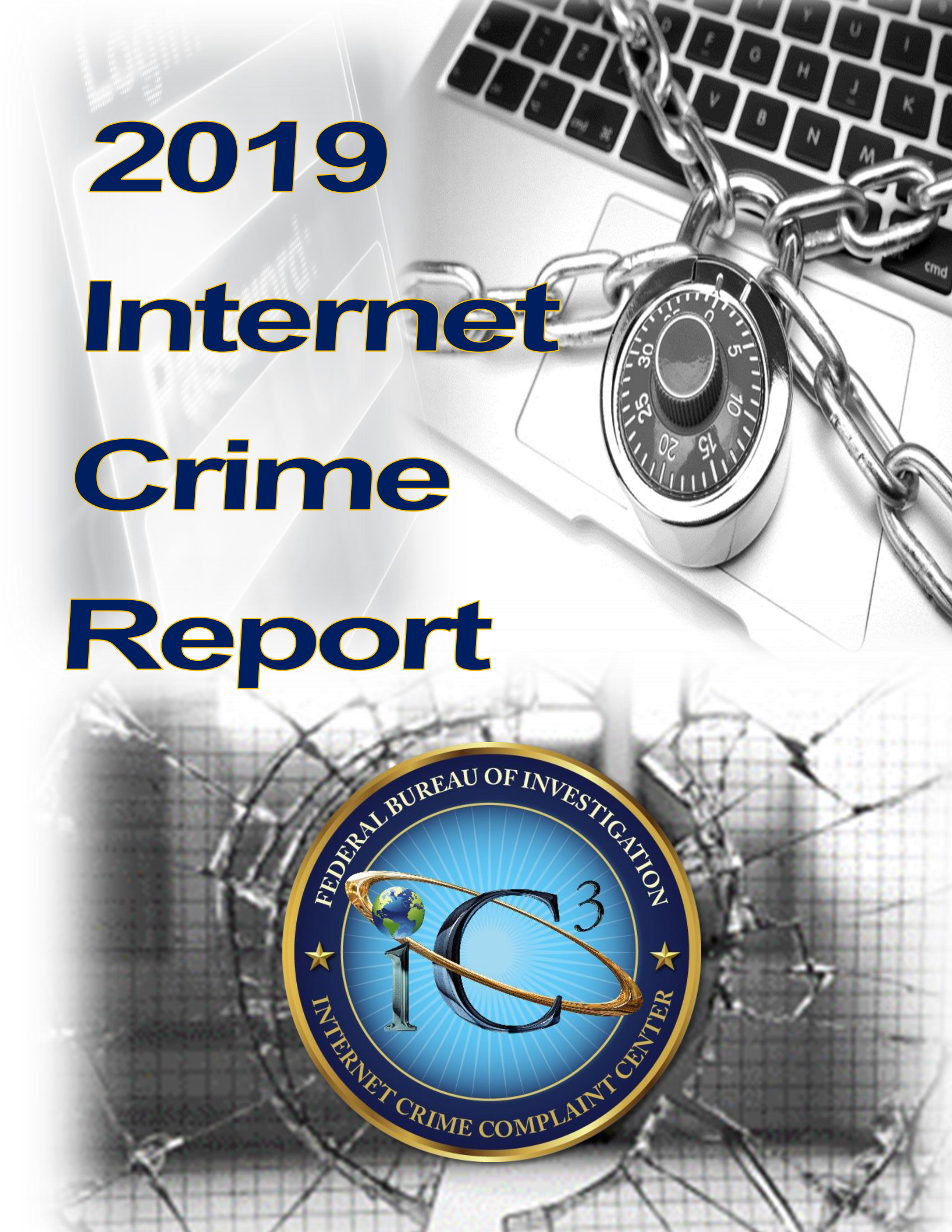
2019 Internet Crime Report



2019 INTERNET CRIME REPORT

TABLE OF CONTENTS

Introduction 3
About the Internet Crime Complaint Center 4
IC3 History 5
The IC3 Role in Combating Cyber Crime 6
IC3 Core Functions 7
Supporting Law Enforcement 8
IC3 Database Remote Access 8
Hot Topics for 2019 9
Business Email Compromise (BEC) 9
IC3 Recovery Asset Team 10
RAT Successes 11
Elder Fraud 12
Tech Support Fraud 13
Ransomware 14
2019 Victims by Age Group 16
2019 - Top 20 International Countries by Victim 17
2019 - Top 10 States by Number of Victims 18
2019 - Top 10 States by Victim Loss 18
2019 Crime Types 19
2019 Overall State Statistics 21
Appendix A: Crime Type Definitions 25
Appendix B: Additional information about IC3 Data 28

INTRODUCTION

Dear Reader,

The FBI is the lead federal agency for investigating malicious cyber activity by criminals, nation-state adversaries, and terrorists. To fulfill this mission, the FBI often develops resources to enhance operations and collaboration. One such resource is the FBI's Internet Crime Complaint Center (IC3) which provides the public with a trustworthy and convenient mechanism for reporting information concerning suspected Internet-facilitated criminal activity. At the end of every year, the IC3 collates information collected into an annual report.

This year's Internet Crime Report highlights the IC3's efforts to monitor trending scams such as Business Email Compromise (BEC), Ransomware, Elder Fraud, and Tech Support Fraud. As the report indicates, in 2019, IC3 received a total of 467,361 complaints with reported losses exceeding $3.5 billion. The most prevalent crime types reported were Phishing/Vishing/Smishing/Pharming, Non-Payment/Non-Delivery, Extortion, and Personal Data Breach. The top three crime types with the highest reported losses were BEC, Confidence/Romance Fraud, and Spoofing. More details on each of these scams can be found in this report.

Of note, the IC3's Recovery Asset Team (RAT), which assists in recovering funds for victims of BEC schemes, celebrated its first full year of operation. During its inaugural year, the team assisted in the recovery of over $300 million lost through on-line scams, boasting a 79% return rate of reported losses. We're also pleased to announce the creation of a Recovery and Investigative Development (RaID) Team which will assist financial and law enforcement investigators in dismantling money mule organizations.

Information reported to the IC3 helps the FBI gain a better understanding of cyber adversaries and the motives behind their activities. Therefore, we encourage everyone to use IC3 and reach out to their local field office to report malicious activity. Cyber is the ultimate team sport. Working together we hope to create a safer, more secure cyber landscape ensuring confidence as we traverse through a digitally-connected world.

We hope this report provides you with 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.

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.

The IC3 Recovery and Investigative Development (RaID) Team was created in 2019. Its goal is to partner with financial and law enforcement investigators in an effort to dismantle money mule organizations. RaID comprises two teams: the Recovery Asset Team (RAT) and the Money Mule Team (MMT). While the RAT is primarily focused on financial recovery, the MMT performs detailed analysis and research on previously unknown targets in an effort to develop new investigations. The teams work together under the RaID umbrella to leverage resources from cyber security experts and financial and law enforcement partners to help address the ever-changing and growing problem of cyber-enabled fraud.

