INTERNET CRIME REPORT

2020

2020 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 7
IC3 Core Functions 8
Hot Topics for 2020 9
Business Email Compromise (BEC) 10
IC3 Recovery Asset Team (RAT) 11
RAT Successes 12
Tech Support Fraud 13
Ransomware 14
2020 Victims by Age Group 16
2020 - Top 20 International Victim Countries 17
2020 - Top 10 States by Number of Victims 18
2020 - Top 10 States by Victim Loss 18
2020 Crime Types 19
Last 3 Year Complaint Count Comparison 21
2020 Overall State Statistics 23
Appendix A: Definitions 27
Appendix B: Additional information about IC3 Data 30

INTRODUCTION

Dear Reader,

In 2020, while the American public was focused on protecting our families from a global pandemic and helping others in need, cyber criminals took advantage of an opportunity to profit from our dependence on technology to go on an Internet crime spree. These criminals used phishing, spoofing, extortion, and various types of Internet-enabled fraud to target the most vulnerable in our society - medical workers searching for personal protective equipment, families looking for information about stimulus checks to help pay bills, and many others.

Crimes of this type are just a small part of what the FBI combats through our criminal and cyber investigative work. Key to our cyber mission is the Internet Crime Complaint Center (IC3), which provides the public with a trustworthy source for information on cyber criminal activity, and a way for the public to report directly to us when they suspect they are a victim of cyber crime.

IC3 received a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019. Business E-mail Compromise (BEC) schemes continued to be the costliest: 19,369 complaints with an adjusted loss of approximately $1.8 billion. Phishing scams were also prominent: 241,342 complaints, with adjusted losses of over $54 million. The number of ransomware incidents also continues to rise, with 2,474 incidents reported in 2020.

Public reporting is central to the mission and success of IC3. Submitting a cyber crime complaint to IC3.gov not only helps the FBI address specific complaints—and provide support and assistance to victims —but also helps us prevent additional crimes by finding and holding criminal actors accountable. Information reported to the IC3 helps the FBI better understand the motives of cyber-criminals, the evolving threat posed, and tactics utilized, enabling us to most effectively work with partners to mitigate the damage to victims.

IC3 has continued to strengthen its relationships with industry and others in the law enforcement community to reduce financial losses resulting from BEC scams. Through the Recovery Asset Team, IC3 worked with its partners to successfully freeze approximately $380 million of the $462 million in reported losses in 2020, representing a success rate of nearly 82%. In addition, IC3 has a Recovery and Investigative Development Team which assists financial and law enforcement investigators in dismantling organizations that move and transfer funds obtained illicitly.

With our dedicated resources focused on recovering funds and preventing further victimization, we are better aligned to confront the unique challenges faced in cyberspace. Visit IC3.gov to access the latest information on criminal Internet activity.

We strongly encourage readers to submit complaints to IC3 and to reach out to their local FBI field office to report malicious cyber criminal activity. Together we will continue to build safety, security, and confidence into our digitally connected world.

Paul Abbate
Deputy Director
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.

As a response to the increasing prevalence of fraud against the elderly, 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 2020, the IC3 received 105,301 complaints from victims over the age of 60 with total losses in excess of $966 million. Since, age is not a required reporting field, these statistics only reflect 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.

As a result of the significant increases and impact of scams targeting the elderly, IC3 is planning to release its first annual report focusing entirely on Elder Fraud in 2021.

IC3 History

In May 2000, the IC3 was established as a center to receive complaints of Internet crime. A total of 5,679,259 complaints have been reported to the IC3 since its inception. Over the last five years, the IC3 has received an average of 440,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.[1]

IC3 Complaint Statistics

Last Five Years

2,211,396 TOTAL COMPLAINTS

*$13.3 Billion TOTAL LOSSES**

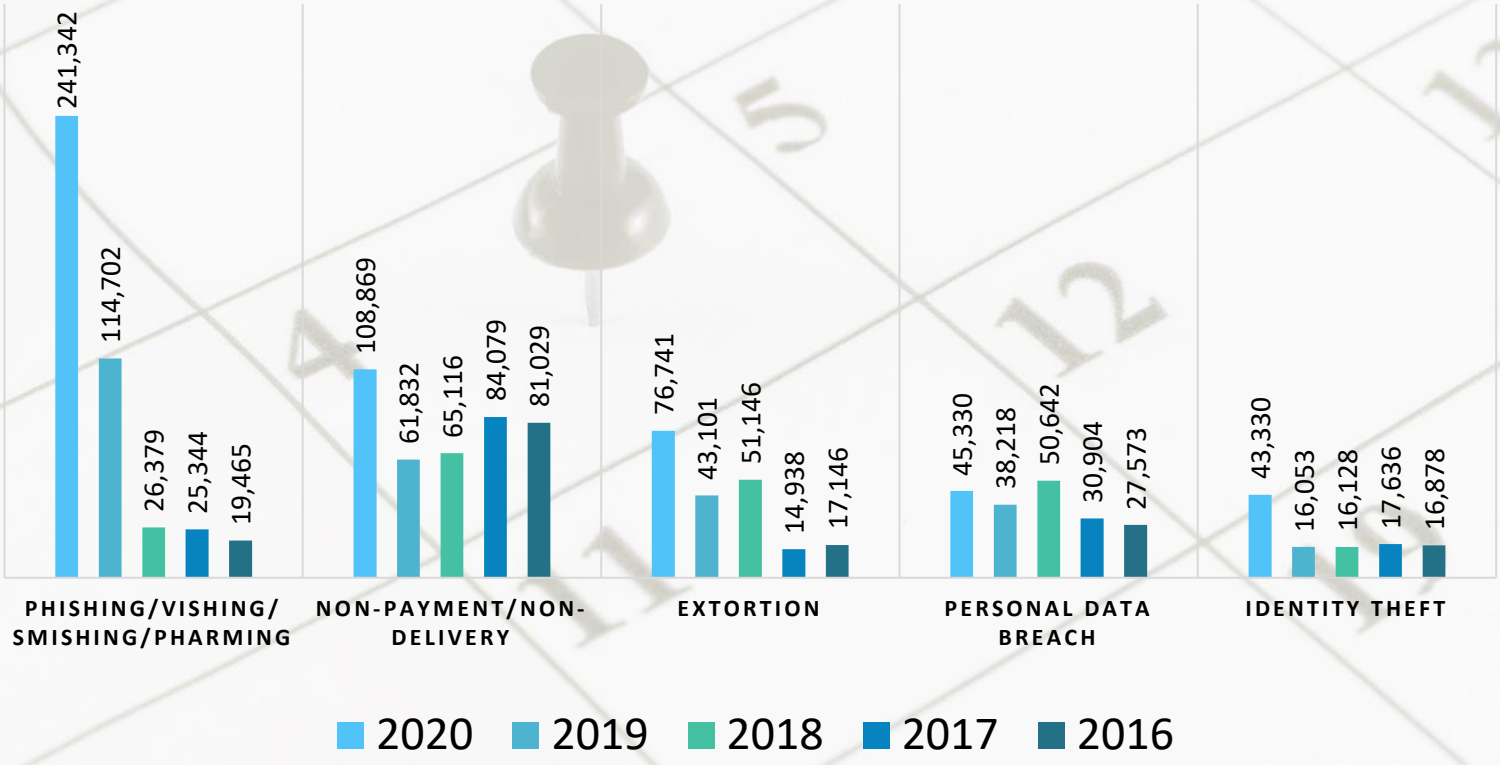
(Rounded to the nearest million)

