



FEDERAL BUREAU of INVESTIGATION Internet Crime Report 2021



INTERNET CRIME COMPLAINT CENTER



Contents

| | |
|---|----|
| INTRODUCTION | 3 |
| THE IC3 | 4 |
| THE IC3 ROLE IN COMBATING CYBER CRIME..... | 5 |
| IC3 CORE FUNCTIONS..... | 6 |
| IC3 COMPLAINT STATISTICS | 7 |
| Last 5 Years..... | 7 |
| Top 5 Crime Type Comparison | 8 |
| THREAT OVERVIEWS FOR 2021 | 9 |
| Business Email Compromise (BEC) | 9 |
| IC3 RECOVERY ASSET TEAM | 10 |
| RAT SUCCESSES | 11 |
| Confidence Fraud / Romance Scams | 12 |
| Cryptocurrency (Virtual Currency) | 13 |
| Ransomware..... | 14 |
| Tech Support Fraud..... | 17 |
| IC3 by the Numbers..... | 18 |
| 2021 Victims by Age Group | 19 |
| 2021 - Top 20 International Victim Countries | 20 |
| 2021 - Top 10 States by Number of Victims | 21 |
| 2021 - Top 10 States by Victim Loss in \$ Millions..... | 21 |
| 2021 CRIME TYPES | 22 |
| 2021 Crime Types continued..... | 23 |
| Last 3 Year Complaint Count Comparison | 24 |
| Last 3 Year Complaint Loss Comparison | 25 |
| Overall State Statistics..... | 26 |
| Overall State Statistics continued..... | 27 |
| Overall State Statistics continued..... | 28 |
| Overall State Statistics continued..... | 29 |
| Appendix A: Definitions | 30 |
| Appendix B: Additional Information about IC3 Data | 33 |

INTRODUCTION

Dear Reader,

In 2021, America experienced an unprecedented increase in cyber attacks and malicious cyber activity. These cyber attacks compromised businesses in an extensive array of business sectors as well as the American public. As the cyber threat evolves and becomes increasingly intertwined with traditional foreign intelligence threats and emerging technologies, the FBI continues to leverage our unique authorities and partnerships to impose risks and consequences on our nation's cyber adversaries.

The FBI's Internet Crime Complaint Center (IC3) provides the American public with a direct outlet to report cyber crimes to the FBI. We analyze and investigate the reporting to track the trends and threats from cyber criminals and then share this data with our intelligence and law enforcement partners. The FBI, alongside our partners, recognizes how crucial information sharing of cyber activities is to prepare our partners to combat the cyber threat, through a whole-of-government approach. Critical to that approach is public reporting to IC3 - enabling us to fill in the missing pieces with this valuable information during the investigatory process. Not only does this reporting help to prevent additional crimes, it allows us to develop key insights on the ever-evolving trends and threats we face from malign cyber actors.

In 2021, IC3 continued to receive a record number of complaints from the American public: 847,376 reported complaints, which was a 7% increase from 2020, with potential losses exceeding \$6.9 billion. Among the 2021 complaints received, ransomware, business e-mail compromise (BEC) schemes, and the criminal use of cryptocurrency are among the top incidents reported. In 2021, BEC schemes resulted in 19,954 complaints with an adjusted loss of nearly \$2.4 billion.

IC3's commitment to cyber victims and partnerships allow for the continued success through programs such as the IC3's Recovery Asset Team (RAT). Established in 2018, RAT streamlines communications with financial institutions and FBI field offices to assist freezing of funds for victims. In 2021, the IC3's RAT initiated the Financial Fraud Kill Chain (FFKC) on 1,726 BEC complaints involving domestic to domestic transactions with potential losses of \$443,448,237. A monetary hold was placed on approximately \$329 million, which represents a 74% success rate.

In 2021, heightened attention was brought to the urgent need for more cyber incident reporting to the federal government. Cyber incidents are in fact crimes deserving of an investigation, leading to judicial repercussions for the perpetrators who commit them. Thank you to all those readers who reported crimes to IC3 throughout the year. Without this reporting, we could not be as effective in ensuring consequences are imposed on those perpetrating these attacks and our understanding of these threats would not be as robust. Please visit [IC3.gov](https://ic3.gov) to access the latest information on criminal internet activity.

The FBI's Cyber Division is working harder than ever to protect the American public and to instill safety, security, and confidence in a digitally connected world. We encourage everyone to use IC3 and reach out to their local FBI field office to report malicious activity. Together we can continue to create a safer and more secure cyber landscape.



Paul Abbate
Deputy Director
Federal Bureau of Investigation

THE IC3

Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities. We are focused on protecting the American people from terrorism, espionage, cyber attacks and major criminal threats, and on supporting our many partners with information, services, support, training, and leadership. The IC3 serves those needs as a mechanism to gather intelligence on cyber and internet crime so we can stay ahead of the threat.

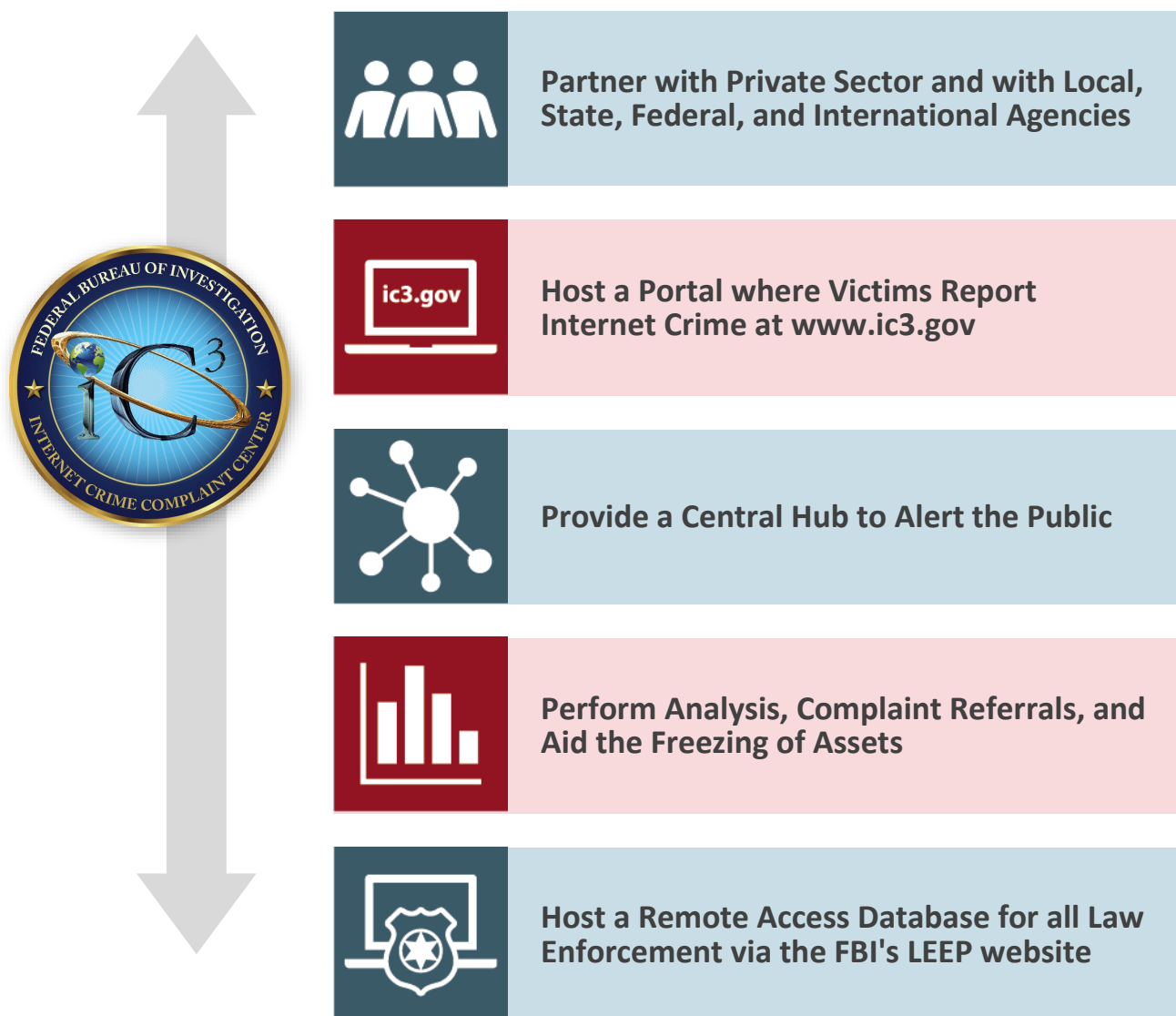
The IC3 was established in May 2000 to receive complaints of internet related crime and has received more than 6.5 million complaints since its inception. Its mission is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected cyber enabled criminal activity, and to develop effective alliances with law enforcement and industry partners to help those who report. Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and for public awareness.

To promote public awareness, the IC3 aggregates the submitted data and produces an annual report to educate on the trends impacting the public. The quality of the data is directly attributable to the information ingested via the public interface, www.ic3.gov, and the data categorized based on the information provided in the individual complaints. The IC3 staff analyzes the data to identify trends in cyber crimes and how those trends may impact the public in the coming year.







THE IC3 ROLE IN COMBATING CYBER CRIME¹

What we do



¹ Accessibility description: Image lists IC3's primary functions including partnering with private sector and with local, state, federal, and international agencies; hosting a victim reporting portal at www.ic3.gov; providing a central hub to alert the public to threats; Perform Analysis, Complaint Referrals, and Asset Recovery; and hosting a remote access database for all law enforcement via the FBI's LEEP website.