RaID enhances investigations by monitoring new activity and notifying law enforcement of time sensitive situations. The team often plays a significant role in uncovering additional victims and criminals involved in fraudulent activity. RaID works as a liaison between financial and law enforcement investigators to facilitate information sharing necessary to support open case work and assist in any required legal process to stop the flow of fraudulent funds.

RaID has partnered with FBI Field Offices to develop an investigative matrix to triage complaint information provided by IC3 victims. The matrix allows analysts and agents to quickly identify potential targets from the hundreds of IC3 complaints received on a daily basis, and to gain a more complete view of the cyber-enabled fraud threat landscape.

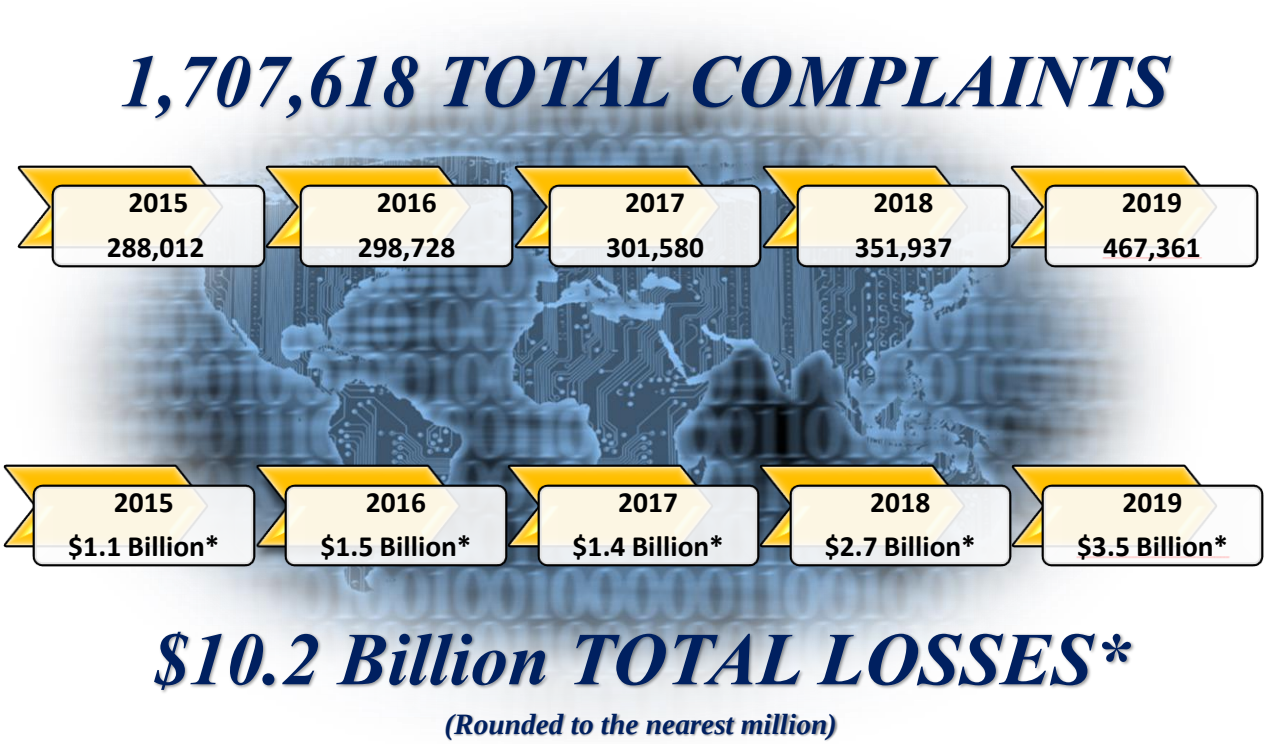
These innovative techniques are leading to successful results, even in investigations that have spanned multiple years. For example, the IC3 provided FBI San Francisco with complaints over three years regarding subjects in one of its cases. The complaints reported incidents of SIM SWAPPING, social engineering, online account takeovers, cryptocurrency theft, online threats, extortion, celebrity account hacking, SWATing and Doxxing. San Francisco ultimately arrested three individuals in connection to these complaints, the most recent being the arrest of a SIM SWAPPING group leader which led to the seizures of over $18 million, five vehicles, a $900,000 home, and hundreds of thousands of dollars in jewelry. The SIM SWAPPING scheme had targeted hundreds of victims, compromised hundreds of cryptocurrency accounts, and caused approximately $40 million in losses.

IC3 HISTORY

In May 2000, the IC3 was established as a center to receive complaints of Internet crime. A total of 4,883,231 complaints have been reported to the IC3 since its inception. Over the last five years, the IC3 has received an average of 340,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.[1]