[1] Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2016 to 2020. Over that time, IC3 received a total of 2,211,396 complaints, reporting a loss of $13.3 billion.

IC3 Complaint Statistics[2]

2020 - Top 5 Crime Type Comparison

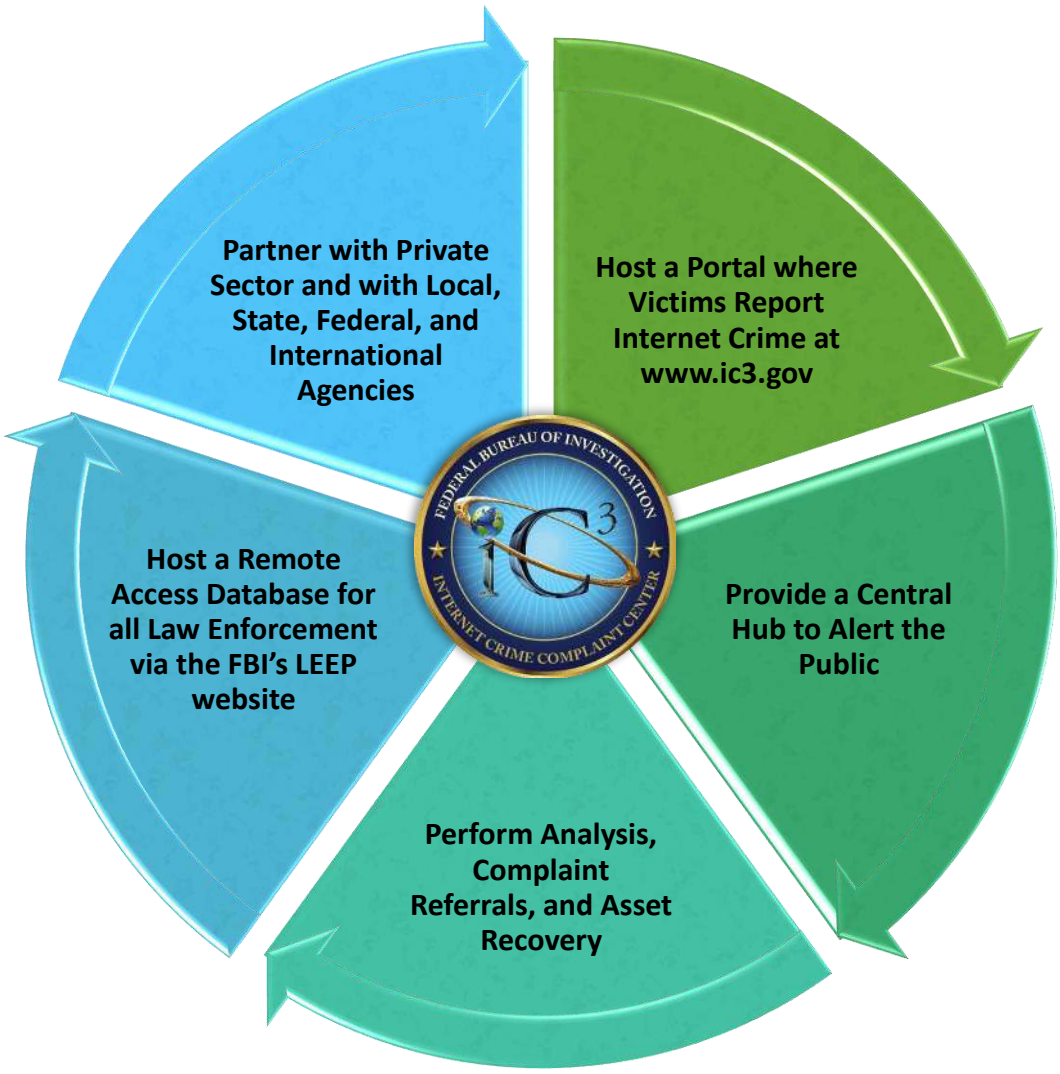
Last Five Years



[2] Accessibility description: Image includes a victim loss comparison for the top five reported crime types of 2020 for the years of 2016 to 2020.

The IC3 Role in Combating Cyber Crime[3]

WHAT WE DO



[3] 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; increasing victim reporting via outreach; and hosting a remote access database for all law enforcement via the FBI's LEEP website.

IC3 Core Functions

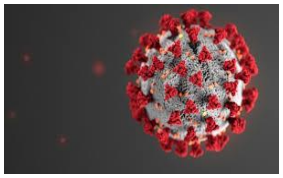
IC3 Core Functions[4]

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, industry 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.

[4] 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.

HOT TOPICS FOR 2020

COVID-19



The year 2020 will forever be remembered as the year of the COVID-19 pandemic. The global impact was unlike anything seen in recent history, and the virus permeated all aspects of life. Fraudsters took the opportunity to exploit the pandemic to target both business and individuals. In 2020, the IC3 received over 28,500 complaints related to COVID-19.