IC3 CORE FUNCTIONS²

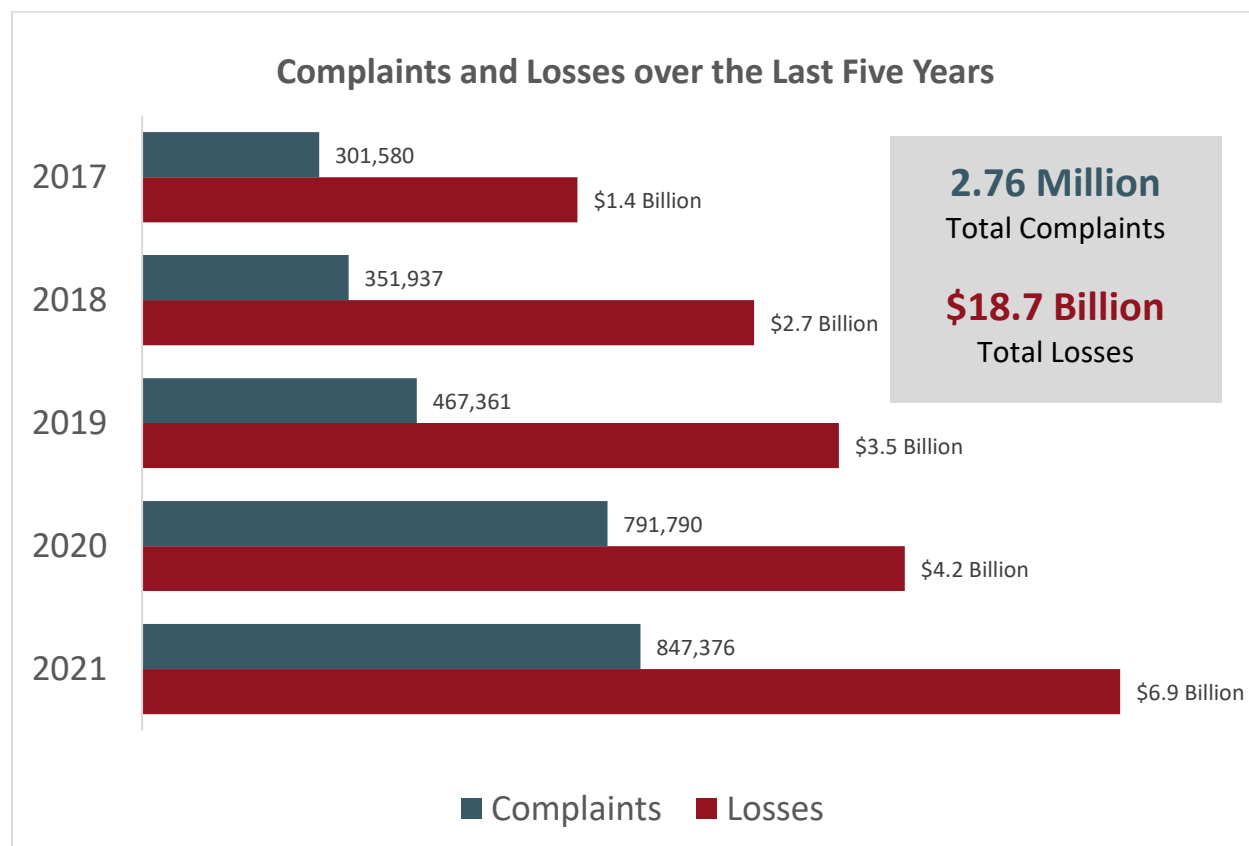
|  |  |  |  |
|---|---|---|--|
| COLLECTION | ANALYSIS | PUBLIC AWARENESS | REFERRALS |
| <p>The IC3 is the central point for Internet crime victims to report and alert the appropriate agencies to suspected criminal Internet activity. Victims are encouraged and often directed by law enforcement to file 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.</p> | <p>The IC3 reviews and analyzes data submitted through its website to identify emerging threats and new trends. In addition, the IC3 quickly alerts financial Institutions to fraudulent transactions which enables the freezing of victim funds.</p> | <p>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.</p> | <p>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 investigates and determines a crime has been committed, legal action may be brought against the perpetrator.</p> |

² 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.

IC3 COMPLAINT STATISTICS

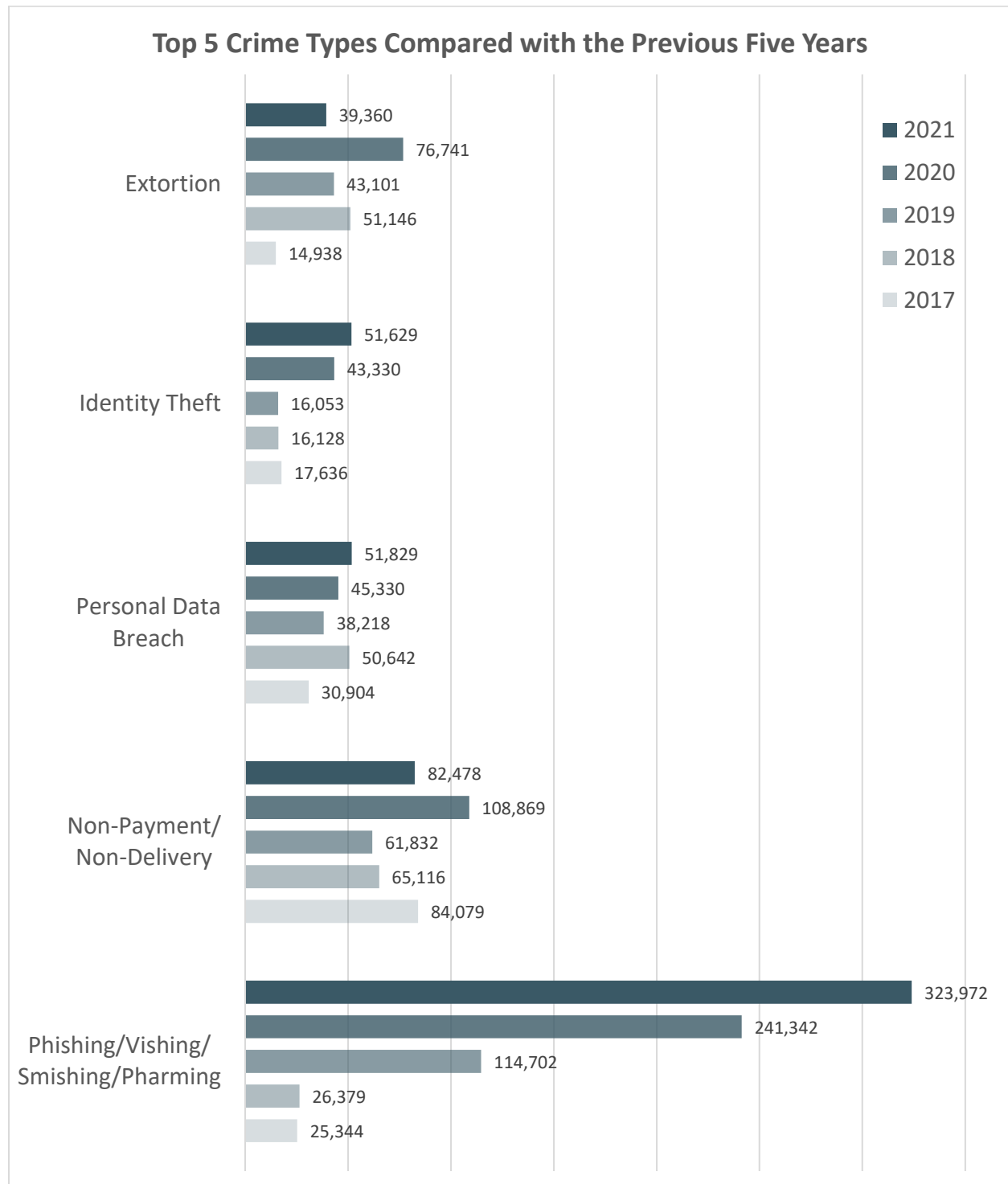
LAST 5 YEARS

Over the last five years, the IC3 has received an average of 552,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.³



³ Accessibility description: Chart includes yearly and aggregate data for complaints and losses over the years 2017 to 2021. Over that time, IC3 received a total of 2,760,044 complaints, reporting a loss of \$18.7 billion.

TOP 5 CRIME TYPE COMPARISON⁴



⁴ Accessibility description: Chart includes a victim loss comparison for the top five reported crime types for the years of 2017 to 2021.

THREAT OVERVIEWS FOR 2021

BUSINESS EMAIL COMPROMISE (BEC)



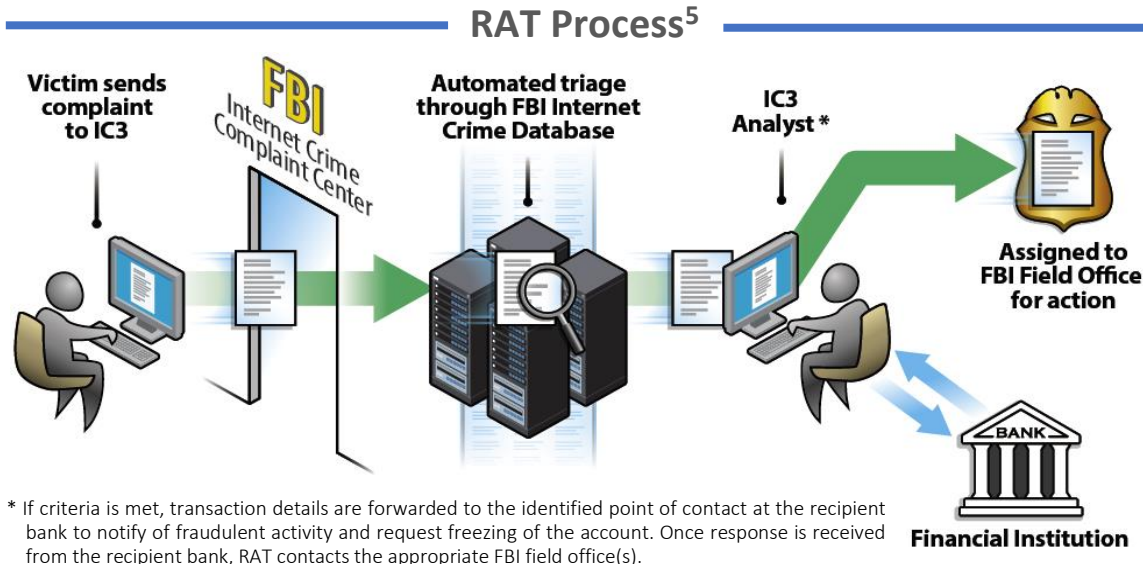
In 2021, the IC3 received 19,954 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints with adjusted losses at nearly \$2.4 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

As fraudsters have become more sophisticated and preventative measures have been put in place, the BEC/EAC scheme has continually evolved in kind. The scheme has evolved from simple hacking or spoofing of business and personal email accounts and a request to send wire payments to fraudulent bank accounts. These schemes historically involved compromised vendor emails, requests for W-2 information, targeting of the real estate sector, and fraudulent requests for large amounts of gift cards. Now, fraudsters are using virtual meeting platforms to hack emails and spoof business leaders' credentials to initiate the fraudulent wire transfers. These fraudulent wire transfers are often immediately transferred to cryptocurrency wallets and quickly dispersed, making recovery efforts more difficult.