IC3 Complaint Statistics

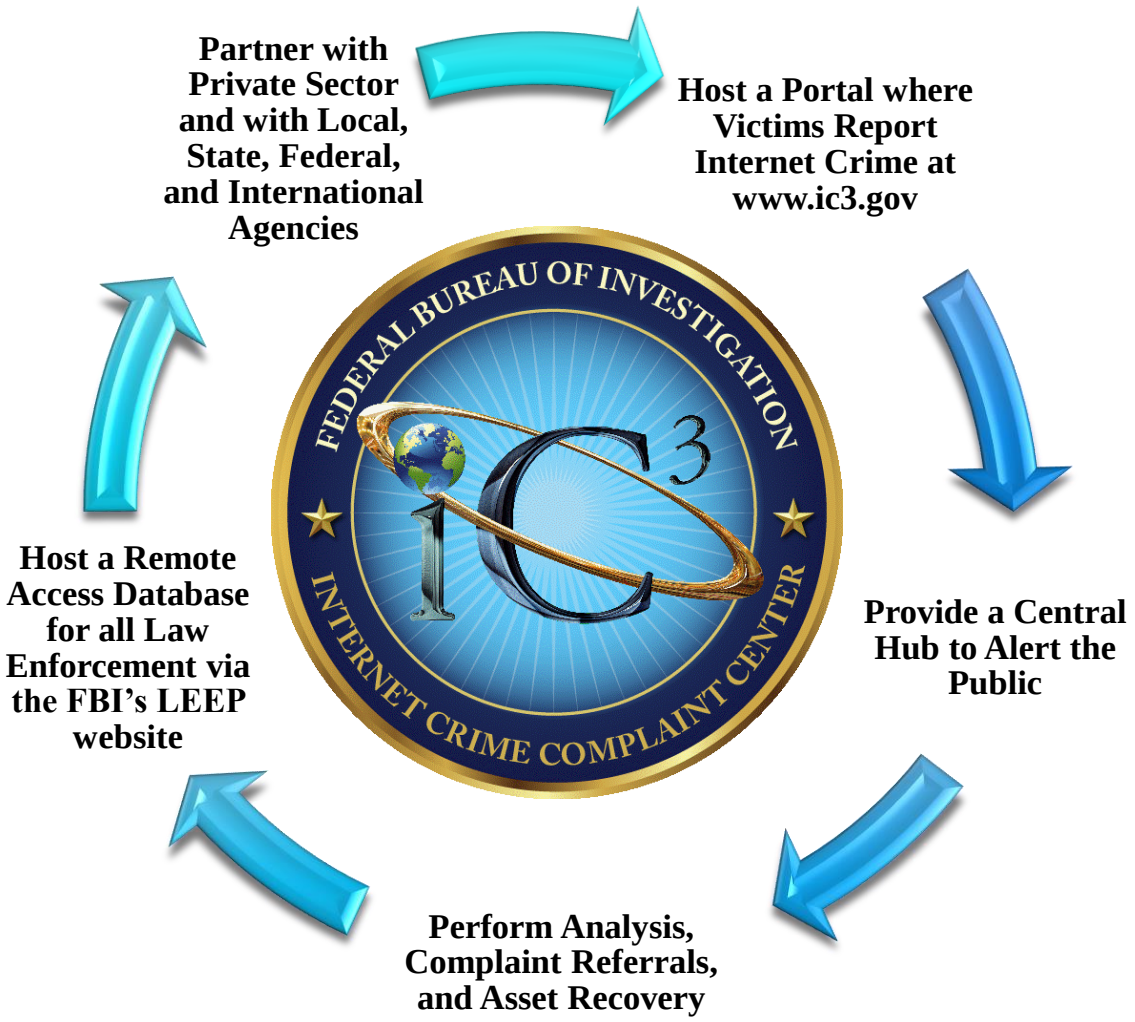
Last Five Years



[1] Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2015 to 2019. Over that time period, IC3 received a total of 1,707,618 complaints, reporting a loss of $10.2 billion.

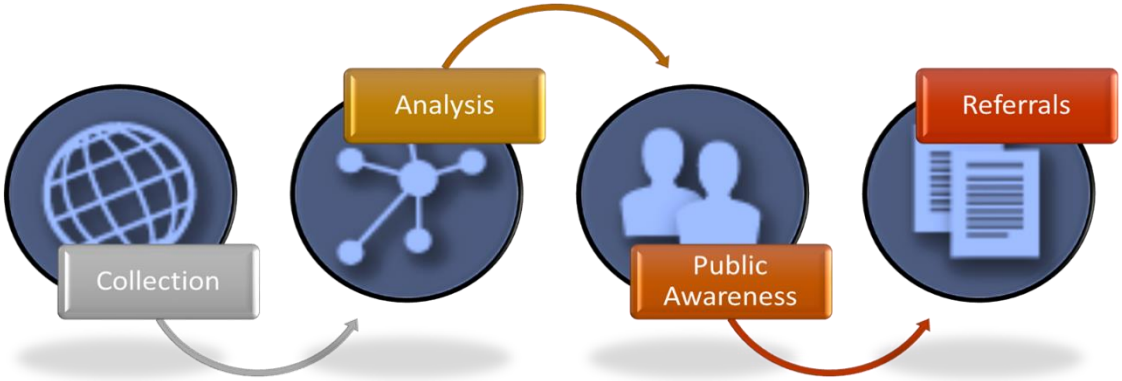
THE IC3 ROLE IN COMBATING CYBER CRIME[2]

WHAT WE DO



[2] Accessibility description: Image lists IC3's primary functions including providing a central hub to alert the public to threats; hosting a victim reporting portal at www.ic3.gov; partnering 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



IC3 Core Functions[3]

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 to identify emerging threats and new trends.	Public service announcements, 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.

[3] Accessibility description: Image contains icons with the core functions. Core functions - Collection, Analysis, Public Awareness, and Referrals - are listed in individual blocks 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 has 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 in 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.

The IC3 routinely provides training to law enforcement regarding the IC3 database and remote query capabilities. Throughout 2019, the IC3 provided three separate training sessions to state and local law enforcement personnel in Providence, Rhode Island; Grand Rapids, Michigan; and Orlando, Florida, which improved their understanding of FBI information available to law enforcement via LEEP.

HOT TOPICS FOR 2019

BUSINESS EMAIL COMPROMISE (BEC)



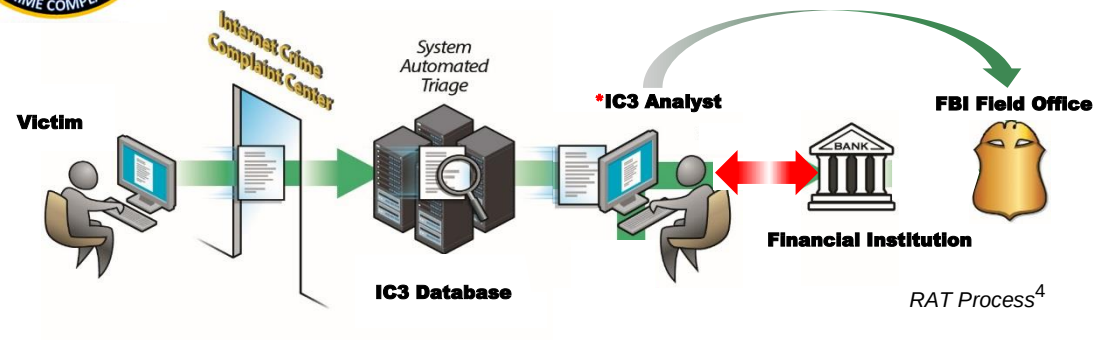
In 2019, the IC3 received 23,775 Business Email Compromise (BEC) / Email Account Compromise (EAC) complaints with adjusted losses of over $1.7 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing a transfer of funds. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

BEC/EAC is 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. Over the years, the scam evolved to include compromise of personal emails, compromise of vendor emails, spoofed lawyer email accounts, requests for W-2 information, the targeting of the real estate sector, and fraudulent requests for large amounts of gift cards.

In 2019, the IC3 observed an increase in the number of BEC/EAC complaints related to the diversion of payroll funds. In this type of scheme, a company's human resources or payroll department receives an email appearing to be from an employee requesting to update their direct deposit information for the current pay period. The new direct deposit information generally routes to a pre-paid card account.

IC3 RECOVERY ASSET TEAM

The 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.



RAT Process[4]

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

Recovery 2019:

Incidents: 1,307

Losses: $384,237,651

Recovery: $304,930,696

Recovery Rate: 79%

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

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.