Fraudsters targeted the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which included provisions to help small businesses during the pandemic. The IC3 received thousands of complaints reporting emerging financial crime revolving around CARES Act stimulus funds, specifically targeting unemployment insurance, Paycheck Protection Program (PPP) loans, and Small Business Economic Injury Disaster Loans, as well as other COVID-related fraud.

Most of the IC3 complaints related to CARES Act fraud involved grant fraud, loan fraud, and phishing for Personally Identifiable Information (PII). Complaints have been filed from citizens in several states describing fraudulently submitted online unemployment insurance claims using their identities. Many victims of this identity theft scheme did not know they had been targeted until they attempted to file their own legitimate claim for unemployment insurance benefits. At that time, they received a notification from the state unemployment insurance agency, received an IRS Form 1099-G showing the benefits collected from unemployment insurance, or were notified by their employer that a claim had been filed while the victim is still employed.

People are encouraged to protect themselves from scammers by:

- Using extreme caution in online communication. Verify the sender of an email. Criminals will sometimes change just one letter in an email address to make it look like one you know. Also, be very wary of attachments or links. Hover your mouse over a link before clicking to see where it is sending you.
- Questioning anyone offering you something that is "too good to be true" or is a secret investment opportunity or medical advice.
- Relying on trusted sources, like your own doctor, the Center for Disease Control, and your local health department for medical information and agencies like the Federal Trade Commission and Internal Revenue Service for financial and tax information.

"Unfortunately, criminals are very opportunistic. They see a vulnerable population out there that they can prey upon.", FBI Section Chief Steven Merrill, Financial Crimes Section.

One of the most prevalent schemes seen during the pandemic has been government impersonators. Criminals are reaching out to people through social media, emails, or phone calls pretending to be from the government. The scammers attempt to gather personal information or illicit money through charades or threats.

As the response to COVID-19 turned to vaccinations, scams emerged asking people to pay out of pocket to receive the vaccine, put their names on a vaccine waiting, or obtain early access. Fraudulent advertisements for vaccines popped up on social media platforms, or came via email, telephone calls, online, or from unsolicited/unknown sources.

As we continue to battle COVID-19, protect yourself from fraud and scams. Do not give out your personal information to unknown sources. If you are a victim of an online crime involving COVID-19, report it.

Business Email Compromise (BEC)

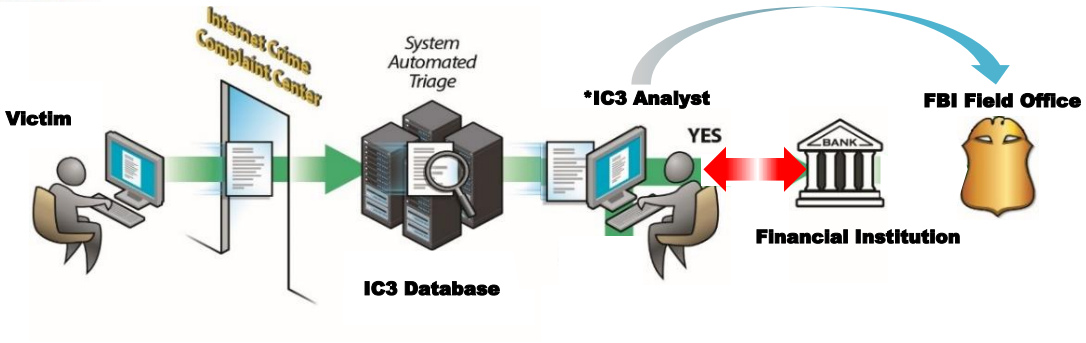
In 2020, the IC3 received 19,369 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints with adjusted losses of over $1.8 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

As the fraudsters have become more sophisticated, the BEC/EAC scheme has evolved in kind. 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 2020, the IC3 observed an increase in the number of BEC/EAC complaints related to the use of identity theft and funds being converted to cryptocurrency. In these variations, we saw an initial victim being scammed in non-BEC/EAC situations to include Extortion, Tech Support, Romance scams, etc., that involved a victim providing a form of ID to a bad actor. That identifying information was then used to establish a bank account to receive stolen BEC/EAC funds and then transferred to a cryptocurrency account.

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 freezing of funds for victims who made transfers to domestic accounts under fraudulent pretenses.



RAT Process[5]

*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).

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

Success in 2020

Incidents: 1,303

Losses: $462,967,963.72

Frozen: $380,211,432.04

Success Rate: 82%

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 and 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, like trends targeting real estate, pre-paid cards, and W-2s, for example.
- Never make any payment changes without verifying the change with the intended recipient; Verify email addresses are accurate when checking email on a cell phone or other mobile device.

[5] 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.

St. Louis

In June 2020, the IC3 received a complaint filed by a victim company regarding a wire transfer of $60 million to a fraudulent overseas bank account in Hong Kong. The reported transaction date fell outside of the International Financial Fraud Kill Chain (FFKC) time frame for action; however, The IC3 RAT notified the Legal Attaché of Hong Kong and the St. Louis Field Office of the large dollar loss. Through the collaboration efforts of the IC3 RAT, the Legal Attaché of Hong Kong, and Hong Kong banking and law enforcement partners, the wire was located and immediately blocked from entering the beneficiary account in Hong Kong. The St. Louis Field Office quickly contacted the victim of this incident to initiate a recall letter with the originating bank and Hong Kong Police. Through these efforts, the full amount of $60 million was returned to the victim.

Chicago

In June 2020, the IC3 was notified of two fraudulent wires totaling $977,411 sent by a victim company specializing in hand sanitizer. The money was intended for an investment in ventilators due to the COVID-19 pandemic. Upon receipt of this notification, the RAT initiated the domestic FFKC to request the recipient financial institution freeze the associated account and any remaining funds. Collaboration with the beneficiary bank resulted in the more recent of the two transfers being frozen in full. The older transfer had already been depleted via wire to a cryptocurrency exchange at another financial institution. Collaboration with the bank, which housed the cryptocurrency account, and with the cryptocurrency account holder company resulted in tracing the wallet path of the funds upon being converted into Bitcoin.

Houston

In April 2020, the IC3 received a complaint from a health care victim regarding five wire transfers sent totaling more than $2 million. The RAT Team initiated the FFKC and, after collaboration with the financial institution, holds were placed on the funds to allow the victim time for the indemnification process. Later inquiries into the recipient account number by the IC3 RaID Team found additional suspicious activity information from financial databases on the possible money mules involved with the account. This information was then compiled into two targeting packages and forwarded to the Houston Field Office for case enhancement purposes.

