



FEDERAL BUREAU of INVESTIGATION Internet Crime Report 2023



INTERNET CRIME COMPLAINT CENTER

CONTENTS

| | |
|--|----|
| INTRODUCTION | 3 |
| THE IC3 | 3 |
| THE IC3's ROLE IN COMBATTING CYBER CRIME | 5 |
| IC3 CORE FUNCTIONS | 6 |
| IC3 COMPLAINT STATISTICS | 7 |
| LAST FIVE YEARS | 7 |
| TOP FIVE CRIME TYPE COMPARISON | 8 |
| THE IC3 RECOVERY ASSET TEAM (RAT) | 9 |
| RAT SUCCESSES | 10 |
| 2023 OVERVIEW | 11 |
| BUSINESS EMAIL COMPROMISE (BEC)..... | 11 |
| INVESTMENT..... | 12 |
| RANSOMWARE | 13 |
| TECH/CUSTOMER SUPPORT AND GOVERNMENT IMPERSONATION | 15 |
| IC3 BY THE NUMBERS..... | 16 |
| 2023 - COMPLAINANTS BY AGE GROUP | 17 |
| 2023 - TOP 20 INTERNATIONAL COMPLAINT COUNTRIES | 18 |
| 2023 - TOP 10 STATES BY NUMBER OF COMPLAINTS | 19 |
| 2023 - TOP 10 STATES BY LOSS (IN MILLIONS) | 19 |
| 2023 CRIME TYPES | 20 |
| 2023 CRIME TYPES <i>continued</i> | 21 |
| LAST-THREE-YEAR COMPLAINT COUNT COMPARISON | 22 |
| LAST-THREE-YEAR COMPLAINT LOSS COMPARISON | 23 |
| OVERALL STATE STATISTICS..... | 24 |
| OVERALL STATE STATISTICS <i>continued</i> | 25 |
| OVERALL STATE STATISTICS <i>continued</i> | 26 |
| OVERALL STATE STATISTICS <i>continued</i> | 27 |
| OVERALL STATE STATISTICS <i>continued</i> | 28 |
| OVERALL STATE STATISTICS <i>continued</i> | 29 |
| APPENDIX A: DEFINITIONS..... | 30 |
| APPENDIX B: ADDITIONAL INFORMATION ABOUT IC3 DATA | 33 |
| APPENDIX C: PUBLIC SERVICE ANNOUNCEMENTS PUBLISHED | 34 |

INTRODUCTION

Dear Reader,

Today's cyber landscape is threatened by a multitude of malicious actors who have the tools to conduct large-scale fraud schemes, hold our money and data for ransom, and endanger our national security. Profit-driven cybercriminals and nation-state adversaries alike have the capability to paralyze entire school systems, police departments, healthcare facilities, and individual private sector entities. The FBI continues to combat this evolving cyber threat. Our strategy focuses on building strong partnerships with the private sector; removing threats from US networks; pulling back the cloak of anonymity many of these actors hide behind; and hitting cybercriminals where it hurts: their wallets, including their virtual wallets.

Critical to the FBI's efforts is the Internet Crime Complaint Center (IC3). IC3 gives the public a direct way to report cybercrime to the FBI and enables us to collect data, advance investigations, and identify changes in the threat landscape. In 2023, IC3 received a record number of complaints from the American public: 880,418 complaints were registered, with potential losses exceeding \$12.5 billion. This is a nearly 10% increase in complaints received, and it represents a 22% increase in losses suffered, compared to 2022. As impressive as these figures appear, we know they are conservative regarding cybercrime in 2023. Consider that when the FBI recently infiltrated the Hive ransomware group's infrastructure, we found that only about 20% of Hive's victims reported to law enforcement. More reporting from victims would mean superior insight for the FBI.

The past year, investment fraud was once again the costliest type of crime tracked by IC3. Losses to investment scams rose from \$3.31 billion in 2022 to \$4.57 billion in 2023—a 38% increase. The second-costliest type of crime was business e-mail compromise (BEC), with 21,489 complaints amounting to \$2.9 billion in reported losses. Tech support scams, meanwhile, were the third-costliest type of crime tracked by IC3. Notably, different age groups tended to be impacted by different crimes. Victims 30 to 49 years old were the most likely group to report losses from investment fraud, while the elderly accounted for well over half of losses to tech support scams.

In 2023, ransomware incidents continued to be impactful and costly. After a brief downturn in 2022, ransomware incidents were again on the rise with over 2,825 complaints. This represents an increase of 18% from 2022. Reported losses rose 74%, from \$34.3 million to \$59.6 million. Cybercriminals continue to adjust their tactics, and the FBI has observed emerging ransomware trends, such as the deployment of multiple ransomware variants against the same victim and the use of data-destruction tactics to increase pressure on victims to negotiate.

Last year also saw notable achievements for law enforcement. The FBI's commitment to assisting cyber victims and fostering partnerships allowed for the continued success of IC3's Recovery Asset Team (RAT). Established in 2018, RAT streamlines communications with financial institutions and FBI field offices to facilitate the freezing of funds for victims. In 2023, IC3's RAT initiated the Financial Fraud Kill Chain (FFKC) on 3,008 incidents, with potential losses of \$758.05 million. A monetary hold was placed on \$538.39 million, representing a success rate of 71%.