The COVID-19 pandemic and the restrictions on in-person meetings led to increases in telework or virtual communication practices. These work and communication practices continued into 2021, and the IC3 has observed an emergence of newer BEC/EAC schemes that exploit this reliance on virtual meetings to instruct victims to send fraudulent wire transfers. They do so by compromising an employer or financial director's email, such as a CEO or CFO, which would then be used to request employees to participate in virtual meeting platforms. In those meetings, the fraudster would insert a still picture of the CEO with no audio, or a "deep fake" audio through which fraudsters, acting as business executives, would then claim their audio/video was not working properly. The fraudsters would then use the virtual meeting platforms to directly instruct employees to initiate wire transfers or use the executives' compromised email to provide wiring instructions.

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.



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

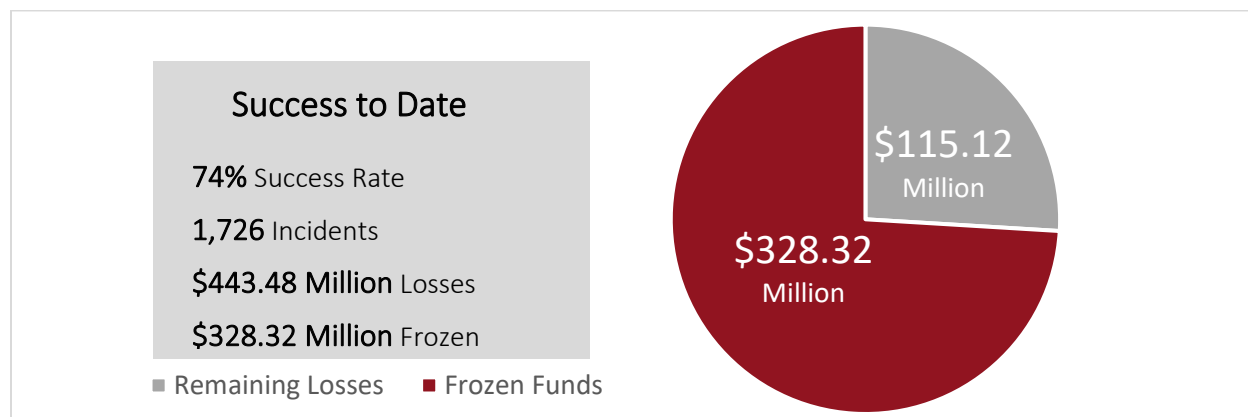
Goals of RAT-Financial Institution Partnership

- 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 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 SUCCESSES⁶

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:

Philadelphia

In December 2021, the IC3 received a complaint filed by a victim roadway commission regarding a wire transfer of more than \$1.5 million to a fraudulent U.S. domestic bank account. The IC3 RAT quickly notified the recipient financial institution of the fraudulent account by initiating the financial fraud kill chain. Collaboration between the IC3 RAT, the recipient financial institution, and the Philadelphia Field office resulted in learning the subject quickly depleted the wired funds from the original account into two separate accounts held at the same institution. The financial institution was able to quickly identify the second-hop accounts and freeze the funds, making a full recovery possible.

Memphis

In June 2021, the IC3 received a complaint filed by a victim law office regarding a wire transfer of more than \$198k to a fraudulent U.S. domestic account. IC3 RAT collaboration with the Memphis Field Office and the recipient financial institution resulted in learning the domestic account was a correspondent account for a fraudulent account in Nigeria. IC3 RAT immediately initiated the international FFKC to FinCEN and LEGAT Abuja, which resulted in freezing the full wired amount. The victim forwarded a note of gratitude for all the work put into their case.

Albany

In October 2021, the IC3 received a complaint filed by a victim of a tech support scam where an unauthorized wire transfer of \$53k was sent from their account to a U.S. domestic custodial account held by a cryptocurrency exchange (CE). The IC3 RAT immediately notified the recipient financial institution and collaborated with the CE that held the account. With the knowledge that funds sent to cryptocurrency accounts will be depleted to crypto faster than the usual wire transfer gets depleted, the immediate efforts of initiating the financial fraud kill chain with the CE resulted in the freezing of the funds in the custodial account before they could be depleted to purchase or withdraw cryptocurrency. Further collaboration with the domestic financial institution and the Albany Field Office confirmed the funds were frozen in the account, making a full recovery possible.

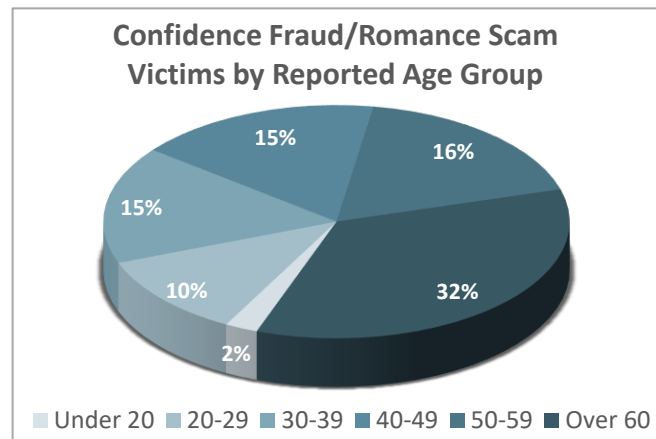
⁶ Accessibility description: Image shows Success to Date to include 74% Success Rate; 1,726 Incidents; \$443.48 Million in Losses; and \$328.32. Million Frozen.

CONFIDENCE FRAUD / ROMANCE SCAMS⁷



Confidence Fraud/Romance scams encompass those designed to pull on a victim's "heartstrings." In 2021, the IC3 received reports from 24,299 victims who experienced more than \$956 million in losses to Confidence Fraud/Romance scams. This type of fraud accounts for the third highest losses reported by victims.

Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and confidence. The scammer uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim. The criminals who carry out Romance scams are experts at what they do and will seem genuine, caring, and believable. The scammer's intention is to quickly establish a relationship, endear himself/herself to the victim, gain trust, and eventually ask for money. Scammers may propose marriage and make plans to meet in person, but that will never happen. Scam artists often say they are in the military, or a trades-based industry engaged in projects outside the U.S. That makes it easier to avoid meeting in person—and more plausible when they request money be sent overseas for a medical emergency or unexpected legal fee. Grandparent Scams also fall into this category, where criminals impersonate a panicked loved one, usually a grandchild, nephew, or niece of an elderly person. The loved one claims to be in trouble and needs money immediately.



Con artists are present on most dating and social media sites. In 2021, the IC3 received thousands of complaints from victims of online relationships resulting in sextortion or investment scams.

- Sextortion occurs when someone threatens to distribute your private and sensitive material if their demands are not met. In 2021, the IC3 received more than 18,000 sextortion-related complaints, with losses over \$13.6 million. Please see the September 2021 IC3 PSA on Sextortion for more information.⁸
- Many victims of Romance scams also report being pressured into investment opportunities, especially using cryptocurrency. In 2021, the IC3 received more than 4,325 complaints, with losses over \$429 million, from Confidence Fraud/Romance scam victims who also reported the use of investments and cryptocurrencies, or "pig butchering" —so named because victims' investment accounts are fattened up before draining, much a like a pig before slaughter. Additional information on "pig butchering" can be found in the September 2021 IC3 PSA I-091621-PSA.⁹

⁷ Accessibility description: Chart shows Confidence Fraud/Romance Scam Victim by Reported Age Group. Under 20 2%; 20-29 10%; 30-39 15%; 40-49 15%; 50-59 16%; Over 60 32%

⁸ FBI Warns about an Increase in Sextortion Complaints. <https://www.ic3.gov/Media/Y2021/PSA210902>

⁹ Scammers Defraud Victims of Millions of Dollars in New Trend in Romance Scams.

CRYPTOCURRENCY (VIRTUAL CURRENCY)



In 2021, the IC3 received 34,202 complaints involving the use of some type of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, or Ripple. While that number showed a decrease from 2020's victim count (35,229), the loss amount reported in IC3 complaints increased nearly seven-fold, from 2020's reported amount of \$246,212,432, to total reported losses in 2021 of more than \$1.6 billion.

Initially worth only fractions of pennies on the dollar, several cryptocurrencies have seen their values increase substantially, sometimes exponentially. Once limited to hackers, ransomware groups, and other denizens of the "dark web," cryptocurrency is becoming the preferred payment method for all types of scams – SIM swaps, tech support fraud, employment schemes, romance scams, even some auction fraud. It is extremely pervasive in investment scams, where losses can reach into the hundreds of thousands of dollars per victim. The IC3 has noted the following scams particularly using cryptocurrencies.

- **Cryptocurrency ATMs:** Automated Teller Machines (ATMs) used to purchase cryptocurrency are popping up everywhere. Regulations on the machines are lax and purchases are almost instantaneous and irreversible, making this payment method lucrative to criminals. In 2021, the IC3 received more than 1,500 reports of scams using crypto ATMs, with losses of approximately \$28 million. The most common scams reported were Confidence Fraud/Romance, Investment, Employment, and Government Impersonation. Read more about crypto ATM scams in IC3 PSA I-110421-PSA.10
- **Cryptocurrency support impersonators:** Increasingly, crypto owners are falling victim to scammers impersonating support or security from cryptocurrency exchanges. Owners are alerted of an issue with their crypto wallet and are convinced to either give access to their crypto wallet or transfer the contents of their wallet to another wallet to "safeguard" the contents. Crypto owners are also searching online for support with their cryptocurrencies. Owners contact fake support numbers located online and are convinced to give up login information or control of their crypto accounts.
- **Many victims of Romance scams also report being pressured into investment opportunities, especially using cryptocurrency.** In 2021, the IC3 received more than 4,325 complaints, with losses over \$429 million, from Confidence Fraud/Romance scam victims who also reported the use of investments and cryptocurrencies, or "pig butchering." The scammer's initial contact is typically made via dating apps and other social media sites. The scammer gains the confidence and trust of the victim, and then claims to have knowledge of cryptocurrency investment or trading opportunities that will result in substantial profits.