[4] Accessibility description: Image shows the different stages of a complaint in the RAT process.

RAT SUCCESSES

The IC3 RAT has proven to be a valuable resource for field offices and victims. The following are three examples of the RAT's successful contributions to investigative and recovery efforts.

Dallas

In December 2019, the Dallas Field Office reached out to RAT for assistance on a transfer for a $190,000 BEC incident where the victim wired funds on two separate occasions for invoice payments. The IC3 RAT's quick action, in conjunction with the alliance built with key financial partners, led to the successful recovery of funds. This collaboration between IC3 RAT and their financial partners resulted in the exchange of key information that allowed the IC3 RAT to work in conjunction with the FBI field office to refer the case to local law enforcement. As a result, federal and local law enforcement worked together to ultimately pursue the case, which led to successful prosecution of the perpetrator.

Los Angeles

In November 2019, the IC3 RAT was asked by the Los Angeles Field Office to provide an analytical report that concentrated on elderly victims who fell victim to a variety of scams, including BEC and Romance scams, resulting in the victims transferring funds to possible money mules located in the Los Angeles area of responsibility. The IC3 RAT provided an analytical report that consisted of 19 IC3 complaints and a total loss of over $866,000. As a result of the research and analysis done by the IC3 RAT, the Los Angeles Field Office was able to conduct multiple interviews and disseminate cease and desist letters to the money mules identified.

Fort Lauderdale

In February 2019, the IC3 RAT received a complaint involving a BEC incident for $138,000, where the victim received a spoofed email and wired funds to a fraudulent bank account in Florida. The RAT took quick action and worked with key financial partners to freeze the funds. When the perpetrator attempted to withdraw funds, the RAT's collaboration with financial partners enabled the bank employee to request the perpetrator provide documents to support the receipt of the wire. When the account holder was unable to provide legitimate documentation, the bank alerted local law enforcement and as a result, the account holder was arrested by the Fort Lauderdale Police Department.

ELDER FRAUD



The Elder Abuse Prevention and Prosecution Act was signed into law in October 2017 to prevent elder abuse and exploitation and improve the justice system's response to victims in elder abuse and exploitation cases. As a response to the increasing prevalence of crimes against the elderly, especially Elder Fraud, the Department of Justice and the FBI partnered to create the Elder Justice Initiative. Elder Fraud is defined as a financial fraud scheme which targets or disproportionately affects people over the age of 60. The FBI, including IC3, has worked tirelessly to educate this population on how to take steps to protect themselves from being victimized. In 2019, the IC3 released PSAs to educate the public about Romance Fraud, common Elder Fraud schemes, and money mule activity. The FBI has held hundreds of outreach events in order to educate the public about Elder Fraud.

The Department of Justice Consumer Protection Branch (DOJ-CPB) and the FBI have also partnered to pursue fraudsters and facilitators of schemes who target the elderly. In March 2019, the FBI and other federal law enforcement partners undertook an Elder Fraud and Tech Support Fraud sweep, targeting over 260 defendants who had allegedly defrauded over 2 million U.S. victims of more than $750 million. DOJ-CPB and the FBI also target money mules who serve as the witting or unwitting facilitators of laundering proceeds from Elder Fraud schemes.

In 2019, the IC3 received 68,013 complaints from victims over the age of 60 with adjusted losses in excess of $835 million. Age is not a required reporting field. These statistics reflect only those complaints in which the victim voluntarily provided their age range as "OVER 60." Victims over the age of 60 are targeted by perpetrators because they are believed to have significant financial resources.

Victims over the age of 60 may encounter scams including Advance Fee Schemes, Investment Fraud Schemes, Romance Scams, Tech Support Scams, Grandparent Scams, Government Impersonation Scams, Sweepstakes/Charity/Lottery Scams, Home Repair Scams, TV/Radio Scams, and Family/Caregiver Scams. If the perpetrators are successful after initial contact, they will often continue to victimize these individuals. Further information about the Elder Justice Initiative is available at https://www.justice.gov/elderjustice.

TECH SUPPORT FRAUD



Tech Support Fraud continues to be a growing problem. This scheme involves a criminal claiming to provide customer, security, or technical support or service in an effort to defraud unwitting individuals. Criminals may pose as support or service representatives offering to resolve such issues as a compromised e-mail or bank account, a virus on a computer, or a software license renewal. Some recent complaints involve criminals posing as customer support for well-known travel industry companies, financial institutions, or virtual currency exchanges.

In 2019, the IC3 received 13,633 complaints related to Tech Support Fraud from victims in 48 countries. The losses amounted to over $54 million, which represents a 40 percent increase in losses from 2018. 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 PSA on the IC3 website: https://www.ic3.gov/media/2018/180328.aspx.

Investigative efforts have yielded many successes, including the two examples below.

Charlotte

A North Carolina man pleaded guilty to conspiracy to access a protected computer, for his role in an international tech support scam that defrauded hundreds of victims, including seniors, of more than $3 million. The subject was part of a conspiracy that carried out the scam by placing fake pop-up ads on victims' computers to convince them they had a serious computer problem, and to induce them to pay for purported "technical support" services to resolve the issue. The IC3 provided ongoing assistance to the Charlotte Field Office and the prosecuting attorneys in this case.

Philadelphia

A Pennsylvania man pleaded guilty to wire fraud and was sentenced to 15 months imprisonment to be followed by two years of supervised release. The subject admitted to perpetrating a computer-based fraud scheme that targeted victims across the United States. As part of the scheme, the subject and others pretended to work for technology companies and contacted victims through computer pop-ups and telephone calls. Once contact was made, the subject and others induced victims to authorize payments under false pretenses and utilized remote desktop access applications to initiate unauthorized financial transactions from the victims' financial accounts. The IC3 provided ongoing assistance to the Philadelphia Field Office for this case.

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 that result in the rapid encryption of sensitive files on a corporate network. When the victim organization determines it is no longer able to access its data, the cyber actor demands the payment of a ransom, typically in virtual currency. The actor will purportedly provide an avenue to the victim to regain access to its data once the ransom is paid.

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

The FBI advises not to pay the ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to its 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 a lucrative environment for other criminals. 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.

The decision to pay the ransom should not dissuade someone from contacting the FBI. In all cases the FBI encourages organizations to contact a local FBI field office immediately to report a ransomware event and request assistance.

In 2019, the IC3 received 2,047 complaints identified as ransomware with adjusted losses of over $8.9 million.