As the cyber threat continues to evolve, the FBI remains appreciative of those who report cyber incidents to IC3. Information reported to the FBI helps advance our investigations. Your reporting is critical for our efforts to pursue adversaries, share intelligence with our partners, and protect your fellow citizens. Cybersecurity is the ultimate team sport, and we are in this fight together. The FBI is committed to fostering greater security in a digitally connected world, and we are eager to work with the American public to defeat cyber adversaries and bring criminals to justice.

Timothy Langan
Executive Assistant 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 which are increasingly emanating from our digitally connected world. To do that, the FBI leverages the IC3 as a mechanism to gather intelligence on internet crime so that we can provide the public and our many partners with information, services, support, training, and leadership to stay ahead of the threat.

The IC3 was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (Hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet-facilitated crimes. As of December 31, 2023, the IC3 has received over eight million complaints. The IC3's mission is to provide the public and our partners with a reliable and convenient reporting mechanism to submit information 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 public awareness.

The information submitted to the IC3 can be impactful in the individual complaints, but it is most impactful in the aggregate. That is, when the individual complaints are combined with other data, it allows the FBI to connect complaints, investigate reported crimes, track trends and threats, and, in some cases, even freeze stolen funds. Just as importantly, the IC3 shares reports of crime throughout its vast network of FBI field offices and law enforcement partners, strengthening our nation's collective response both locally and nationally.

To promote public awareness and as part of its prevention mission, the IC3 aggregates the submitted data and produces an annual report on the trends impacting the public as well as routinely providing intelligence reports about trends. The success of these efforts is directly related to the quality of the data submitted by the public through the www.ic3.gov interface. Their efforts help the IC3, and the FBI better protect their fellow citizens.



THE IC3'S ROLE IN COMBATting CYBER CRIME¹



¹ Accessibility description: Image lists the IC3's primary functions including partnering with private sector and with local, state, federal, and international agencies; hosting a 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

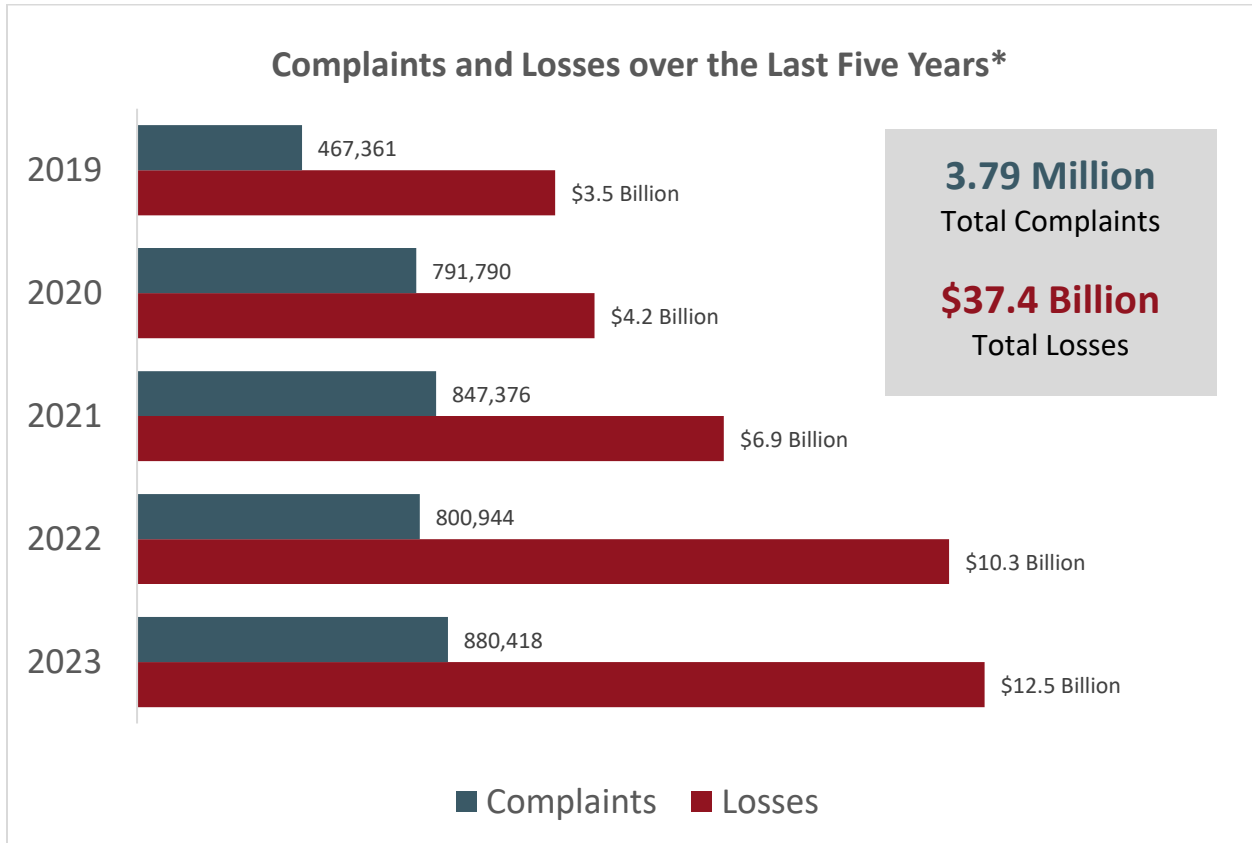


² Accessibility description: Image contains icons with the core functions. Core functions - Collection, Analysis, Public Awareness, and Referrals - are listed in individual blocks as components of an ongoing process.