<https://www.ic3.gov/Media/Y2021/PSA210916>

¹⁰ The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment
<https://www.ic3.gov/Media/Y2021/PSA211104>

RANSOMWARE¹¹



In 2021, the IC3 received 3,729 complaints identified as ransomware with adjusted losses of more than \$49.2 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.

Ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally. Although cyber criminals use a variety of techniques to infect victims with ransomware, phishing emails, Remote Desktop Protocol (RDP) exploitation, and exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents reported to the IC3. Once a ransomware threat actor has gained code execution on a device or network access, they can deploy ransomware. Note: these infection vectors likely remain popular because of the increased use of remote work and schooling starting in 2020 and continuing through 2021. This increase expanded the remote attack surface and left network defenders struggling to keep pace with routine software patching.¹²

Immediate Actions You Can Take Now to Protect Against Ransomware:

- Update your operating system and software.
 - Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
 - If you use Remote Desktop Protocol (RDP), secure and monitor it.
 - Make an offline backup of your data.
-

Ransomware and Critical Infrastructure Sectors

In June 2021, the IC3 began tracking reported ransomware incidents in which the victim was a member of a critical infrastructure sector. There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on our security, national economy, public health or safety, or any combination thereof.

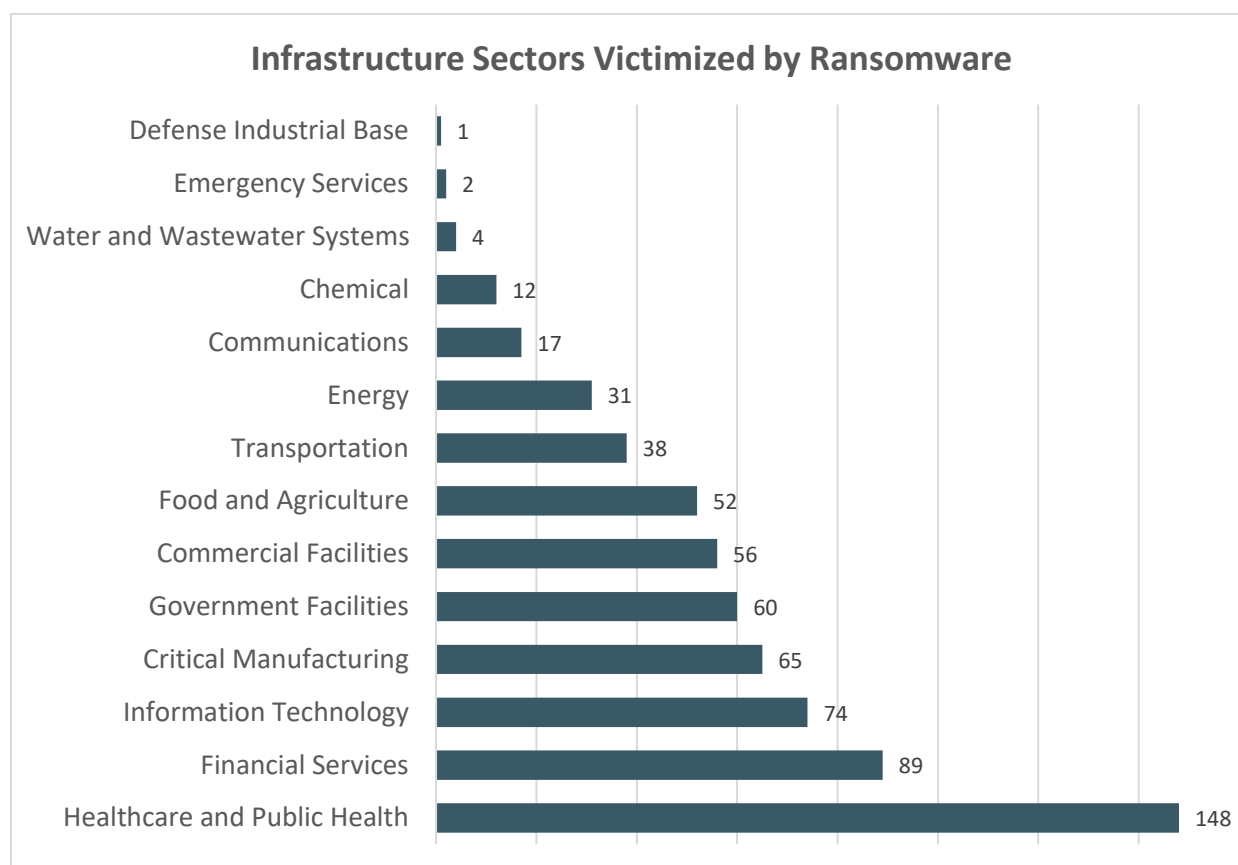
¹¹ Accessibility description: Image shows actions you can Take to Protect Against Ransomware: Update your operating system. Implement user training and phishing exercises to raise awareness, secure and monitor Remote Desktop Protocol (DDP) if used, and make an offline backup of our data.

¹² 2021 Trends Show Increased Globalized Threat of Ransomware.
<https://www.ic3.gov/Media/News/2022/220209.pdf>

In October 2021, the IC3 posted a Joint Cybersecurity Advisory (CSA) to ic3.gov regarding ongoing cyber threats to U.S. Water and Wastewater Systems. In September 2021, the IC3 posted a Private Industry Notification (PIN) which warned that ransomware attacks targeting the Food and Agriculture sector disrupt operations, cause financial loss, and negatively impact the food supply chain. In May 2021, the IC3 posted an FBI Liaison Alert System (FLASH) report that advised the FBI identified at least 16 CONTI ransomware attacks targeting US Healthcare and First Responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year. And in March 2021, the IC3 posted a FLASH warning that FBI reporting indicated an increase in PYSA ransomware targeting education institutions in 12 US states and the United Kingdom.

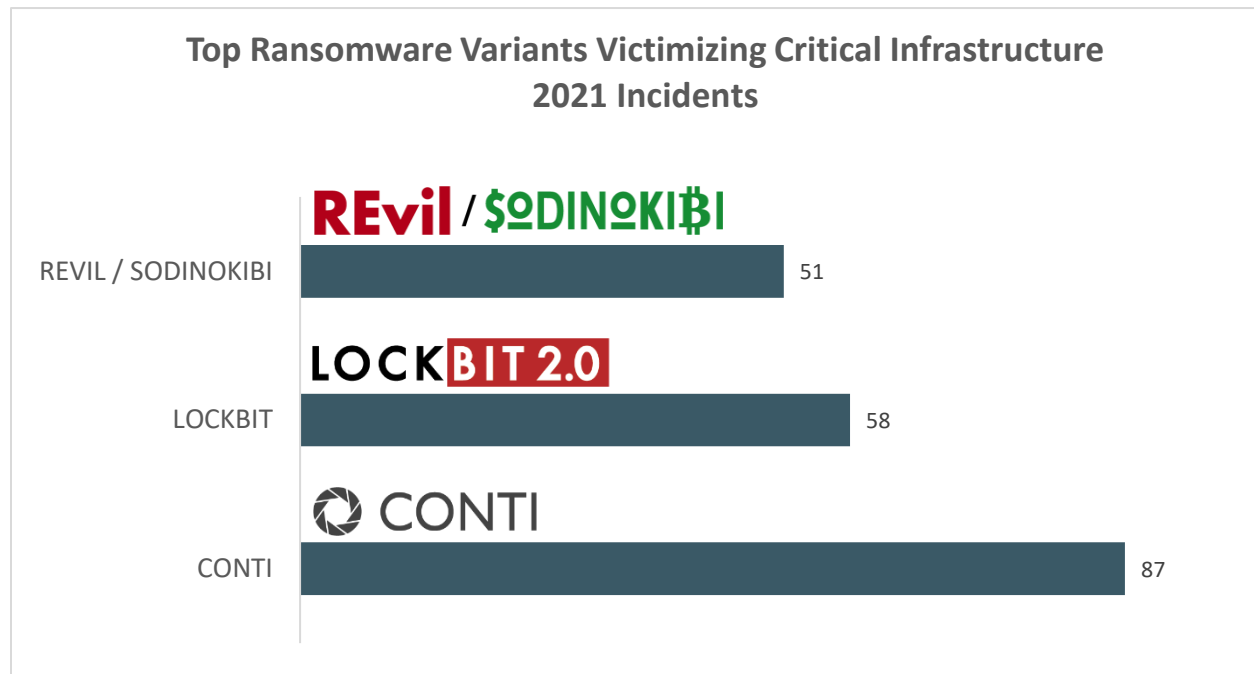
The IC3 received 649 complaints that indicated organizations belonging to a critical infrastructure sector were victims of a ransomware attack. Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 sectors had at least 1 member that fell victim to a ransomware attack in 2021.

13



¹³ Accessibility description: Chart shows Infrastructure Sectors Victimized by Ransomware. Healthcare and Public Health was highest with 148 followed by Financial Services 89; Information Technology 74; Critical Manufacturing 65; Government Facilities 60; Commercial Facilities 56; Food and Agriculture 52; Transportation 38; Energy 31; Communications 17; Chemical 12; Water and Wastewater Systems 4; Emergency Services 2; Defense Industrial Base 1.

Of the known ransomware variants reported to IC3, the three top variants that victimized a member of a critical infrastructure sector were CONTI, LockBit, and REvil/Sodinokibi.



14

According to information submitted to the IC3, CONTI most frequently victimized the Critical Manufacturing, Commercial Facilities, and Food and Agriculture sectors. LockBit most frequently victimized the Government Facilities, Healthcare and Public Health, and Financial Services sectors. REvil/Sodinokibi most frequently victimized the Financial Services, Information Technology, and Healthcare and Public Health sectors.

Of all critical infrastructure sectors reportedly victimized by ransomware in 2021, the Healthcare and Public Health, Financial Services, and Information Technology sectors were the most frequent victims. The IC3 anticipates an increase in critical infrastructure victimization in 2022.