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 to defraud unwitting individuals. Criminals may pose as support or service representatives offering to resolve such issues as a compromised email or bank account, a virus on a computer, or a software license renewal. Recent complaints involve criminals posing as customer support for financial institutions, utility companies, or virtual currency exchanges. Many victims report being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards.

Although pandemic lockdowns caused a brief slowdown to this fraud activity, victims still reported increases in incidences and losses to tech support fraud.

In 2020, the IC3 received 15,421 complaints related to Tech Support Fraud from victims in 60 countries.

The losses amounted to over $146 million, which represents a 171 percent increase in losses from 2019.

The majority of victims, at least 66 percent, report to be over 60 years of age, and experience at least 84 percent of the losses (over $116 million).

Additional information, explanations, and suggestions for protection regarding Tech Support Fraud is available in the most recent 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.

Knoxville

In 2016, the IC3 identified a subject receiving and processing payments for a call center conducting tech support fraud out of India. The subject received checks from victims who believed they were paying for legitimate tech support services. The subsequent investigation by the Knoxville Field Office revealed a larger group of U.S.-based subjects working with the call center owner and connected over 15,000 victims with losses of approximately $7 million. In November 2019, five subjects were indicted in U.S. District Court, Eastern District of Tennessee. By early 2020, all subjects were arrested and charged. One subject from India is accused of being the owner/director of the call center in India. Three subjects in Iowa and one subject in Maryland are accused of facilitating payments on behalf of the Indian call center. Trials are pending.

Legat New Delhi

In July 2018, the IC3 received a complaint filed by an Indian citizen regarding an illegal call center in Noida, India. IC3 research and analysis identified companies operating on behalf of the call center and over 130 victims who experienced losses of more than $50,000. The IC3 complaints and analysis were provided to FBI Legat New Delhi, who worked with Indian law enforcement who raided the call center in late 2018. In February 2020, confirmation was received from India's Central Bureau of Investigation that charges were filed in India on four subjects, three of which have been were arrested and incarcerated.

Ransomware

In 2020, the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.

Although cyber criminals use a variety of techniques to infect victims with ransomware, the most common means of infection are:

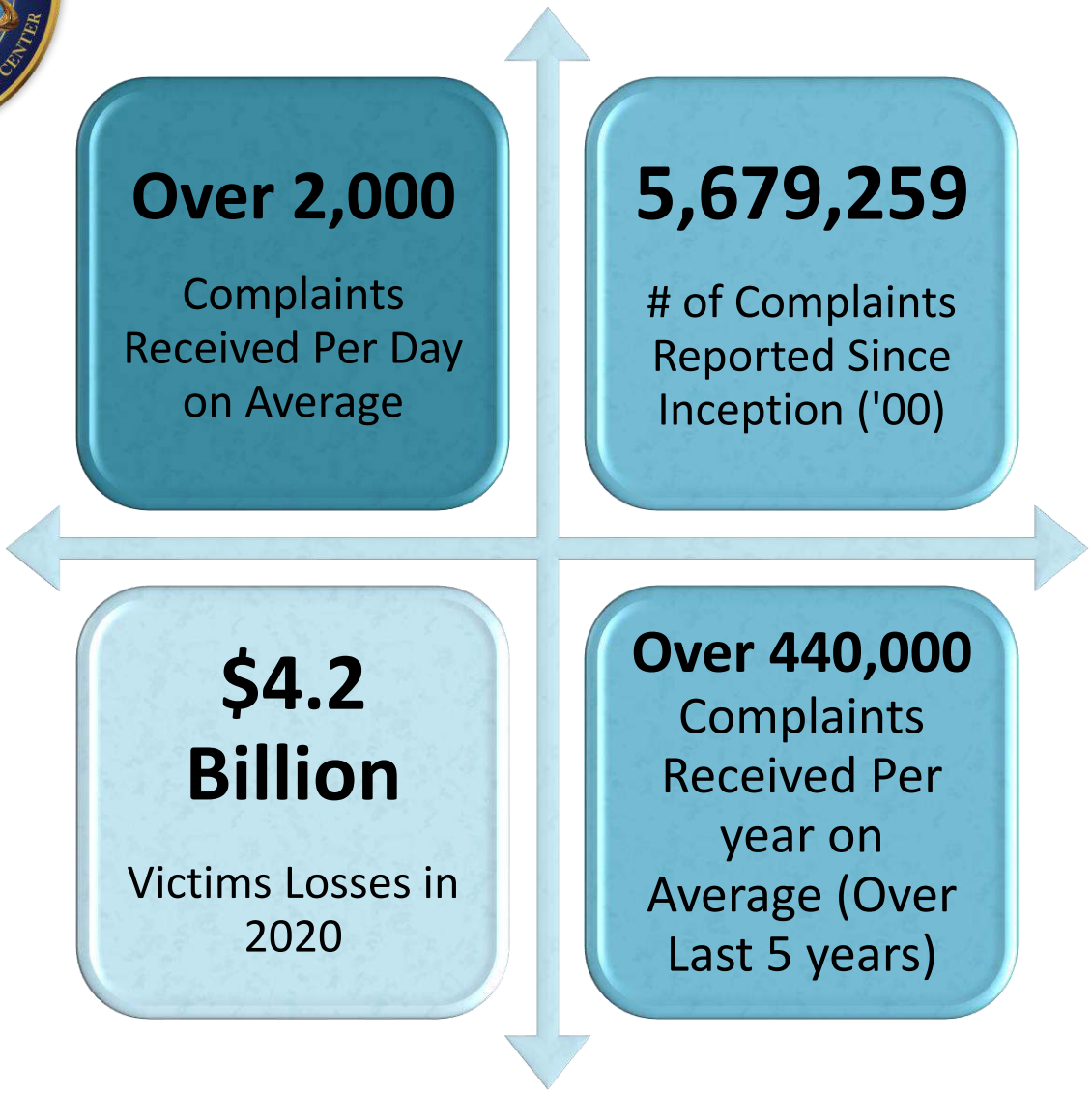
- Email phishing campaigns: The cyber criminal sends an email containing a malicious file or link which deploys malware when clicked by a recipient. Cyber criminals historically have used generic, broad-based spamming strategies to deploy their malware, through recent ransomware campaigns have been more targeted and sophisticated. Criminals may also compromise a victim's email account by using precursor malware, which enables the cyber criminal to use a victim's email account to further spread the infection.