IC3 by the Numbers[5]

Over 1,200

Complaints Received Per Day on Average

4,883,231

# of Complaints Reported Since Inception (‘00)



$3.5 Billion

Victim Losses in **2019**

Over 340,000

Complaints Received Per Year on Average
(Over Last 5 Years)

[5] Accessibility description: Image depicts key statistics regarding complaints and victim loss. Total losses of $3.5 billion were reported in 2019. The total number of complaints received since the year 2000 is 4,883,231. IC3 has received approximately 340,000 complaints per year on average over the last five years, or more than 1,200 complaints per day.

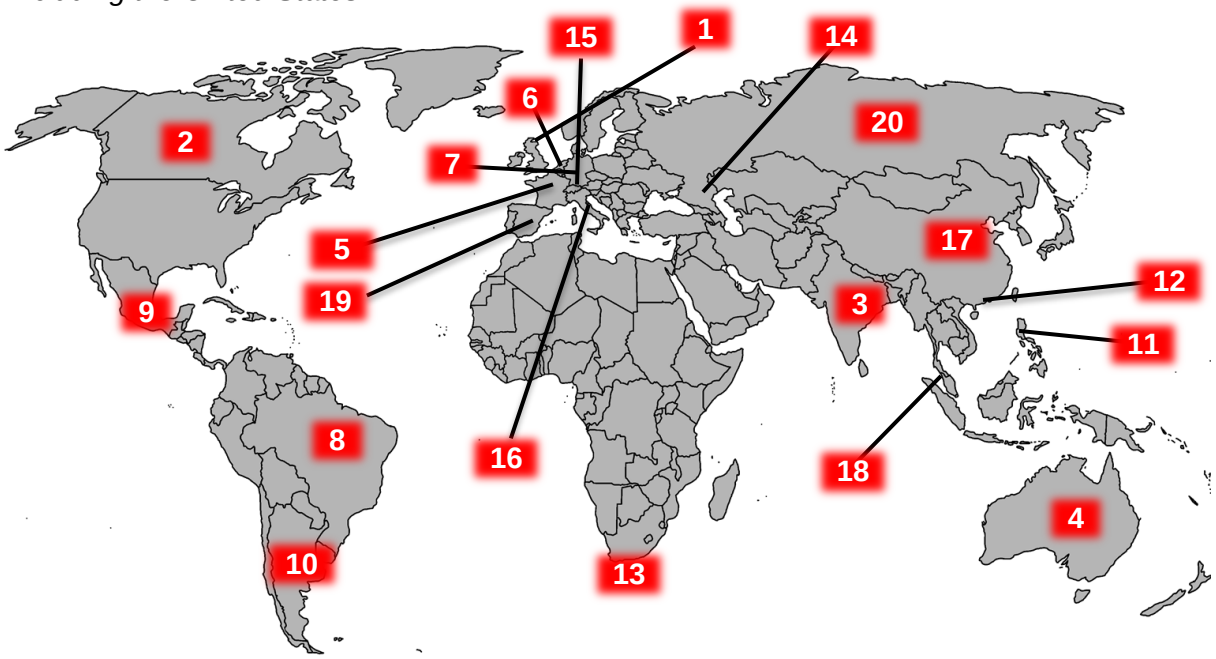
2019 VICTIMS BY AGE GROUP

Victims		
Age Range[6]	**Total Count**	**Total Loss**
Under 20	10,724	$421,169,232
20 - 29	44,496	$174,673,470
30 - 39	52,820	$332,208,189
40 - 49	51,864	$529,231,267
50 - 59	50,608	$589,624,844
Over 60	68,013	$835,164,766

[6] Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix B for more information regarding IC3 data.

2019 - TOP 20 INTERNATIONAL VICTIM COUNTRIES

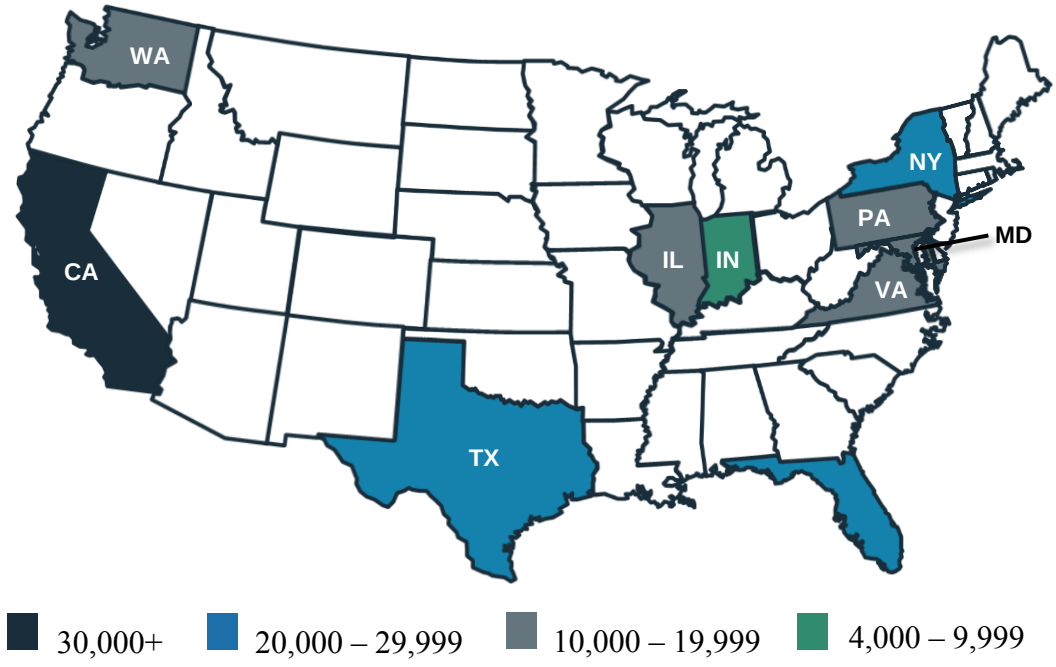
Excluding the United States[7]