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 FBI field office or the 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.

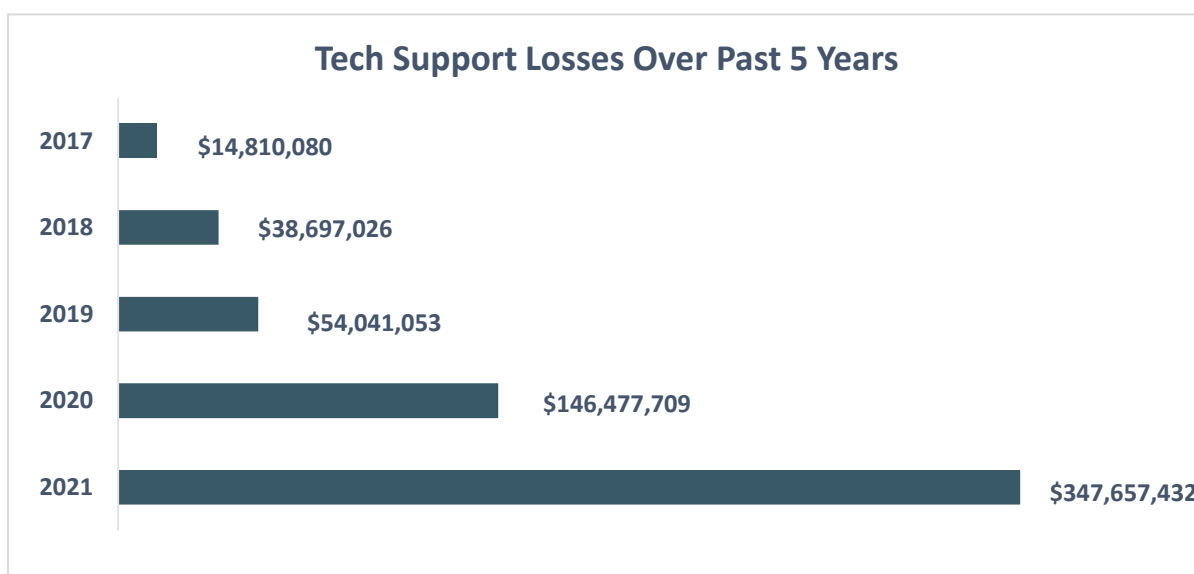
¹⁴ Accessibility description: Chart shows top variants Victimizing Critical Infrastructure 2021 Incidents. REvil/Sodinokibi, Lockbit, and CONTI.

TECH SUPPORT FRAUD¹⁵



Tech Support Fraud 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.

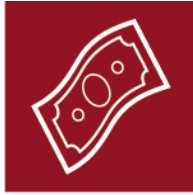
Many victims report being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards. In 2021, the IC3 received 23,903 complaints related to Tech Support Fraud from victims in 70 countries. The losses amounted to more than \$347 million, which represents a 137 percent increase in losses from 2020. Most victims, almost 60 percent, report to be over 60 years of age, and experience at least 68 percent of the losses (almost \$238 million).



Tech support scammers continue to impersonate well-known tech companies, offering to fix non-existent technology issues or renew fraudulent software or security subscriptions. However, in 2021, the IC3 observed an increase in complaints reporting the impersonation of customer support, which has taken on a variety of forms, such as financial and banking institutions, utility companies, or virtual currency exchanges.

¹⁵ Accessibility description: Chart shows Tech Support Losses Over Past 5 Years. 2021 \$347,657,432; 2020 \$146,477,709; 2019 \$54,041,053; 2018 \$38,697,026; 2017 \$14,810,080.

IC3 by the Numbers¹⁶



\$6.9 Billion

Victim losses in 2021



2,300+

Average complaints received daily



552,000+

Average complaints received per year (last 5 years)

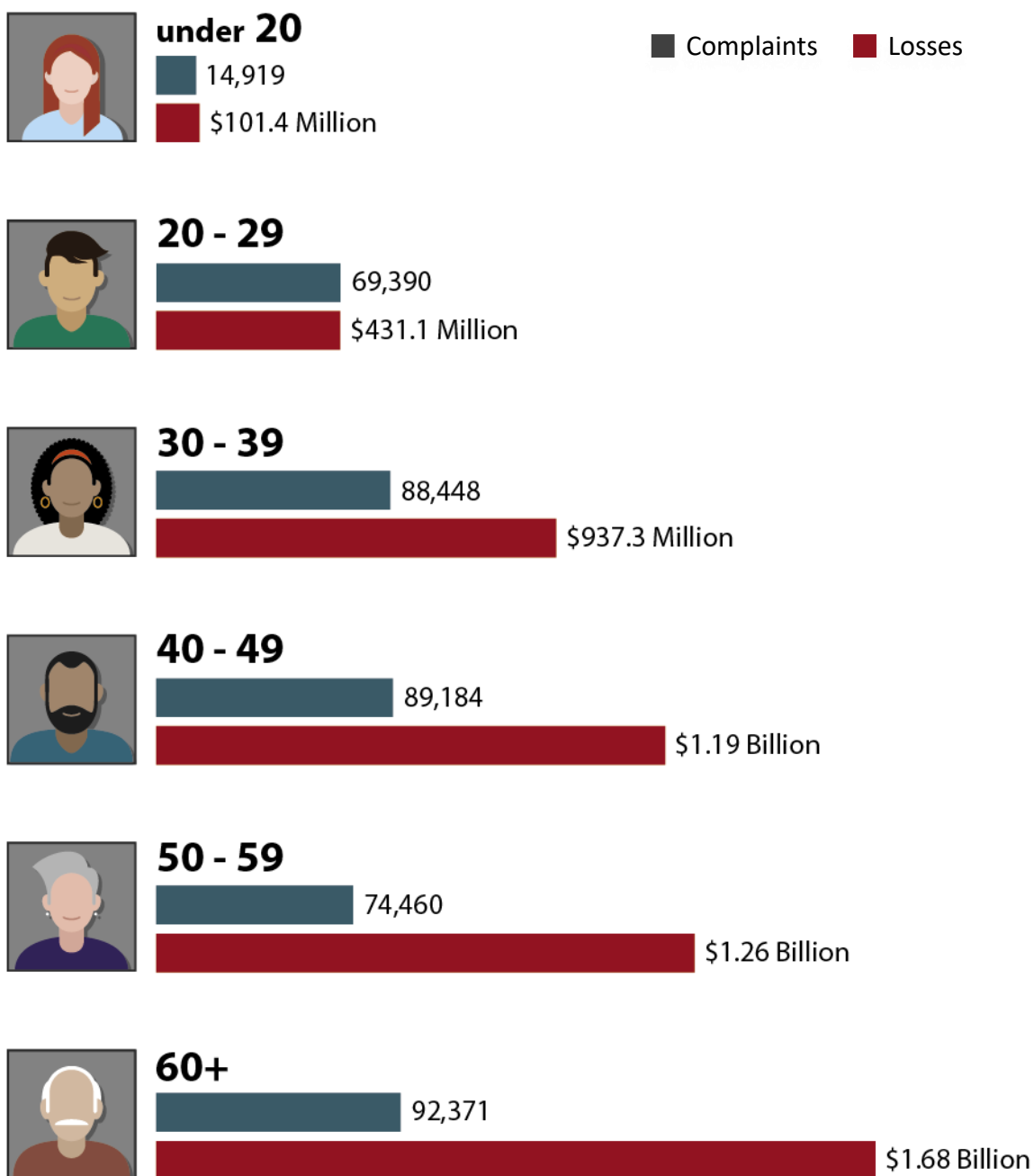


Over 6.5 Million

Complaints reported since inception

¹⁶ Accessibility description: Image depicts key statistics regarding complaints and victim loss. Total losses of \$6.9 billion were reported in 2021. The total number of complaints received since the year 2000 is over 6.5 million. IC3 has received approximately 552,000 complaints per year on average over the last five years, or more than 2,300 complaints per day.