IC3 COMPLAINT STATISTICS

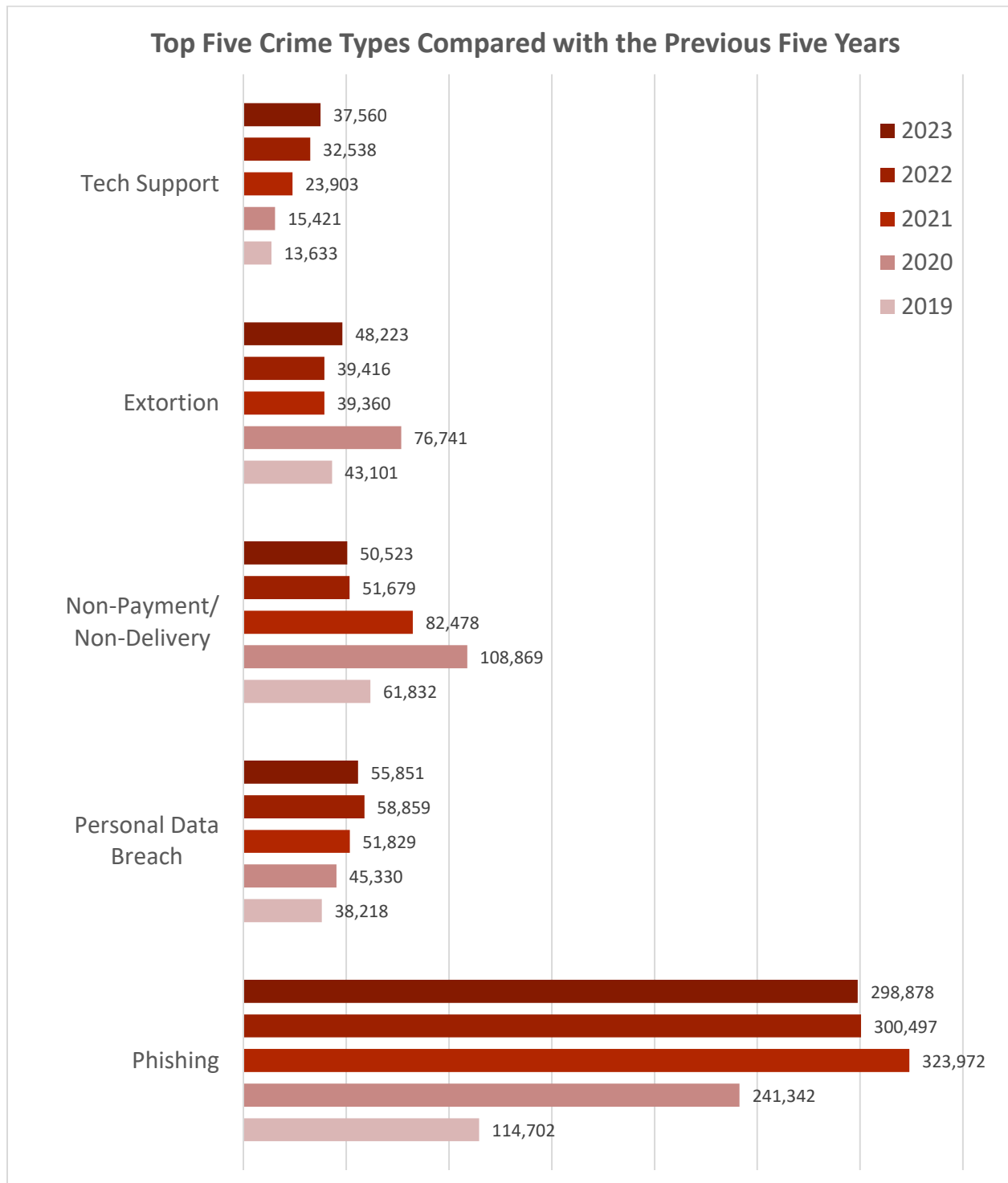
LAST FIVE YEARS

Over the last five years, the IC3 has received an average of 758,000 complaints per year. These complaints address a wide array of Internet scams affecting individuals across the globe.³



³ Accessibility description: Chart includes yearly and aggregate data for complaints and losses over the years 2019 to 2023. Over this time, the IC3 received a total of 3.79 million complaints, reporting a loss of \$37.5 billion. * Please see Appendix B for more information regarding IC3 data.