- Remote Desktop Protocol (RDP) vulnerabilities: RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet. Cyber criminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on dark web marketplaces to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware – including ransomware – to victim systems.

- Software vulnerabilities: Cyber criminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware.

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and /or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local field office or the FBI's Internet Crime Complaint Center (IC3). Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

IC3 by the Numbers[6]



[6] Accessibility description: Image depicts key statistics regarding complaints and victim loss. Total losses of $4.2 billion were reported in 2020. The total number of complaints received since the year 2000 is 5,679,259. IC3 has received approximately 440,000 complaints per year on average over the last five years, or more than 2,000 complaints per day.

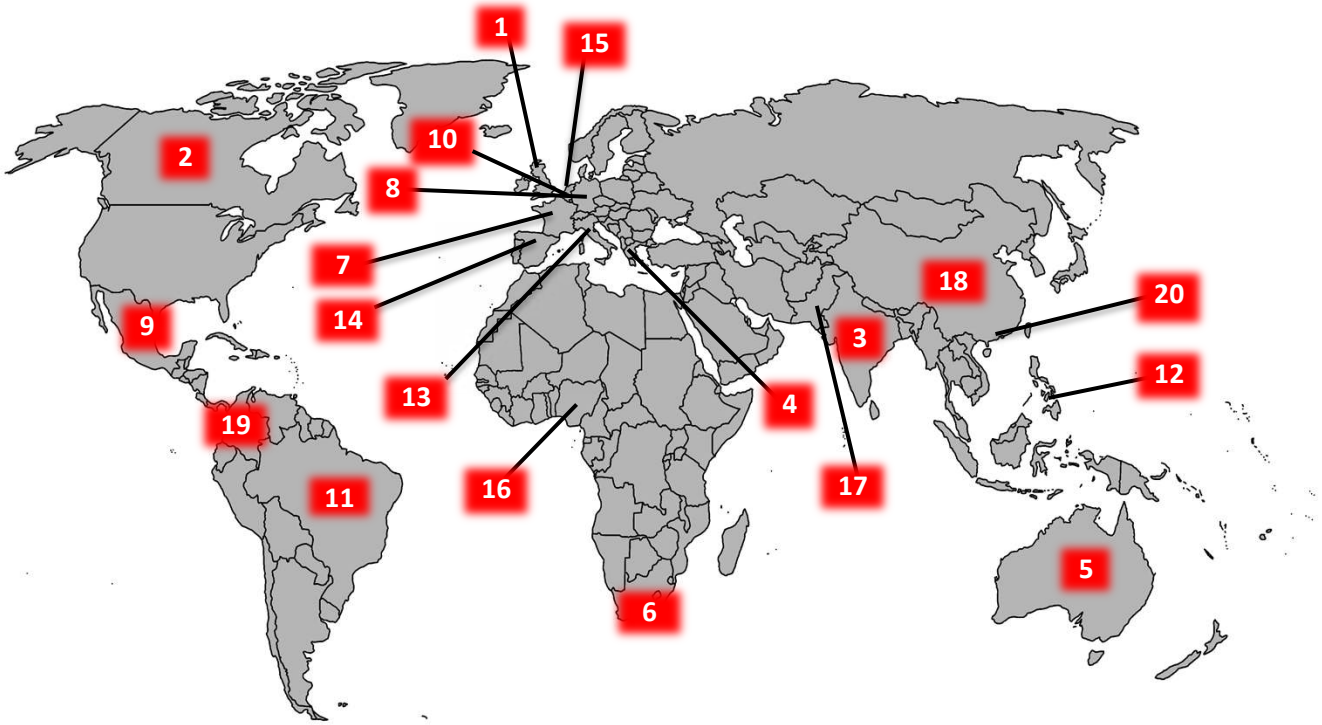
2020 VICTIMS BY AGE GROUP

Victims		
Age Range[7]	**Total Count**	**Total Loss**
Under 20	23,186	$70,980,763
20 - 29	70,791	$197,402,240
30 - 39	88,364	$492,176,845
40 - 49	91,568	$717,161,726
50 - 59	85,967	$847,948,101
Over 60	105,301	$966,062,236

[7] 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.

2020 - TOP 20 INTERNATIONAL VICTIM COUNTRIES

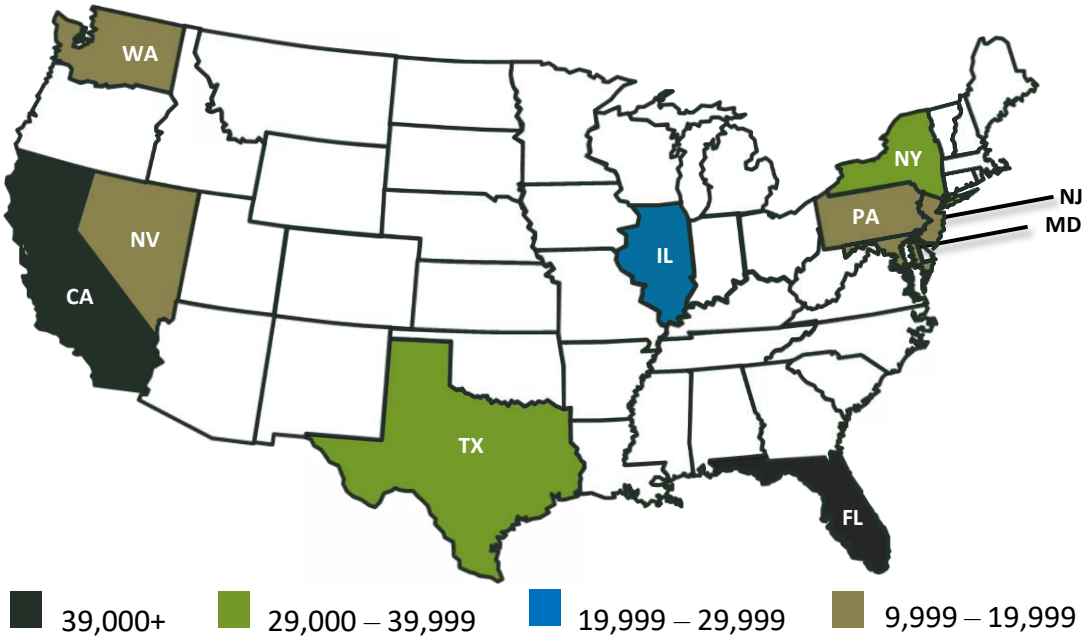
Excluding the United States[8]