2021 Victims by Age Group¹⁷

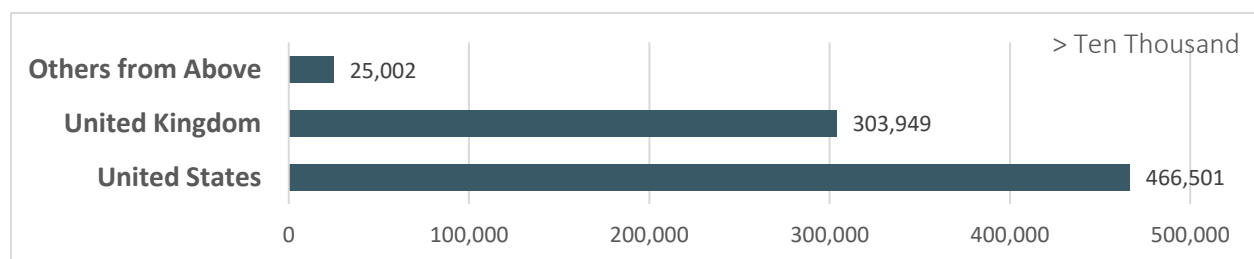
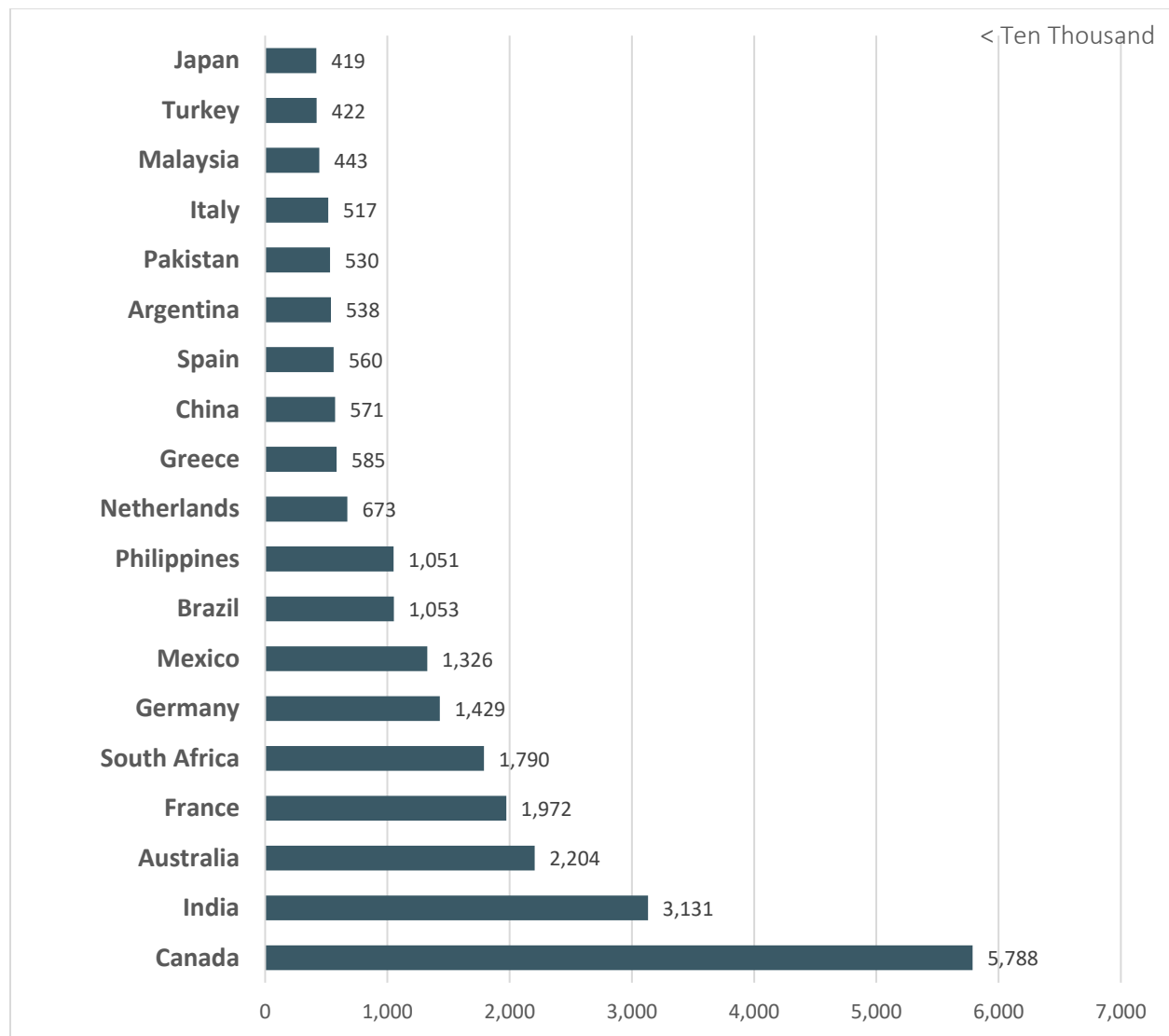


¹⁷ Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix B for more information regarding IC3 data.

Accessibility description: Chart shows number of complaints and Loss for Victims by Age Group. Under 20 14,919 victims \$101.4 Million losses; 20-29 69,390 Victims \$431.1. Million losses; 30-39 88,448 Victims \$937.3 Million losses; 40-49 89,184 victims \$1.19 Billion losses; 50-59 74,460 Victims \$1.26 Billion losses; 60+ 92,371 Victims \$1.68 Billion losses.

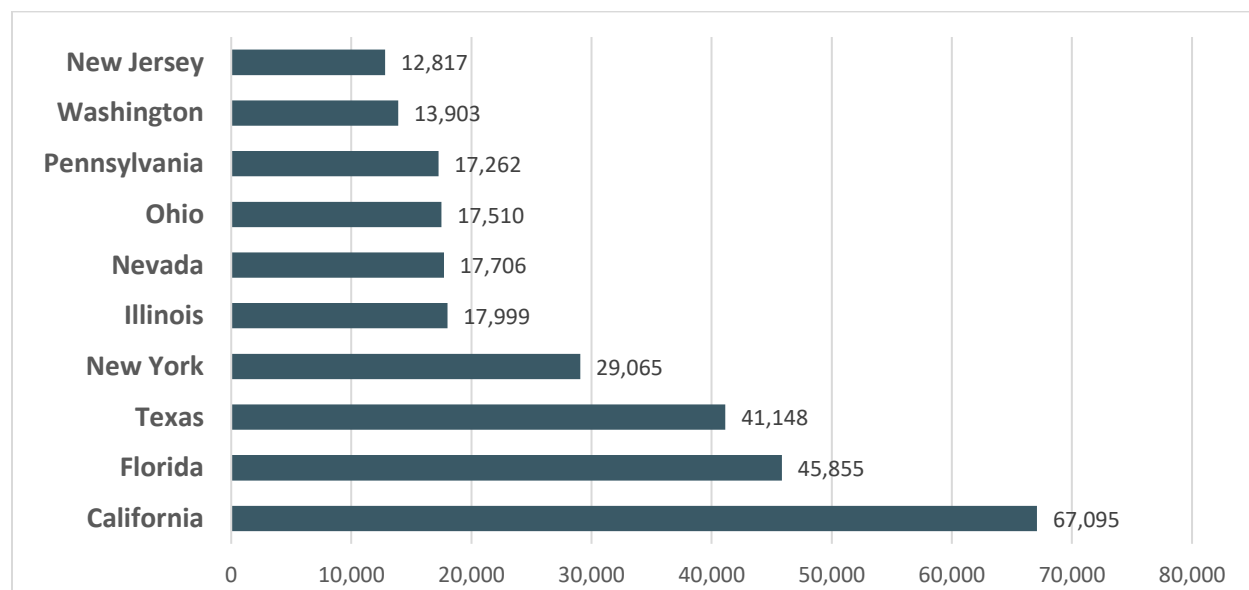
2021 - Top 20 International Victim Countries¹⁸

Compared to the United States

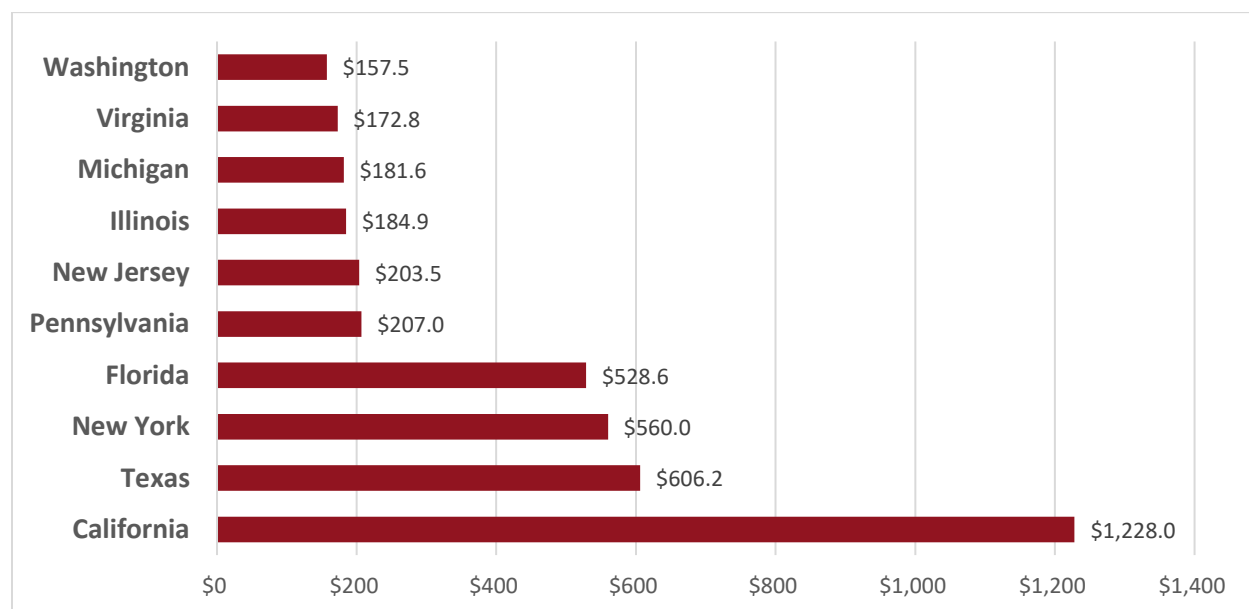


¹⁸ Accessibility description: The charts list the top 20 countries by number of total victims as compared to the United States. The specific number of victims for each country are listed in ascending order to the right of the graph. Please see Appendix B for more information regarding IC3 data.

2021 - Top 10 States by Number of Victims¹⁹



2021 - Top 10 States by Victim Loss in \$ Millions²⁰



¹⁹ Accessibility description: Chart depicts the top 10 states based on number of reporting victims are labeled. These include California, Florida, Texas, New York, Illinois, Nevada, Ohio, Pennsylvania, Washington, and New Jersey. Please see Appendix B for more information regarding IC3 data.

²⁰ Accessibility description: Chart depicts the top 10 states based on reported victim loss are labeled. These include California, Texas, New York, Florida, Pennsylvania, New Jersey, Illinois, Michigan, Virginia, and Washington. Please see Appendix B for more information regarding IC3 data.

2021 CRIME TYPES

| By Victim Count | | | |
|------------------------------------|---------|---------------------------------|---------|
| Crime Type | Victims | Crime Type | Victims |
| Phishing/Vishing/Smishing/Pharming | 323,972 | Government Impersonation | 11,335 |
| Non-Payment/Non-Delivery | 82,478 | Advanced Fee | 11,034 |
| Personal Data Breach | 51,829 | Overpayment | 6,108 |
| Identity Theft | 51,629 | Lottery/Sweepstakes/Inheritance | 5,991 |
| Extortion | 39,360 | IPR/Copyright and Counterfeit | 4,270 |
| Confidence Fraud/Romance | 24,299 | Ransomware | 3,729 |
| Tech Support | 23,903 | Crimes Against Children | 2,167 |
| Investment | 20,561 | Corporate Data Breach | 1,287 |
| BEC/EAC | 19,954 | Civil Matter | 1,118 |
| Spoofing | 18,522 | Denial of Service/TDoS | 1,104 |
| Credit Card Fraud | 16,750 | Computer Intrusion | 979 |
| Employment | 15,253 | Malware/Scareware/Virus | 810 |
| Other | 12,346 | Health Care Related | 578 |
| Terrorism/Threats of Violence | 12,346 | Re-shipping | 516 |
| Real Estate/Rental | 11,578 | Gambling | 395 |
| Descriptors* | | | |
| Social Media | 36,034 | Virtual Currency | 34,202 |

*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.