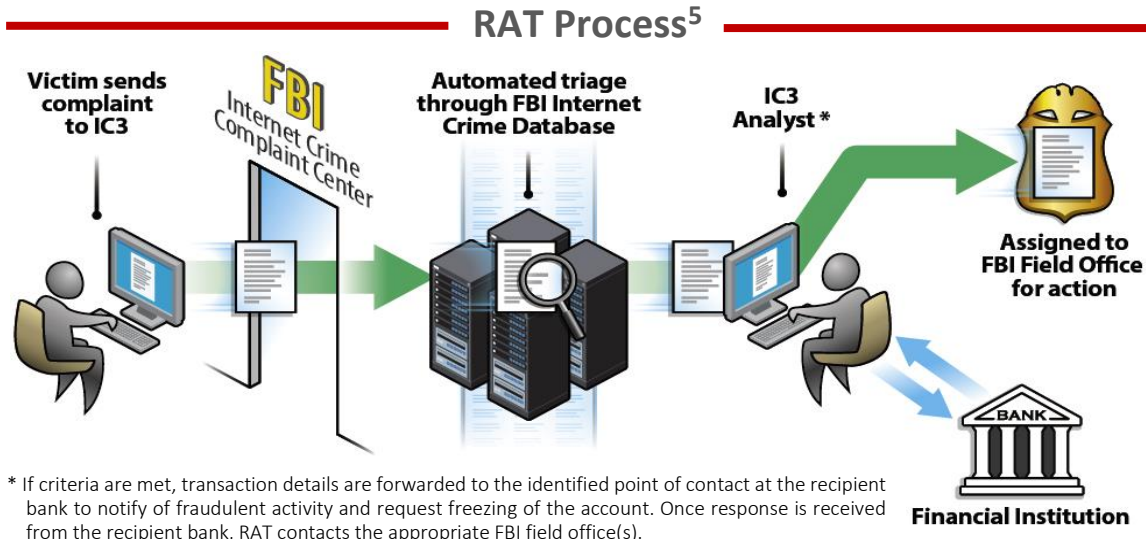
TOP FIVE CRIME TYPE COMPARISON⁴



⁴ Accessibility description: Chart includes a loss comparison for the top five reported crime types for the years of 2019 to 2023.

THE IC3 RECOVERY ASSET TEAM (RAT)

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 those 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

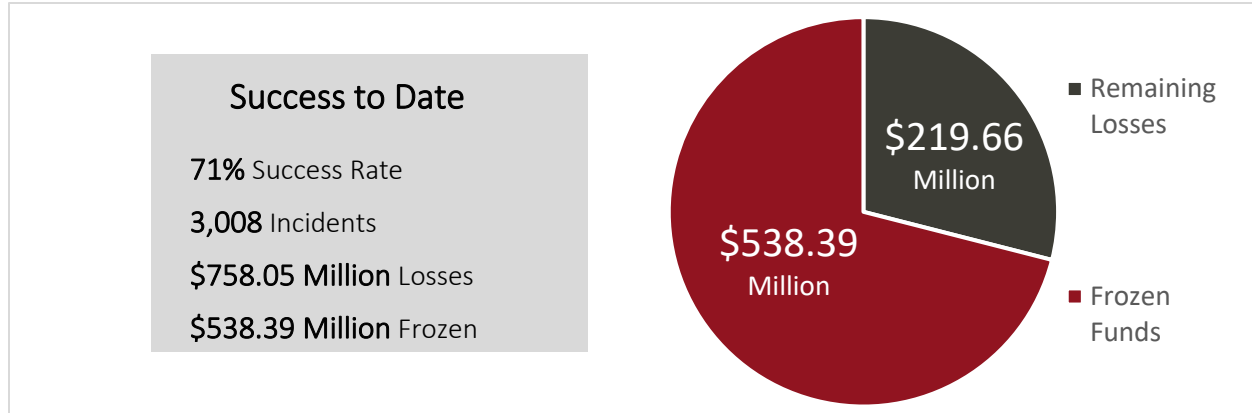
- Assist in the identification of potentially fraudulent accounts across the sector.
- Remain at the forefront of emerging trends among financial fraud schemes.
- Foster a symbiotic relationship in which information is appropriately shared.

Guidance for Complainants who send Wire Transfers

- 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.
- 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 two examples of the RAT's successful contributions to investigative and recovery efforts:

New York

In March of 2023, the IC3 received a complaint filed by a critical infrastructure construction project entity located in New York, New York area of a \$50,000,000 loss due to a BEC incident. The RAT immediately sent the Financial Fraud Kill Chain (FFKC) request to the recipient financial institution and was advised that \$44,936,460 was frozen in the account. Second-hop information was provided by the recipient financial institution, and the RAT pursued the secondary wires to two additional recipient financial institutions. FFKC responses from the second wires reported a frozen amount of an additional \$1,008,526.

Connecticut

In March 2023, the IC3 received a complaint filed by an individual located in the Stamford, Connecticut area of a BEC related to a real estate transaction. The individual was in the process of purchasing a home and received a spoofed email from their supposed attorney instructing them to wire \$426,000.00 to a financial institution to finalize the closing. Two days after the wire was initiated, it was realized the instructions came from a spoofed email. Upon notification, the IC3 RAT immediately initiated the FFKC process to freeze the fraudulent recipient financial bank account. Collaboration with the domestic recipient financial institution and the local police department confirmed \$425,000.00 was frozen and returned to the individual which enabled them to complete the real estate transaction.

⁶ Accessibility description: Image shows Success to Date to include 71% Success Rate; 3,008 Incidents; \$758.05 Million in Losses; and \$538.39 Million Frozen.

2023 OVERVIEW

BUSINESS EMAIL COMPROMISE (BEC)



In 2023, the IC3 received 21,489 BEC complaints with adjusted losses over 2.9 billion. BEC 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.