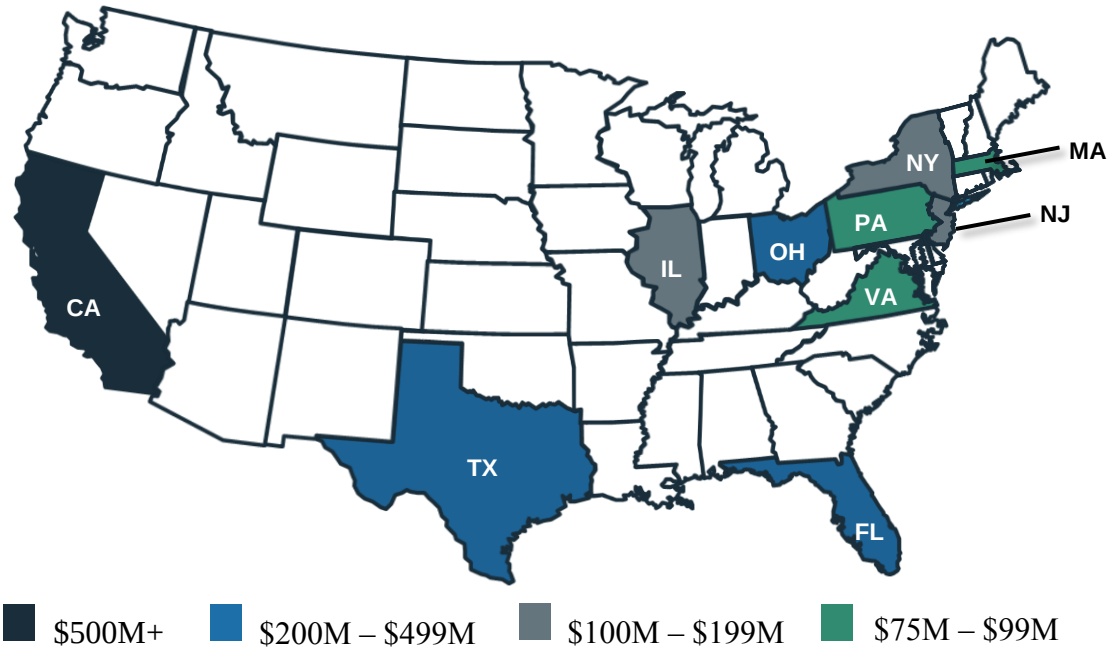
1. United Kingdom	**93,796**	**6. Belgium**	**1,031**	**11. Philippines**	**561**	**16. Italy**	**428**
2. Canada	**3,721**	**7. Germany**	**850**	**12. Hong Kong**	**535**	**17. China**	**403**
3. India	**2,901**	**8. Brazil**	**628**	**13. South Africa**	**465**	**18. Malaysia**	**362**
4. Australia	**1,298**	**9. Mexico**	**605**	**14. Georgia**	**454**	**19. Spain**	**358**
5. France	**1,243**	**10. Argentina**	**578**	**15. Switzerland**	**438**	**20. Russian Federation**	**349**

[7] Accessibility description: Image includes a world map with labels indicating the top 20 countries by number of total victims. The specific number of victims for each country are listed in descending order in the text table immediately below the image. Please see Appendix B for more information regarding IC3 data.

2019 - TOP 10 STATES BY NUMBER OF VICTIMS[8]



2019 - TOP 10 STATES BY VICTIM LOSS[9]



[8] Accessibility description: Image depicts a map of the United States. The top 10 states based on number of reporting victims are labeled. These include California, Texas, Florida, New York, Washington, Pennsylvania, Virginia, Illinois, Maryland, and Indiana. Please see Appendix B for more information regarding IC3 data.
[9] Accessibility description: Image depicts a map of the United States. The top 10 states based on reported victim loss are labeled. These include California, Texas, Florida, Ohio, New Jersey, Illinois, New York, Pennsylvania, Virginia, and Massachusetts. Please see Appendix B for more information regarding IC3 data.

2019 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	114,702	Lottery/Sweepstakes/Inheritance	7,767
Non-Payment/Non-Delivery	61,832	Misrepresentation	5,975
Extortion	43,101	Investment	3,999
Personal Data Breach	38,218	IPR/Copyright and Counterfeit	3,892
Spoofing	25,789	Malware/Scareware/Virus	2,373
BEC/EAC	23,775	Ransomware	2,047
Confidence Fraud/Romance	19,473	Corporate Data Breach	1,795
Identity Theft	16,053	Denial of Service/TDoS	1,353
Harassment/Threats of Violence	15,502	Crimes Against Children	1,312
Overpayment	15,395	Re-shipping	929
Advanced Fee	14,607	Civil Matter	908
Employment	14,493	Health Care Related	657
Credit Card Fraud	14,378	Charity	407
Government Impersonation	13,873	Gambling	262
Tech Support	13,633	Terrorism	61
Real Estate/Rental	11,677	Hacktivist	39
Other	10,842		

Descriptors*

Social Media	29,093
Virtual Currency	29,313

*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 as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

2019 Crime Types *Continued*

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

Descriptors*

Social Media	$78,775,408	*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. Please see Appendix B for more information regarding IC3 data.
Virtual Currency	$159,329,101	

**** Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or 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 overall 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.**

2019 OVERALL STATE STATISTICS

Count by Victim per State*

Rank	State	Victims	Rank	State	Victims
1	California	50,132	30	Utah	3,304
2	Florida	27,178	31	Kentucky	3,083
3	Texas	27,178	32	Oklahoma	2,887
4	New York	21,371	33	New Mexico	2,037
5	Washington	13,095	34	Arkansas	1,991
6	Maryland	11,709	35	Kansas	1,970
7	Virginia	11,674	36	Mississippi	1,654
8	Pennsylvania	10,914	37	Idaho	1,485
9	Illinois	10,337	38	Alaska	1,451
10	Indiana	9,746	39	District of Columbia	1,407
11	Colorado	9,689	40	Hawaii	1,396
12	Ohio	9,321	41	Nebraska	1,350
13	Georgia	9,074	42	West Virginia	1,227
14	New Jersey	9,067	43	New Hampshire	1,155
15	Michigan	8,249	44	Delaware	1,062
16	North Carolina	8,223	45	Rhode Island	1,011
17	Arizona	7,795	46	Montana	967
18	Massachusetts	6,492	47	Maine	880
19	Nevada	6,381	48	Puerto Rico	839
20	Wisconsin	6,378	49	Wyoming	550
21	Tennessee	5,586	50	Vermont	500
22	Iowa	5,094	51	North Dakota	489
23	Missouri	5,083	52	South Dakota	473
24	Oregon	4,813	53	U.S. Virgin Islands	75
25	South Carolina	4,541	54	Guam	71
26	Connecticut	4,412	55	U.S. Minor Outlying Islands	46
27	Minnesota	4,388	56	American Samoa	23
28	Alabama	4,108	57	Northern Marina Islands	11
29	Louisiana	3,804			

***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. Please see Appendix B for more information regarding IC3 data.**