2021 Crime Types continued

| By Victim Loss | | | |
|--------------------------|-----------------|------------------------------------|-----------------|
| Crime Type | Loss | Crime Type | Loss |
| BEC/EAC | \$2,395,953,296 | Lottery/Sweepstakes/Inheritance | \$71,289,089 |
| Investment | \$1,455,943,193 | Extortion | \$60,577,741 |
| Confidence Fraud/Romance | \$956,039,740 | Ransomware | *\$49,207,908 |
| Personal Data Breach | \$517,021,289 | Employment | \$47,231,023 |
| Real Estate/Rental | \$350,328,166 | Phishing/Vishing/Smishing/Pharming | \$44,213,707 |
| Tech Support | \$347,657,432 | Overpayment | \$33,407,671 |
| Non-Payment/Non-Delivery | \$337,493,071 | Computer Intrusion | \$19,603,037 |
| Identity Theft | \$278,267,918 | IPR/Copyright/Counterfeit | \$16,365,011 |
| Credit Card Fraud | \$172,998,385 | Health Care Related | \$7,042,942 |
| Corporate Data Breach | \$151,568,225 | Malware/Scareware/Virus | \$5,596,889 |
| Government Impersonation | \$142,643,253 | Terrorism/Threats of Violence | \$4,390,720 |
| Advanced Fee | \$98,694,137 | Gambling | \$1,940,237 |
| Civil Matter | \$85,049,939 | Re-shipping | \$631,466 |
| Spoofing | \$82,169,806 | Denial of Service/TDos | \$217,981 |
| Other | \$75,837,524 | Crimes Against Children | \$198,950 |
| Descriptors** | | | |
| Social Media | \$235,279,057 | Virtual Currency | \$1,602,647,341 |

* 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.

**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.

Last 3 Year Complaint Count Comparison

| By Victim Count | ▼ ▲ = Trend from previous Year | | | |
|------------------------------------|--------------------------------|--|-----------|-----------|
| Crime Type | 2021 | | 2020 | 2019 |
| Advanced Fee | 11,034 ▼ | | 13,020 ▼ | 14,607 ▼ |
| BEC/EAC | 19,954 ▲ | | 19,369 ▼ | 23,775 ▲ |
| Civil Matter | 1,118 ▲ | | 968 ▲ | 908 ▲ |
| Confidence Fraud/Romance | 24,299 ▲ | | 23,751 ▲ | 19,473 ▲ |
| Corporate Data Breach | 1,287 ▼ | | 2,794 ▲ | 1,795 ▼ |
| Credit Card Fraud | 16,750 ▼ | | 17,614 ▲ | 14,378 ▼ |
| Crimes Against Children | 2,167 ▼ | | 3,202 ▲ | 1,312 ▼ |
| Denial of Service/TDoS | 1,104 ▼ | | 2,018 ▲ | 1,353 ▼ |
| Employment | 15,253 ▼ | | 16,879 ▲ | 14,493 ▼ |
| Extortion | 39,360 ▼ | | 76,741 ▲ | 43,101 ▼ |
| Gambling | 395 ▲ | | 391 ▲ | 262 ▲ |
| Government Impersonation | 11,335 ▼ | | 12,827 ▼ | 13,873 ▲ |
| Health Care Related | 578 ▼ | | 1,383 ▲ | 657 ▲ |
| Identity Theft | 51,629 ▲ | | 43,330 ▲ | 16,053 ▼ |
| Investment | 20,561 ▲ | | 8,788 ▲ | 3,999 ▲ |
| IPR/Copyright and Counterfeit | 4,270 ▲ | | 4,213 ▲ | 3,892 ▲ |
| Lottery/Sweepstakes/Inheritance | 5,991 ▼ | | 8,501 ▲ | 7,767 ▲ |
| Malware/Scareware/Virus | 810 ▼ | | 1,423 ▼ | 2,373 ▼ |
| Non-Payment/Non-Delivery | 82,478 ▼ | | 108,869 ▲ | 61,832 ▼ |
| Other | 12,346 ▲ | | 10,372 ▼ | 10,842 ▲ |
| Overpayment | 6,108 ▼ | | 10,988 ▼ | 15,395 ▼ |
| Personal Data Breach | 51,829 ▲ | | 45,330 ▲ | 38,218 ▼ |
| Phishing/Vishing/Smishing/Pharming | 323,972 ▲ | | 241,342 ▲ | 114,702 ▲ |
| Ransomware | 3,729 ▲ | | 2,474 ▲ | 2,047 ▲ |
| Real Estate/Rental | 11,578 ▼ | | 13,638 ▲ | 11,677 ▲ |
| Re-Shipping | 516 ▼ | | 883 ▼ | 929 ▲ |
| Spoofing | 18,522 ▼ | | 28,218 ▲ | 25,789 ▲ |
| Tech Support | 23,903 ▲ | | 15,421 ▲ | 13,633 ▼ |
| Terrorism/Threats of Violence | 12,346 ▼ | | 20,669 ▲ | 15,563 ▼ |

Last 3 Year Complaint Loss Comparison

| By Victim Loss | | ▼ ▲ = Trend from previous Year | | |
|------------------------------------|-------------------|--------------------------------|-------------------|--|
| Crime Type | 2021 | 2020 | 2019 | |
| Advanced Fee | \$98,694,137 ▲ | \$83,215,405 ▼ | \$100,602,297 ▲ | |
| BEC/EAC | \$2,395,953,296 ▲ | \$1,866,642,107 ▲ | \$1,776,549,688 ▲ | |
| Civil Matter | \$85,049,939 ▲ | \$24,915,958 ▲ | \$20,242,867 ▲ | |
| Confidence Fraud/Romance | \$956,039,739 ▲ | \$600,249,821 ▲ | \$475,014,032 ▲ | |
| Corporate Data Breach | \$151,568,225 ▲ | \$128,916,648 ▲ | \$53,398,278 ▼ | |
| Credit Card Fraud | \$172,998,385 ▲ | \$129,820,792 ▲ | \$111,491,163 ▲ | |
| Crimes Against Children | \$198,950 ▼ | \$660,044 ▼ | \$975,311 ▲ | |
| Denial of Service/TDoS | \$217,981 ▼ | \$512,127 ▼ | \$7,598,198 ▲ | |
| Employment | \$47,231,023 ▼ | \$62,314,015 ▲ | \$42,618,705 ▼ | |
| Extortion | \$60,577,741 ▼ | \$70,935,939 ▼ | \$107,498,956 ▲ | |
| Gambling | \$1,940,237 ▼ | \$3,961,508 ▲ | \$1,458,118 ▲ | |
| Government Impersonation | \$142,643,253 ▲ | \$109,938,030 ▼ | \$124,292,606 ▲ | |
| Health Care Related | \$7,042,942 ▼ | \$29,042,515 ▲ | \$1,128,838 ▼ | |
| Identity Theft | \$278,267,918 ▲ | \$219,484,699 ▲ | \$160,305,789 ▲ | |
| Investment | \$1,455,943,193 ▲ | \$336,469,000 ▲ | \$222,186,195 ▼ | |
| IPR/Copyright and Counterfeit | \$16,365,011 ▲ | \$5,910,617 ▼ | \$10,293,307 ▼ | |
| Lottery/Sweepstakes/Inheritance | \$71,289,089 ▲ | \$61,111,319 ▲ | \$48,642,332 ▼ | |
| Malware/Scareware/Virus | \$5,596,889 ▼ | \$6,904,054 ▲ | \$2,009,119 ▼ | |
| Non-Payment/Non-Delivery | \$337,493,071 ▲ | \$265,011,249 ▲ | \$196,563,497 ▲ | |
| Other | \$75,837,524 ▼ | \$101,523,082 ▲ | \$66,223,160 ▲ | |
| Overpayment | \$33,407,671 ▼ | \$51,039,922 ▼ | \$55,820,212 ▲ | |
| Personal Data Breach | \$517,021,289 ▲ | \$194,473,055 ▲ | \$120,102,501 ▼ | |
| Phishing/Vishing/Smishing/Pharming | \$44,213,707 ▼ | \$54,241,075 ▼ | \$57,836,379 ▲ | |
| Ransomware | \$49,207,908 ▲ | \$29,157,405 ▲ | \$8,965,847 ▲ | |
| Real Estate/Rental | \$350,328,166 ▲ | \$213,196,082 ▼ | \$221,365,911 ▲ | |
| Re-Shipping | \$631,466 ▼ | \$3,095,265 ▲ | \$1,772,692 ▲ | |
| Spoofing | \$82,169,806 ▼ | \$216,513,728 ▼ | \$300,478,433 ▲ | |
| Tech Support | \$347,657,432 ▲ | \$146,477,709 ▲ | \$54,041,053 ▲ | |
| Terrorism/Threats of Violence | \$4,390,720 ▼ | \$6,547,449 ▼ | \$19,916,243 ▲ | |

Overall State Statistics

| Victim per State* | | | | | |
|-------------------|----------------|---------|------|-----------------------------|---------|
| Rank | State | Victims | Rank | State | Victims |
| 1 | California | 67,095 | 30 | Louisiana | 4,248 |
| 2 | Florida | 45,855 | 31 | Utah | 4,242 |
| 3 | Texas | 41,148 | 32 | Oklahoma | 4,156 |
| 4 | New York | 29,065 | 33 | Arkansas | 2,745 |
| 5 | Illinois | 17,999 | 34 | Kansas | 2,693 |
| 6 | Nevada | 17,706 | 35 | New Mexico | 2,644 |
| 7 | Ohio | 17,510 | 36 | Nebraska | 2,407 |
| 8 | Pennsylvania | 17,262 | 37 | Mississippi | 2,170 |
| 9 | Washington | 13,903 | 38 | West Virginia | 2,135 |
| 10 | New Jersey | 12,817 | 39 | Delaware | 2,132 |
| 11 | Arizona | 12,375 | 40 | District of Columbia | 2,103 |
| 12 | Virginia | 11,785 | 41 | Puerto Rico | 1,923 |
| 13 | Georgia | 11,776 | 42 | Idaho | 1,882 |
| 14 | Maryland | 11,693 | 43 | Alaska | 1,787 |
| 15 | Indiana | 11,399 | 44 | Hawaii | 1,615 |
| 16 | Michigan | 10,930 | 45 | New Hampshire | 1,487 |
| 17 | Colorado | 10,537 | 46 | Maine | 1,402 |
| 18 | North Carolina | 10,363 | 47 | Rhode Island | 1,205 |
| 19 | Missouri | 9,692 | 48 | Montana | 1,188 |
| 20 | Massachusetts | 9,174 | 49 | South Dakota | 951 |
| 21 | Iowa | 8,853 | 50 | Wyoming | 735 |
| 22 | Wisconsin | 8,646 | 51 | Vermont | 715 |
| 23 | Kentucky | 7,148 | 52 | North Dakota | 670 |
| 24 | Tennessee | 7,129 | 53 | Virgin Islands, U.S. | 100 |
| 25 | Oregon | 5,954 | 54 | U.S. Minor Outlying Islands | 93 |
| 26 | Minnesota | 5,844 | 55 | Guam | 64 |
| 27 | South Carolina | 5,426 | 56 | Northern Mariana Islands | 29 |
| 28 | Alabama | 5,347 | 57 | American Samoa | 25 |
| 29 | Connecticut | 4,524 | | | |

*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.