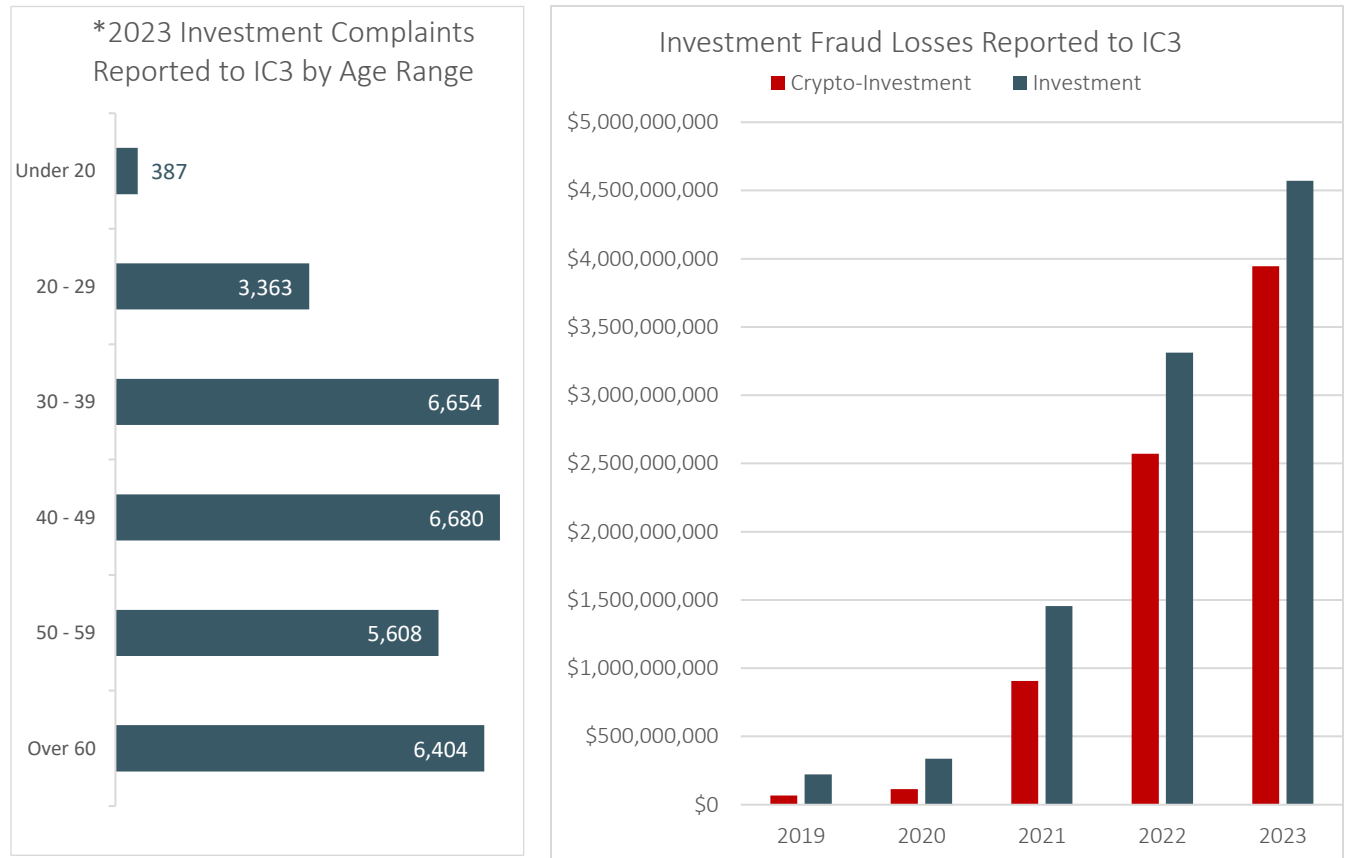
These BEC schemes historically involved compromised vendor emails, requests for W-2 information, targeting of the real estate sector, and fraudulent requests for large amounts of gift cards. More recently, the IC3 data suggests fraudsters are increasingly using custodial accounts held at financial institutions for cryptocurrency exchanges or third-party payment processors, or having targeted individuals send funds directly to these platforms where funds are quickly dispersed.

With these increased tactics of funds going directly to cryptocurrency platforms and third-party payment processors or through a custodial account held at a financial institution, it emphasizes the importance of leveraging two-factor or multi-factor authentication as an additional security layer. Procedures should be put in place to verify payments and purchase requests outside of email communication and can include direct phone calls but to a known verified number and not relying on information or phone numbers included in the email communication. Other best practices include carefully examining the email address, URL, and spelling used in any correspondence and not clicking on anything in an unsolicited email or text message asking you to update or verify account information.

INVESTMENT



In 2023, the losses reported due to Investment scams became the most of any crime type tracked by the IC3. Investment fraud losses rose from \$3.31 billion in 2022 to \$4.57 billion in 2023, a 38% increase. Within these numbers, investment fraud with a reference to cryptocurrency rose from \$2.57 billion in 2022 to \$3.96 billion in 2023, an increase of 53%. These scams are designed to entice those targeted with the promise of lucrative returns on their investments.^{7,8}



**Does not include complainants that did not provide an age range.*

IC3 publications in 2023 Related to Investment Fraud

- [The FBI Warns of a Spike in Cryptocurrency Investment Schemes](#)
- [FBI Guidance for Cryptocurrency Scam Victims](#)
- [Increase in Companies Falsely Claiming an Ability to Recover Funds Lost in Cryptocurrency Investment Scams](#)
- [Criminals Pose as Non-Fungible Token \(NFT\) Developers to Target Internet Users with an Interest in NFT Acquisition](#)

⁷ Accessibility description: 2023 Investment Complaints Reported to IC3 by Age Range.

⁸ Accessibility description: Chart shows Investment Fraud Losses Reported to the IC3 by Year for 2019 to 2023.