2019 Overall State Statistics *Continued*

Total Losses by Victim per State*

Rank	State	Loss	Rank	State	Loss
1	California	$573,624,151	30	Wisconsin	$21,576,109
2	Florida	$293,445,963	31	Alabama	$20,586,392
3	Ohio	$264,663,456	32	South Carolina	$20,186,041
4	Texas	$221,535,479	33	New Mexico	$17,983,833
5	New York	$198,765,769	34	Kentucky	$17,014,895
6	Illinois	$107,152,415	35	Kansas	$16,107,619
7	New Jersey	$106,474,464	36	Nebraska	$14,596,769
8	Pennsylvania	$94,281,611	37	Idaho	$12,627,102
9	Virginia	$92,467,791	38	District of Columbia	$12,175,460
10	Massachusetts	$84,173,754	39	Rhode Island	$10,182,363
11	Georgia	$79,732,460	40	Mississippi	$10,129,650
12	Washington	$71,286,037	41	Hawaii	$10,005,566
13	Colorado	$65,118,524	42	Alaska	$9,654,238
14	Maryland	$52,830,779	43	Montana	$8,295,010
15	North Carolina	$48,425,764	44	Wyoming	$8,138,463
16	Michigan	$47,122,182	45	Puerto Rico	$7,668,517
17	Arizona	$47,058,842	46	New Hampshire	$7,284,552
18	Utah	$46,458,273	47	Delaware	$6,105,401
19	Minnesota	$39,421,520	48	West Virginia	$5,442,899
20	Oregon	$37,088,022	49	North Dakota	$4,527,733
21	Nevada	$35,720,611	50	Maine	$3,267,370
22	Connecticut	$33,789,138	51	South Dakota	$3,086,846
23	Tennessee	$33,052,233	52	Vermont	$2,329,973
24	Oklahoma	$28,556,326	53	U.S. Virgin Islands	$2,113,723
25	Iowa	$27,919,567	54	Guam	$898,265
26	Missouri	$27,290,803	55	U.S. Minor Outlying Islands	$143,012
27	Louisiana	$24,214,439	56	American Samoa	$16,359
28	Indiana	$24,030,998	57	Northern Mariana Islands	$2,300
29	Arkansas	$22,681,002			

***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. Please see Appendix B for more information regarding IC3 data.**

2019 Overall State Statistics *Continued*

Count by Subject per State*

Rank	State	Subjects	Rank	State	Subjects
1	California	17,517	30	New Mexico	943
2	Florida	11,047	31	Oklahoma	940
3	Texas	10,093	32	Utah	934
4	New York	8,345	33	Wisconsin	933
5	Maryland	7,228	34	Connecticut	846
6	Virginia	4,829	35	Montana	832
7	Illinois	3,465	36	Kentucky	789
8	Georgia	3,325	37	District of Columbia	779
9	Washington	3,317	38	Mississippi	748
10	New Jersey	3,312	39	Iowa	612
11	Pennsylvania	2,793	40	Hawaii	547
12	Ohio	2,506	41	Arkansas	532
13	Nevada	2,481	42	Puerto Rico	476
14	North Carolina	2,259	43	Idaho	432
15	Tennessee	2,186	44	North Dakota	377
16	Arizona	2,119	45	Maine	312
17	Michigan	2,029	46	New Hampshire	264
18	Indiana	1,933	47	West Virginia	262
19	Colorado	1,848	48	Rhode Island	241
20	Massachusetts	1,480	49	Alaska	222
21	Missouri	1,376	50	Wyoming	175
22	Minnesota	1,276	51	South Dakota	133
23	Oregon	1,240	52	Vermont	131
24	Nebraska	1,201	53	U.S. Minor Outlying Islands	19
25	South Carolina	1,137	54	U.S. Virgin Islands	12
26	Louisiana	1,103	55	Guam	11
27	Alabama	1,049	56	American Samoa	7
28	Kansas	976	57	Northern Mariana Islands	1
29	Delaware	948			

***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. Please see Appendix B for more information regarding IC3 data.**

2019 Overall State Statistics *Continued*

Subject Earnings per Destination State*

Rank	State	Loss	Rank	State	Loss
1	Indiana	$231,002,496	30	Utah	$7,912,016
2	California	$183,168,069	31	Missouri	$6,432,347
3	Texas	$126,282,907	32	Idaho	$5,892,792
4	New York	$95,996,214	33	Iowa	$5,763,972
5	Florida	$95,910,080	34	Louisiana	$4,958,777
6	Georgia	$55,338,192	35	Hawaii	$4,761,209
7	Illinois	$48,100,395	36	Kentucky	$4,704,251
8	New Jersey	$32,048,215	37	New Hampshire	$3,520,598
9	Washington	$31,928,985	38	Montana	$3,235,197
10	Pennsylvania	$29,787,276	39	Arkansas	$3,206,417
11	Arizona	$25,960,706	40	West Virginia	$2,754,324
12	Virginia	$24,879,452	41	Nebraska	$2,614,627
13	Maryland	$23,977,444	42	Delaware	$2,548,620
14	Massachusetts	$20,192,012	43	Mississippi	$2,518,412
15	Connecticut	$17,845,526	44	Rhode Island	$2,105,153
16	Colorado	$16,678,494	45	New Mexico	$1,889,690
17	Tennessee	$15,532,247	46	Maine	$1,656,784
18	Ohio	$14,569,674	47	Wyoming	$1,547,198
19	North Carolina	$13,983,462	48	North Dakota	$1,452,038
20	Nevada	$13,497,823	49	Alaska	$1,431,485
21	Michigan	$13,466,196	50	South Dakota	$975,629
22	Oklahoma	$12,082,341	51	Puerto Rico	$852,121
23	Minnesota	$11,518,980	52	Vermont	$686,424
24	Wisconsin	$10,722,858	53	U.S. Minor Outlying Islands	$77,491
25	Oregon	$9,325,763	54	U.S. Virgin Islands	$27,748
26	Kansas	$8,954,238	55	Guam	$15,014
27	South Carolina	$8,454,695	56	American Samoa	$12,100
28	District of Columbia	$8,280,731	57	Northern Mariana Islands	$0.00
29	Alabama	$7,988,933			

***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. Please see Appendix B for more information regarding IC3 data.**

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

Employment: Individuals believe they are legitimately employed, and lose 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, or 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, 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: A 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: Individuals are 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.

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.

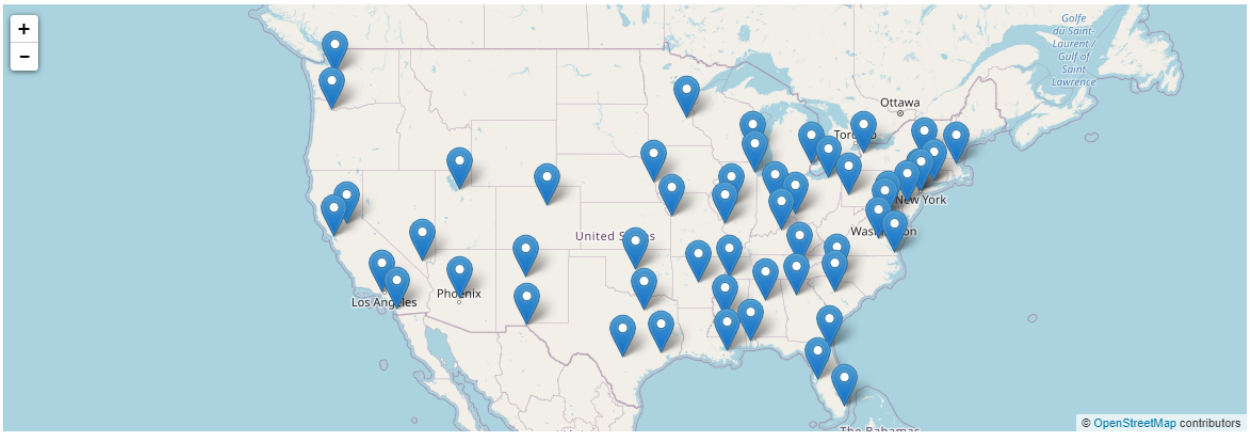
Virtual Currency: A complaint mentioning a form of virtual cryptocurrency, such as Bitcoin, Litecoin, or Potcoin.