Overall State Statistics continued

| Total Victim Losses by State* | | | | | |
|-------------------------------|----------------|-----------------|------|-----------------------------|--------------|
| Rank | State | Loss | Rank | State | Loss |
| 1 | California | \$1,227,989,139 | 30 | Louisiana | \$38,783,908 |
| 2 | Texas | \$606,179,646 | 31 | Kentucky | \$37,953,949 |
| 3 | New York | \$559,965,598 | 32 | Iowa | \$33,821,569 |
| 4 | Florida | \$528,573,929 | 33 | Kansas | \$26,031,546 |
| 5 | Pennsylvania | \$206,982,032 | 34 | North Dakota | \$21,246,355 |
| 6 | New Jersey | \$203,510,341 | 35 | Mississippi | \$20,578,948 |
| 7 | Illinois | \$184,860,704 | 36 | District of Columbia | \$20,096,921 |
| 8 | Michigan | \$181,622,993 | 37 | Nebraska | \$19,743,241 |
| 9 | Virginia | \$172,767,012 | 38 | Hawaii | \$18,964,018 |
| 10 | Washington | \$157,454,331 | 39 | South Dakota | \$18,131,095 |
| 11 | Massachusetts | \$150,384,982 | 40 | Idaho | \$17,682,386 |
| 12 | Georgia | \$143,998,767 | 41 | Arkansas | \$15,302,829 |
| 13 | Ohio | \$133,666,156 | 42 | New Hampshire | \$15,302,618 |
| 14 | Colorado | \$130,631,286 | 43 | Delaware | \$15,041,717 |
| 15 | Arizona | \$124,158,717 | 44 | Puerto Rico | \$14,650,062 |
| 16 | Tennessee | \$103,960,100 | 45 | Alaska | \$13,070,648 |
| 17 | Maryland | \$99,110,757 | 46 | New Mexico | \$12,761,850 |
| 18 | North Carolina | \$91,416,226 | 47 | Rhode Island | \$11,191,079 |
| 19 | Nevada | \$83,712,410 | 48 | Wyoming | \$10,249,609 |
| 20 | Minnesota | \$82,535,103 | 49 | Montana | \$10,107,283 |
| 21 | Oregon | \$75,739,646 | 50 | Vermont | \$9,826,787 |
| 22 | Connecticut | \$72,476,672 | 51 | West Virginia | \$9,453,607 |
| 23 | Utah | \$65,131,003 | 52 | Maine | \$7,261,234 |
| 24 | Indiana | \$60,524,818 | 53 | Guam | \$2,168,956 |
| 25 | Missouri | \$53,797,188 | 54 | Virgin Islands, U.S. | \$895,946 |
| 26 | Wisconsin | \$51,816,862 | 55 | Northern Mariana Islands | \$705,244 |
| 27 | Oklahoma | \$50,196,339 | 56 | U.S. Minor Outlying Islands | \$403,844 |
| 28 | Alabama | \$49,522,904 | 57 | American Samoa | \$177,533 |
| 29 | South Carolina | \$42,768,322 | | | |

*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.

Overall State Statistics continued

| Count by Subject per State* | | | | | |
|-----------------------------|----------------|----------|------|-----------------------------|----------|
| Rank | State | Subjects | Rank | State | Subjects |
| 1 | California | 27,706 | 30 | Nebraska | 1,243 |
| 2 | Texas | 13,518 | 31 | Kentucky | 1,238 |
| 3 | Florida | 11,527 | 32 | District of Columbia | 1,107 |
| 4 | New York | 10,696 | 33 | Utah | 1,063 |
| 5 | Maryland | 5,244 | 34 | Delaware | 924 |
| 6 | Ohio | 5,182 | 35 | New Mexico | 893 |
| 7 | Pennsylvania | 5,168 | 36 | Kansas | 876 |
| 8 | Illinois | 4,587 | 37 | West Virginia | 863 |
| 9 | Georgia | 4,521 | 38 | Arkansas | 831 |
| 10 | New Jersey | 3,913 | 39 | Iowa | 723 |
| 11 | Washington | 3,586 | 40 | Mississippi | 714 |
| 12 | Virginia | 3,542 | 41 | Montana | 681 |
| 13 | Arizona | 3,485 | 42 | Maine | 507 |
| 14 | North Carolina | 3,316 | 43 | Idaho | 486 |
| 15 | Nevada | 3,308 | 44 | New Hampshire | 467 |
| 16 | Colorado | 2,885 | 45 | Hawaii | 435 |
| 17 | Michigan | 2,605 | 46 | Alaska | 429 |
| 18 | Tennessee | 2,384 | 47 | Puerto Rico | 346 |
| 19 | Massachusetts | 2,018 | 48 | Rhode Island | 318 |
| 20 | Indiana | 1,976 | 49 | North Dakota | 297 |
| 21 | Oklahoma | 1,929 | 50 | Wyoming | 251 |
| 22 | Missouri | 1,646 | 51 | South Dakota | 216 |
| 23 | Oregon | 1,598 | 52 | Vermont | 189 |
| 24 | Minnesota | 1,553 | 53 | U.S. Minor Outlying Islands | 34 |
| 25 | Alabama | 1,520 | 54 | Virgin Islands, U.S. | 14 |
| 26 | Connecticut | 1,499 | 55 | Guam | 11 |
| 27 | Louisiana | 1,398 | 56 | Northern Mariana Islands | 7 |
| 28 | South Carolina | 1,358 | 57 | American Samoa | 3 |
| 29 | Wisconsin | 1,316 | | | |

*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.

Overall State Statistics continued

| Subject Earnings per Destination State* | | | | | |
|---|----------------------|---------------|------|-----------------------------|--------------|
| Rank | State | Loss | Rank | State | Loss |
| 1 | California | \$404,965,496 | 30 | South Carolina | \$10,406,812 |
| 2 | New York | \$320,011,292 | 31 | Iowa | \$7,960,272 |
| 3 | Florida | \$174,884,203 | 32 | Wyoming | \$7,007,308 |
| 4 | Texas | \$168,153,129 | 33 | Idaho | \$6,879,088 |
| 5 | Colorado | \$96,949,691 | 34 | Connecticut | \$6,586,016 |
| 6 | Illinois | \$82,985,601 | 35 | Kansas | \$6,527,306 |
| 7 | Ohio | \$65,567,505 | 36 | New Mexico | \$6,441,444 |
| 8 | Georgia | \$62,682,196 | 37 | Kentucky | \$6,260,280 |
| 9 | Washington | \$49,643,646 | 38 | Arkansas | \$5,511,079 |
| 10 | New Jersey | \$46,773,594 | 39 | Delaware | \$5,404,683 |
| 11 | Nevada | \$46,441,562 | 40 | Hawaii | \$5,312,553 |
| 12 | Pennsylvania | \$44,661,540 | 41 | Nebraska | \$5,156,069 |
| 13 | Arizona | \$44,490,075 | 42 | New Hampshire | \$5,082,033 |
| 14 | Louisiana | \$43,427,842 | 43 | Mississippi | \$4,245,861 |
| 15 | North Carolina | \$43,281,815 | 44 | Puerto Rico | \$4,067,734 |
| 16 | Virginia | \$42,989,608 | 45 | Maine | \$3,445,411 |
| 17 | Maryland | \$33,912,104 | 46 | Vermont | \$3,357,692 |
| 18 | Massachusetts | \$29,327,619 | 47 | Rhode Island | \$3,307,726 |
| 19 | Michigan | \$28,857,054 | 48 | North Dakota | \$3,174,006 |
| 20 | Oklahoma | \$19,278,395 | 49 | Montana | \$2,946,504 |
| 21 | Minnesota | \$19,039,734 | 50 | Alaska | \$2,773,302 |
| 22 | Tennessee | \$18,580,987 | 51 | South Dakota | \$2,413,398 |
| 23 | Utah | \$17,137,321 | 52 | West Virginia | \$2,269,994 |
| 24 | Missouri | \$16,619,864 | 53 | Northern Mariana Islands | \$107,000 |
| 25 | District of Columbia | \$15,656,649 | 54 | U.S. Minor Outlying Islands | \$77,350 |
| 26 | Wisconsin | \$14,886,212 | 55 | Virgin Islands, U.S. | \$44,453 |
| 27 | Alabama | \$14,639,799 | 56 | Guam | \$3,932 |
| 28 | Indiana | \$14,634,699 | 57 | American Samoa | \$420 |
| 29 | Oregon | \$10,561,887 | | | |

*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

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.

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.

Computer Intrusion: Unauthorized access or exceeding authorized access into a protected computer system. A protected computer system is one owned or used by the US Government, a financial institution, or any business. This typically excludes personally owned systems and devices.

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 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.

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 based on 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.

Non-Payment/Non-Delivery: Goods or services are shipped, and payment is never rendered (non-payment). Payment is sent, and goods or services are never received, or are of lesser quality (non-delivery).

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.

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/Threats of Violence: Terrorism is 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. 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.

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.