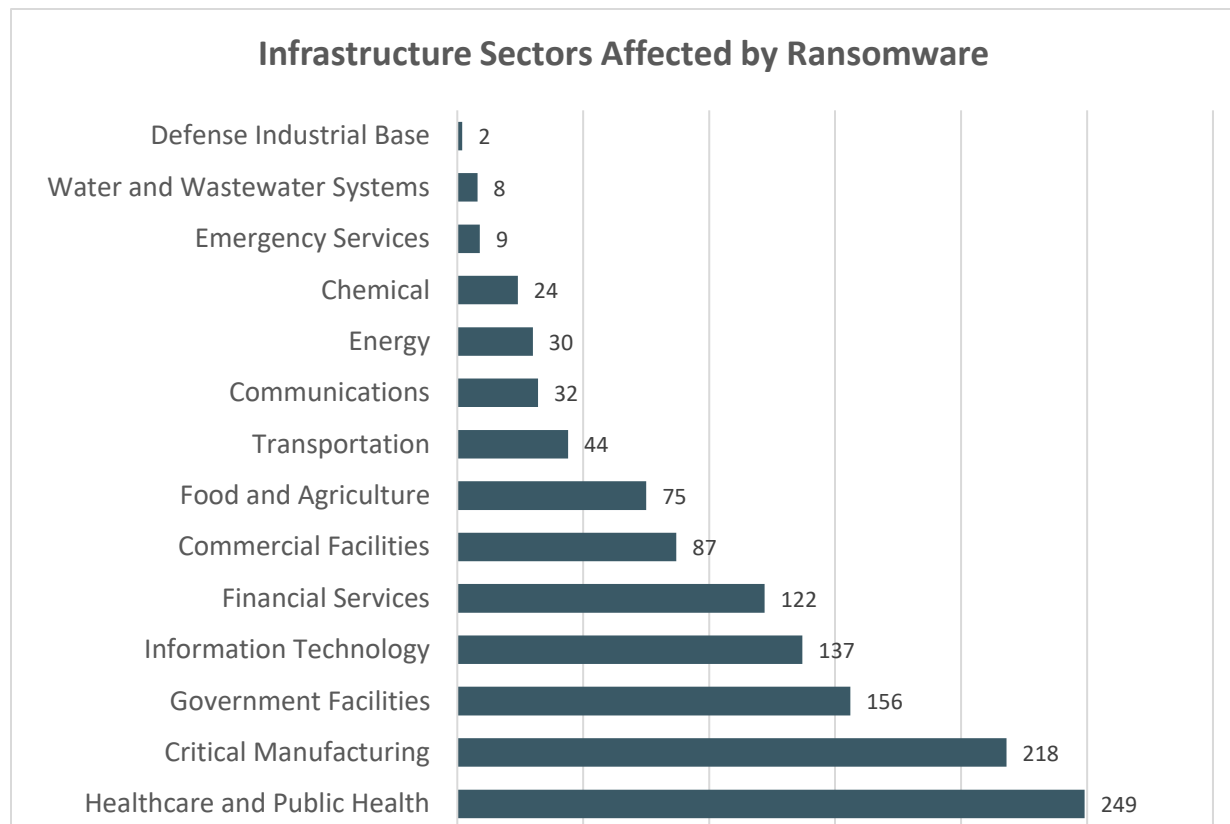
RANSOMWARE



In 2023, the IC3 received 2,825 complaints identified as ransomware with adjusted losses of more than \$59.6 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. In addition to encrypting the network, the cyber-criminal will often steal data off the system and hold that data hostage until the ransom is paid. If the ransom is not paid, the entity’s data remains unavailable.

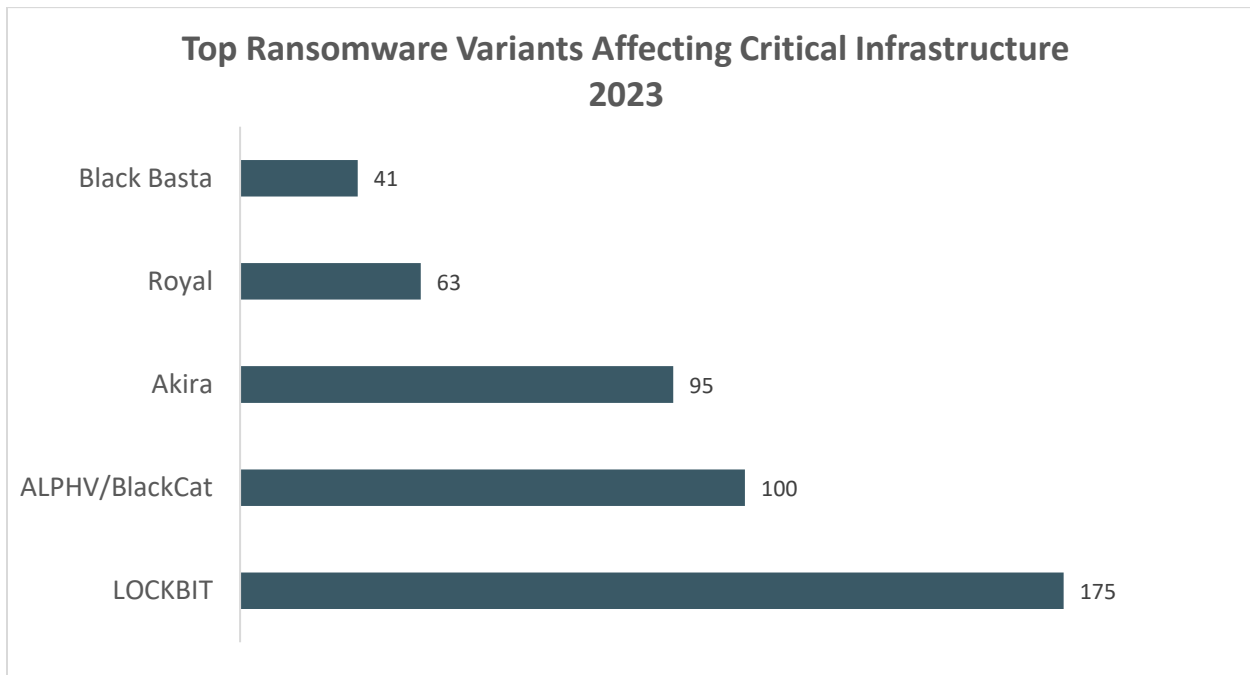
Ransomware and Critical Infrastructure Sectors