APPENDIX B: ADDITIONAL INFORMATION ABOUT IC3 DATA

- 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 complaint.
- All location-based reports are generated from information entered when known/provided by the complainant.
- Losses reported in foreign currencies are 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.

Field Offices | FBI Headquarters | Overseas Offices

Field Offices



Our local FBI offices are all about protecting your communities.

Jacksonville

6061 Gate Parkway
Jacksonville, FL 32256
jacksonville.fbi.gov
(904) 248-7000

Covers 40 counties throughout northern Florida

Miami

2030 SW 145th Avenue
Miramar, FL 33027
miami.fbi.gov
(754) 703-2000

Covers nine counties in southern Florida and responsible for addressing extraterritorial violations of American citizens in Mexico, the Caribbean, and Central and South America

Tampa

5525 West Gray Street
Tampa, FL 33609
tampa.fbi.gov
(813) 253-1000

Covers 18 counties in central and southwest Florida

Financial Fraud Kill Chain

Federal Bureau of Investigation
11 January 2016

Criminal actors are laundering billions of dollars overseas through financial fraud schemes like corporate account takeovers, business e-mail compromise scams, and other financially motivated crimes. The Financial Fraud Kill Chain (FFKC) is a process for recovering large international wire transfers stolen from US victim bank accounts. The FFKC utilizes FINCEN's relationship with the Egmont group, as well as federal law enforcement placement in countries all over the world to help stop the successful withdraw of cyber crime funds by criminal actors.

The FFKC is intended to be utilized as another potential avenue for US financial institutions to get victim funds returned. Normal bank procedures to recover fraudulent funds should also be conducted.

The FFKC can only be implemented if the fraudulent wire transfer meets the following criteria:

- the wire transfer is $50,000 or above;
- the wire transfer is international;
- a SWIFT recall notice has been initiated; and
- the wire transfer has occurred within the last 72 hours.

Any wire transfers that occur outside of these thresholds should still be reported to law enforcement but the FFKC cannot be utilized to return the fraudulent funds.

In order to initiate the FFKC, banks must provide the following information to their local FBI office.

Summary of the Incident:
Victim Name:
Victim Location (City, State):
Originating Bank Name:
Originating Bank Account Number:
Beneficiary Name:
Beneficiary Bank:
Beneficiary Account Number:
Beneficiary Bank Location (if available):
Intermediary Bank Name (if available):
SWIFT Number:
Date:
Amount of Transaction:
Additional Information (if available) - including "FFC"- For Further Credit; "FAV" – In Favor Of:

If the fraudulent funds are returned to the victim's account, the FBI requests that this information be passed back to their local field office contact.



JACKSONVILLE, FL
904.296.0133

MIAMI
305.863.5000

ORLANDO
407.648.6333

TAMPA
813.228.2636

Fraud Notification Procedure

PURPOSE: FLTA has established the following procedures for reporting suspected or detected fraud schemes and attacks. Along with how to document the results to help our industry recognize and avoid similar issues in the future.

PROCEDURES: The following steps are suggested when a fraudulent scheme or deceptive act has been detected.

Step 1. Report to I.T./Support Team: Notify your IT Professional Team immediately.

Step 2. Create a Fraud File: Collect all relevant documentation concerning the event in one file kept in a secure location.

- Timeline of events and, if applicable, any notes you feel may be relevant.
- Any evidence of the fraud or deception (i.e. emails, wire instructions, etc.)
- Any other relevant documentation concerning the fraud.
- All relevant contact information

Step 3. Notify Banks: Call Banks for any accounts that were opened or used in connection with the scheme. Work with Bank to have account shut down and account holder's Tax ID number reported to Financial Crimes Enforcement Network (FinCen).

Contact the sending bank's fraud department and request that a recall of the wire be sent to the receiving bank because of fraud. Provide the details for the wire.

- Ask the sending bank to initiate the FBI's Financial Fraud Kill Chain if the amount of the wire transfer is $50,000 or above; the wire transfer is international; a SWIFT recall notice has been initiated; and the wire transfer has occurred within the last 72 hours.
- Also call the receiving bank's fraud department to notify them that you have requested a recall of the wire because of fraud. Provide the details for the wire and request that the account be frozen.
- If a client or consumer was a victim and your bank/accounts were not directly involved, your client or customer will need to contact the bank themselves but you may have helpful information to share, too. Coordinate quickly!

Step 4. Report to the Appropriate Federal Agencies:

- Local Police/Sheriff: https://www.policeone.com/law-enforcement-directory/
- FBI Field Office: https://www.fbi.gov/contact-us/field-offices
- Secret Service: https://www.secretservice.gov/contact/field-offices/

Step 5. Inform the parties to the transaction: Notify buyer, seller, real estate agents, broker, attorneys, underwriter, notary, etc.) using known, trusted, phone numbers for verbal verification.

Step 6. Review your Incident Response Plan to determine if you need to update passwords, secure hardware, and review email logs to determine how and when email accounts were accessed.

Step 7. Notify Registrar of Domain. If a Spoofed Email is being used in connection with the scheme, contact the registrar who manages the registration of that domain name and report the abuse. Search https://whois.net/ to locate Registrar.

Step 8. Consider contacting your insurance carrier(s) and outside legal counsel.

Step 9. If funds were wired out of the U.S., hire an attorney in that country to help recover funds.

Step 10. Document your response using a Response Worksheet.

- Customize this ALTA Rapid Response Plan for Wire Fraud Incidents
- Customize a Response Worksheet (available in Excel or PDF)
- Assign each step to an appropriate person/entity
- Track progress through to completion or resolution
- Retain the Response Worksheet in your Fraud file for future reference/update

Step 11. File a complaint with the FBI's Internet Crime Complaint Center (IC3). Visit www.ic3.gov and provide the following information:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- For Business Email Compromise (BEC) events, copy email header(s) – Learn how
- Any other relevant information that is necessary to support the claimant