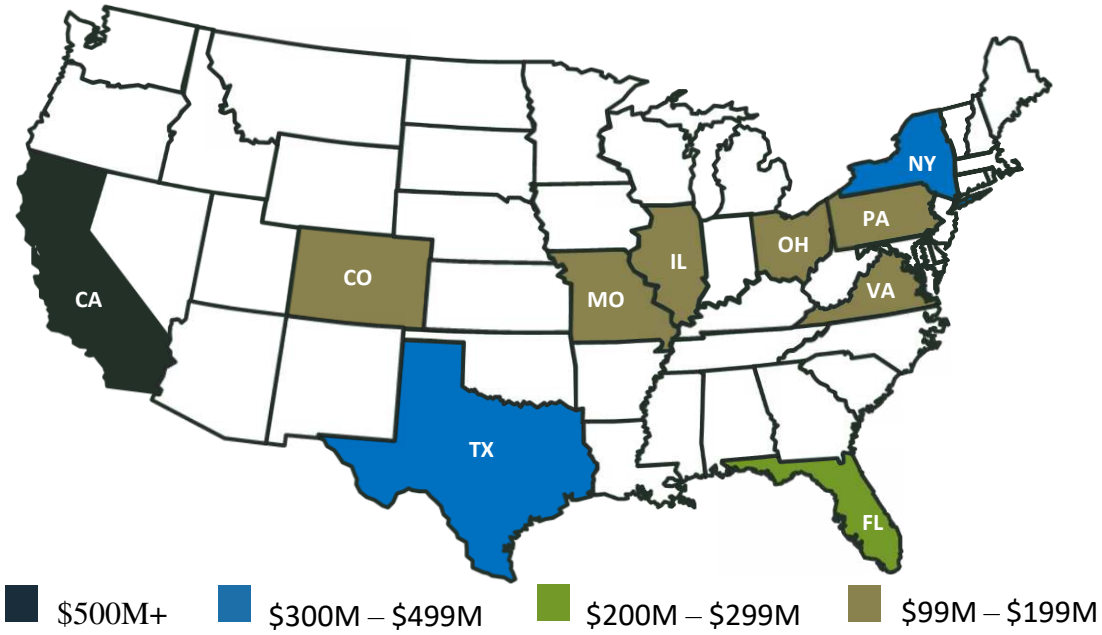
1. United Kingdom	**216,633**	**6. South Africa**	**1,754**	**11. Brazil**	**951**	**16. Nigeria**	**443**
2. Canada	**5,399**	**7. France**	**1,640**	**12. Philippines**	**898**	**17. Pakistan**	**443**
3. India	**2,930**	**8. Germany**	**1,578**	**13. Italy**	**728**	**18. China**	**442**
4. Greece	**2,314**	**9. Mexico**	**1,164**	**14. Spain**	**618**	**19. Colombia**	**418**
5. Australia	**1,807**	**10. Belgium**	**1,023**	**15. Netherlands**	**450**	**20. Hong Kong**	**407**

[8] 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.

2020 - TOP 10 STATES BY NUMBER OF VICTIMS[9]



2020 - TOP 10 STATES BY VICTIM LOSS[10]



[9] 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, Florida, Texas, New York, Illinois, Pennsylvania, Washington, Nevada, New Jersey, and Maryland. Please see Appendix B for more information regarding IC3 data.

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

2020 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	241,342	Other	10,372
Non-Payment/Non-Delivery	108,869	Investment	8,788
Extortion	76,741	Lottery/Sweepstakes/Inheritance	8,501
Personal Data Breach	45,330	IPR/Copyright and Counterfeit	4,213
Identity Theft	43,330	Crimes Against Children	3,202
Spoofing	28,218	Corporate Data Breach	2,794
Misrepresentation	24,276	Ransomware	2,474
Confidence Fraud/Romance	23,751	Denial of Service/TDoS	2,018
Harassment/Threats of Violence	20,604	Malware/Scareware/Virus	1,423
BEC/EAC	19,369	Health Care Related	1,383
Credit Card Fraud	17,614	Civil Matter	968
Employment	16,879	Re-shipping	883
Tech Support	15,421	Charity	659
Real Estate/Rental	13,638	Gambling	391
Advanced Fee	13,020	Terrorism	65
Government Impersonation	12,827	Hacktivist	52
Overpayment	10,988		

Descriptors*		
Social Media	35,439	*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.
Virtual Currency	35,229	

2020 Crime Types *Continued*

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Descriptors*

Social Media	$155,323,073
Virtual Currency	$246,212,432

*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.

**** 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.**

Last 3 Year Complaint Count Comparison

By Victim Count

Crime Type	2020	2019	2018
Advanced Fee	13,020	14,607	16,362
BEC/EAC	19,369	23,775	20,373
Charity	659	407	493
Civil Matter	968	908	768
Confidence Fraud/Romance	23,751	19,473	18,493
Corporate Data Breach	2,794	1,795	2,480
Credit Card Fraud	17,614	14,378	15,210
Crimes Against Children	3,202	1,312	1,394
Denial of Service/TDoS	2,018	1,353	1,799
Employment	16,879	14,493	14,979
Extortion	76,741	43,101	51,146
Gambling	391	262	181
Government Impersonation	12,827	13,873	10,978
Hacktivist	52	39	77
Harassment/Threats of Violence	20,604	15,502	18,415
Health Care Related	1,383	657	337
Identity Theft	43,330	16,053	16,128
Investment	8,788	3,999	3,693
IPR/Copyright and Counterfeit	4,213	3,892	2,249
Lottery/Sweepstakes/Inheritance	8,501	7,767	7,146
Malware/Scareware/Virus	1,423	2,373	2,811
Misrepresentation	24,276	5,975	5,959
Non-Payment/Non-Delivery	108,869	61,832	65,116
Other	10,372	10,842	10,826
Overpayment	10,988	15,395	15,512
Personal Data Breach	45,330	38,218	50,642
Phishing/Vishing/Smishing/Pharming	241,342	114,702	26,379
Ransomware	2,474	2,047	1,493
Real Estate/Rental	13,638	11,677	11,300
Re-Shipping	883	929	907
Spoofing	28,218	25,789	15,569
Tech Support	15,421	13,633	14,408
Terrorism	65	61	120