The IC3 received 1,193 complaints from organizations belonging to a critical infrastructure sector that were affected by a ransomware attack. Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 sectors had at least 1 member that fell to a ransomware attack in 2023.⁹



⁹ Accessibility description: Chart shows Infrastructure Sectors Affected by Ransomware. Healthcare and Public Health was highest with 249; followed by Critical Manufacturing 218; Government Facilities 156; Information Technology 137; Financial Services 122; Commercial Facilities 87; Food and Agriculture 75; Transportation 44; Communications 32; Energy 30; Chemical 24; Emergency Services 9; Water and Wastewater Systems 8; Defense Industrial Base 2.

The five top ransomware variants reported to the IC3 that affected a member of a critical infrastructure sector were Lockbit, ALPHV/Blackcat, Akira, Royal, and Black Basta.¹⁰



Incident reporting

Ransomware infections impact individual users and businesses regardless of size or industry by causing service disruptions, financial loss, and in some cases, permanent loss of valuable data. While ransomware infection statistics are often highlighted in the media and by computer security companies, it has been challenging for the FBI to ascertain the true number of ransomware victims as many infections go unreported to law enforcement. By reporting the incident, the FBI may be able to provide information on decryption, recover stolen data, possibly seize/recover ransom payments, and gain insight on adversary tactics. Ultimately, the information you provide will lead us to bring the perpetrators to justice.

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 an entity's files will be recovered. Regardless of whether you or your organization decided to pay the ransom, the FBI urges you to report ransomware incidents to 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.

¹⁰ Accessibility description: Chart shows Top Ransomware Variants Affecting Critical Infrastructure 2023 Incidents. Lockbit, ALPHV/Blackcat, Akira, Royal, and Black Basta.

TECH/CUSTOMER SUPPORT AND GOVERNMENT IMPERSONATION ¹¹



Impersonation scams defraud thousands of individuals each year. Two categories of fraud reported to IC3, Tech/Customer Support and Government Impersonation, are responsible for over \$1.3 billion in losses.

| | Complaints | Losses | Trend |
|---------------------------|---------------|------------------------|-------|
| Government Impersonation | 14,190 | \$394,050,518 | ▲63% |
| Tech and Customer Support | 37,560 | \$924,512,658 | ▲15% |
| TOTAL | 51,750 | \$1,318,563,176 | |

Call centers overwhelmingly target older adults, with devastating effects. Almost half the complainants report to be Over 60 (40%), and experience 58% of the losses (over \$770 million).

Investigative Success Stories

FBI Knoxville Cyber Squad: The initial complaint received from IC3 spearheaded the investigation by identifying the main subjects, Ankur Khemani, and the Sterks, a family based in Iowa. Khemani and his co-conspirators duped thousands of victims into believing their computers were infected with malicious malware. The resulting investigation grew from 50 initial IC3 reports to over 14,000 victims with over \$4 million in losses. On September 28, 2023, Khemani was sentenced in Knoxville federal court to 75 months for orchestrating a fraudulent computer technical support ring based in India. On December 20, 2023, Marilyn Sterk, along with her daughter Teresa Sterk, and daughter-in-law Jennifer Sterk, were sentenced in Knoxville federal court for their involvement in a tech support scheme. The Sterks opened over 30 bank accounts to launder money obtained from victims of an India-based tech support scam. Marilyn was sentenced to 30 months in prison, while her daughters received three years of probation.

FBI, Legat New Delhi, Washington Field: Since 2022, the DOJ, the FBI Legal Attaché New Delhi, the Washington Field Office (WFO), and IC3 have collaborated with law enforcement in India, such as the Central Bureau of Investigation in New Delhi and local Indian states, to combat cyber-enabled financial crimes and transnational call center fraud. In 2023, Indian law enforcement accomplished multiple call center raids, disruptions, seizures, and arrests of the individuals alleged to be involved in perpetrating these crimes. The FBI enabled 26 arrests through 13 joint operations with Indian authorities. WFO conducted hundreds of interviews and continues to support Indian law enforcement efforts and prosecution of call centers perpetrating these frauds.

IC3 publications in 2023 Related to Tech/Customer Support and Government Impersonation

- ["Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings](#)
- [Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash through Shipping Companies](#)
- [Criminals Pose as Chinese Authorities to Target US-based Chinese Community \(简体中文版\) \(繁體中文版\)](#)

¹¹ Accessibility description: Chart shows number of Government Impersonation and Tech and Customer Support complainants and losses for 2023.