Last 3 Year Complaint Loss Comparison *Continued*

By Victim Loss			
Crime Type	**2020**	**2019**	**2018**
Advanced Fee	$83,215,405	$100,602,297	$92,271,682
BEC/EAC	$1,866,642,107	$1,776,549,688	$1,297,803,489
Charity	$4,428,766	$2,214,383	$1,006,379
Civil Matter	$24,915,958	$20,242,867	$15,172,692
Confidence Fraud/Romance	$600,249,821	$475,014,032	$362,500,761
Corporate Data Breach	$128,916,648	$53,398,278	$117,711,989
Credit Card Fraud	$129,820,792	$111,491,163	$88,991,436
Crimes Against Children	$660,044	$975,311	$265,996
Denial of Service/TDoS	$512,127	$7,598,198	$2,052,340
Employment	$62,314,015	$42,618,705	$45,487,120
Extortion	$70,935,939	$107,498,956	$83,357,901
Gambling	$3,961,508	$1,458,118	$926,953
Government Impersonation	$109,938,030	$124,292,606	$64,211,765
Hacktivist	$50	$129,000	$77,612
Harassment/Threats of Violence	$6,547,449	$19,866,654	$21,903,829
Health Care Related	$29,042,515	$1,128,838	$4,474,792
Identity Theft	$219,484,699	$160,305,789	$100,429,691
Investment	$336,469,000	$222,186,195	$252,955,320
IPR/Copyright and Counterfeit	$5,910,617	$10,293,307	$15,802,011
Lottery/Sweepstakes/Inheritance	$61,111,319	$48,642,332	$60,214,814
Malware/Scareware/Virus	$6,904,054	$2,009,119	$7,411,651
Misrepresentation	$19,707,242	$12,371,573	$20,000,713
Non-Payment/Non-Delivery	$265,011,249	$196,563,497	$183,826,809
Other	$101,523,082	$66,223,160	$63,126,929
Overpayment	$51,039,922	$55,820,212	$53,225,507
Personal Data Breach	$194,473,055	$120,102,501	$148,892,403
Phishing/Vishing/Smishing/Pharming	$54,241,075	$57,836,379	$48,241,748
Ransomware	$29,157,405	$8,965,847	$3,621,857
Real Estate/Rental	$213,196,082	$221,365,911	$149,458,114
Re-Shipping	$3,095,265	$1,772,692	$1,684,179
Spoofing	$216,513,728	$300,478,433	$70,000,248
Tech Support	$146,477,709	$54,041,053	$38,697,026
Terrorism	$0	$49,589	$10,193

2020 Overall State Statistics

Victim per State*

Rank	State	Victims	Rank	State	Victims
1	California	69,541	30	Louisiana	5,077
2	Florida	53,793	31	Utah	4,926
3	Texas	38,640	32	Oklahoma	4,785
4	New York	34,505	33	Arkansas	4,237
5	Illinois	20,185	34	Kansas	3,457
6	Pennsylvania	18,636	35	New Mexico	3,427
7	Washington	17,229	36	Mississippi	2,478
8	Nevada	16,110	37	Delaware	2,230
9	New Jersey	14,829	38	Idaho	2,209
10	Maryland	14,804	39	Nebraska	2,166
11	Virginia	13,770	40	District of Columbia	2,132
12	Ohio	13,421	41	Alaska	2,073
13	Georgia	13,402	42	New Hampshire	2,015
14	Arizona	13,009	43	Hawaii	1,978
15	Indiana	12,786	44	West Virginia	1,902
16	Michigan	12,521	45	Puerto Rico	1,886
17	Colorado	12,325	46	Rhode Island	1,677
18	North Carolina	12,223	47	Maine	1,672
19	Massachusetts	11,468	48	Montana	1,365
20	Iowa	9,367	49	Wyoming	913
21	Tennessee	8,527	50	Vermont	856
22	Wisconsin	8,308	51	South Dakota	777
23	Missouri	8,160	52	North Dakota	760
24	Minnesota	6,847	53	U.S. Minor Outlying Islands	116
25	Oregon	6,817	54	Guam	112
26	Kentucky	6,815	55	Virgin Islands, U.S.	92
27	South Carolina	5,853	56	American Samoa	42
28	Alabama	5,803	57	Northern Mariana Islands	20
29	Connecticut	5,636			

***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.**

2020 Overall State Statistics *Continued*

Total Victim Losses by State*

Rank	State	Loss	Rank	State	Loss
1	California	$621,452,320	30	South Carolina	$25,244,978
2	New York	$415,812,917	31	New Mexico	$23,903,594
3	Texas	$313,565,225	32	Iowa	$21,396,701
4	Florida	$295,032,829	33	Oklahoma	$20,748,692
5	Ohio	$170,171,951	34	Kansas	$19,157,289
6	Illinois	$150,496,678	35	District of Columbia	$18,942,722
7	Missouri	$115,913,584	36	Mississippi	$18,111,738
8	Pennsylvania	$108,506,204	37	Arkansas	$17,371,515
9	Virginia	$101,661,604	38	Hawaii	$13,671,531
10	Colorado	$100,663,897	39	Puerto Rico	$13,275,104
11	Georgia	$98,762,523	40	Kentucky	$12,590,784
12	New Jersey	$98,727,053	41	Nebraska	$11,799,640
13	Massachusetts	$97,583,753	42	Idaho	$11,670,650
14	Washington	$88,020,254	43	American Samoa	$7,806,373
15	Michigan	$83,999,442	44	Rhode Island	$7,669,670
16	Arizona	$72,128,637	45	Alaska	$7,342,743
17	North Carolina	$69,409,152	46	Maine	$7,073,260
18	Maryland	$62,473,193	47	Delaware	$6,486,617
19	Minnesota	$58,341,798	48	Montana	$5,669,293
20	Utah	$47,113,946	49	Wyoming	$5,096,704
21	Nevada	$44,383,452	50	New Hampshire	$4,949,296
22	Connecticut	$41,311,798	51	West Virginia	$4,823,786
23	Tennessee	$40,191,616	52	Vermont	$4,175,799
24	Oregon	$38,389,702	53	South Dakota	$3,208,241
25	Wisconsin	$36,081,681	54	Virgin Islands, U.S.	$620,962
26	Indiana	$35,180,105	55	Guam	$259,338
27	Alabama	$27,549,157	56	U.S. Minor Outlying Islands	$201,022
28	Louisiana	$26,717,928	57	Northern Mariana Islands	$67,403
29	North Dakota	$25,804,940			

***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.**

2020 Overall State Statistics *Continued*

Count by Subject per State*

Rank	State	Subjects	Rank	State	Subjects
1	California	26,379	30	Utah	1,251
2	Florida	19,364	31	Louisiana	1,246
3	Texas	12,914	32	District of Columbia	1,174
4	New Jersey	10,616	33	Kentucky	1,146
5	New York	10,052	34	Delaware	1,096
6	Maryland	7,279	35	Kansas	1,090
7	Illinois	4,780	36	Connecticut	969
8	Georgia	4,321	37	New Mexico	890
9	Pennsylvania	4,066	38	Mississippi	824
10	Virginia	3,929	39	Arkansas	784
11	Washington	3,807	40	Iowa	721
12	Ohio	3,708	41	Maine	691
13	Nevada	3,707	42	Hawaii	490
14	Arizona	3,005	43	West Virginia	449
15	North Carolina	2,940	44	Idaho	448
16	Michigan	2,793	45	North Dakota	425
17	Colorado	2,502	46	New Hampshire	360
18	Tennessee	2,480	47	Puerto Rico	330
19	Indiana	2,211	48	Rhode Island	330
20	Massachusetts	2,192	49	Alaska	292
21	Missouri	1,824	50	Wyoming	277
22	Nebraska	1,734	51	South Dakota	213
23	Oklahoma	1,721	52	Vermont	172
24	Minnesota	1,699	53	U.S. Minor Outlying Islands	32
25	Alabama	1,574	54	Guam	22
26	Oregon	1,543	55	Virgin Islands, U.S.	18
27	Montana	1,507	56	American Samoa	6
28	Wisconsin	1,342	57	Northern Mariana Islands	2
29	South Carolina	1,341			

***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.**

2020 Overall State Statistics *Continued*

Subject Earnings per Destination State*					
Rank	**State**	**Loss**	**Rank**	**State**	**Loss**
1	California	$233,907,224	30	Oregon	$9,473,549
2	New York	$142,689,230	31	Missouri	$9,322,612
3	Texas	$135,573,752	32	Utah	$9,225,351
4	Florida	$125,049,181	33	Kansas	$9,205,096
5	Ohio	$83,544,428	34	Wisconsin	$8,357,864
6	Georgia	$63,933,271	35	Kentucky	$6,623,738
7	Illinois	$52,691,430	36	Iowa	$6,253,965
8	Washington	$47,175,498	37	Maine	$6,138,289
9	Colorado	$42,901,870	38	Alaska	$5,785,807
10	New Jersey	$38,491,372	39	New Mexico	$5,711,844
11	Maryland	$29,971,760	40	Delaware	$5,673,719
12	Nevada	$29,127,283	41	Nebraska	$5,651,920
13	Arizona	$28,473,605	42	Mississippi	$3,978,526
14	Pennsylvania	$28,431,645	43	New Hampshire	$3,595,627
15	Virginia	$25,657,584	44	Idaho	$3,582,262
16	Michigan	$24,395,899	45	Hawaii	$3,168,489
17	North Dakota	$22,018,169	46	Arkansas	$2,546,501
18	North Carolina	$20,552,835	47	South Dakota	$2,486,492
19	District of Columbia	$14,479,130	48	Wyoming	$2,337,866
20	Massachusetts	$14,295,694	49	Rhode Island	$2,013,255
21	Oklahoma	$13,036,365	50	Vermont	$1,506,113
22	Indiana	$12,864,230	51	Puerto Rico	$1,422,863
23	Connecticut	$12,533,843	52	West Virginia	$1,352,504
24	Tennessee	$12,017,224	53	Virgin Islands, U.S.	$248,287
25	Louisiana	$11,932,340	54	U.S. Minor Outlying Islands	$225,488
26	Minnesota	$11,920,258	55	Guam	$12,520
27	Alabama	$10,739,652	56	American Samoa	$494
28	Montana	$10,262,099	57	Northern Mariana Islands	$315
29	South Carolina	$10,063,305			

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

Business Email Compromise/Email Account Compromise: BEC is a scam targeting businesses (not individuals) working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam which targets individuals. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

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

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

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 theft and fraud committed using a credit card or any similar payment mechanism (ACH. EFT, recurring charge, etc.) as a fraudulent source of funds in a transaction.

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

Denial of Service/TDoS: A Denial of Service (DoS) attack floods a network/system or a Telephony Denial of Service (TDoS) floods a voice 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 which usually involving health care providers, companies, or individuals. Schemes may include offers for fake insurance cards, health insurance marketplace assistance, stolen health information, or various other scams and/or any scheme involving medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums/social media, and fraudulent websites.

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

Identity Theft: Someone steals and uses personal identifying information, like a name or Social Security number, without permission to commit fraud or other crimes and/or (Account Takeover) a fraudster 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. (Retirement, 401K, Ponzi, Pyramid, etc.).

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.

Malware/Scareware/Virus: Software or code intended to damage, disable, or capable of copying itself onto a computer and/or computer systems to have a detrimental effect or destroy data.

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/spill of personal data which is released from a secure location to an untrusted environment. Also, a security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual.

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

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

Re-shipping: Individuals receive packages at their residence and subsequently repackage the merchandise for shipment, usually abroad.

Real Estate/Rental: Loss of funds from a real estate investment or fraud involving rental or timeshare property.

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. 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: Subject posing as technical or customer support/service.

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.
- Victim is identified as the individual filing a complaint.
- Subject is identified as the individual perpetrating the scam as reported by the victim.
- “Count by Subject per state” is the number of subjects per state, as reported by victims.
- “Subject earnings per Destination State” is the amount swindled by the subject, as reported by the victim, per state.