IC3 BY THE NUMBERS¹²



\$12.5 Billion

Losses in 2023



2,412

Average complaints received daily

2021
2019
2018
2017
2016

758,000+

Average complaints received per year (last 5 years)

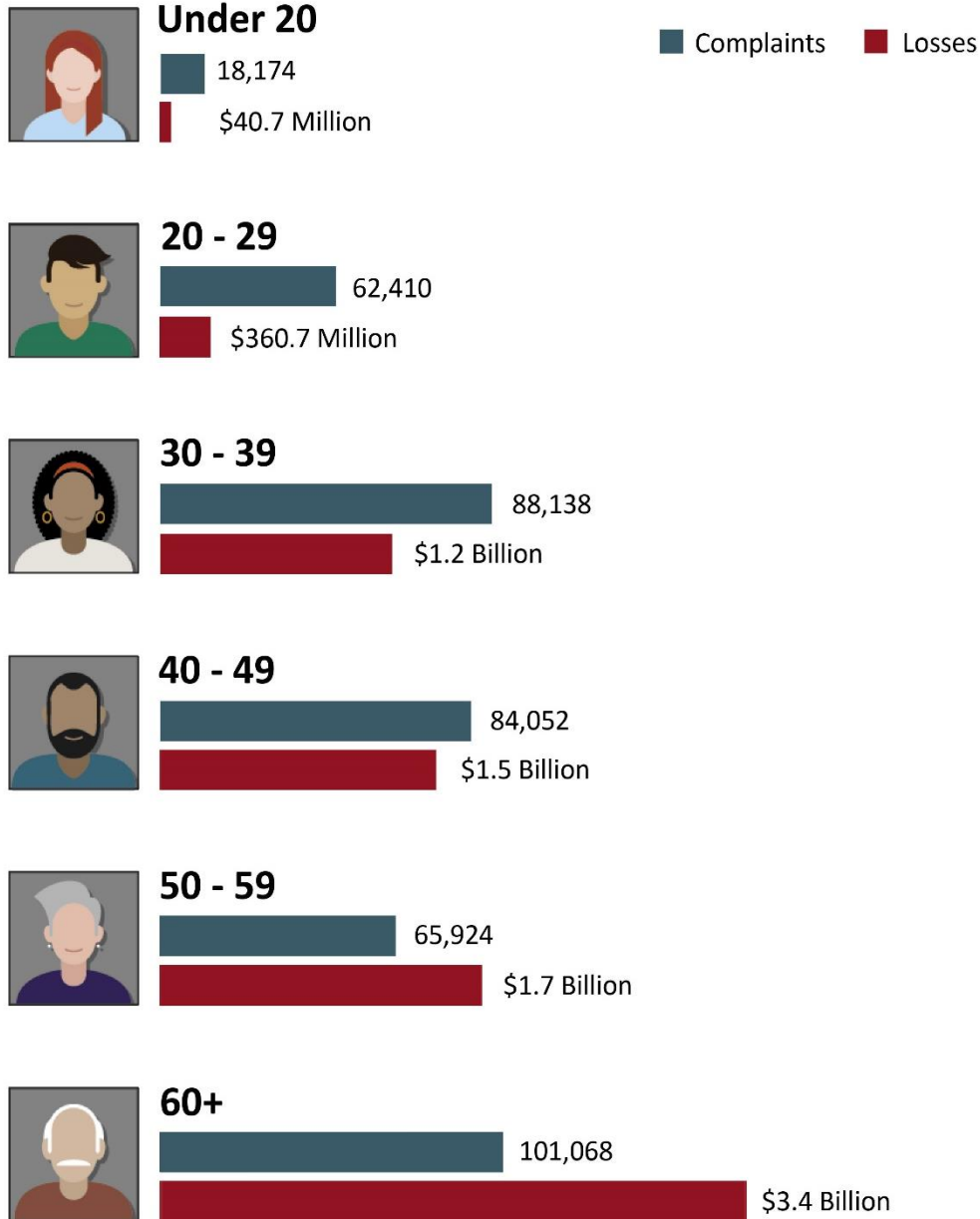


Over 8 Million

Complaints reported since inception

¹² Accessibility description: Image depicts key statistics regarding complaints and losses. Total losses of \$12.5 billion were reported in 2023. The total number of complaints received since the year 2000 is over 8 million. The IC3 has received approximately 758,000 complaints per year on average over the last five years, or more than 2,412 complaints per day.

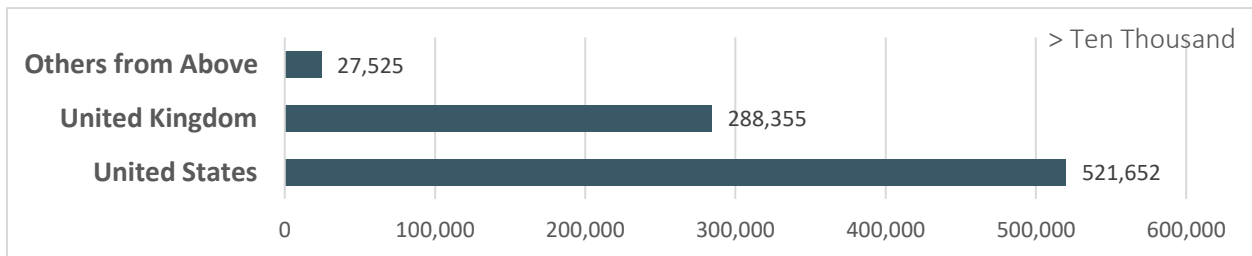
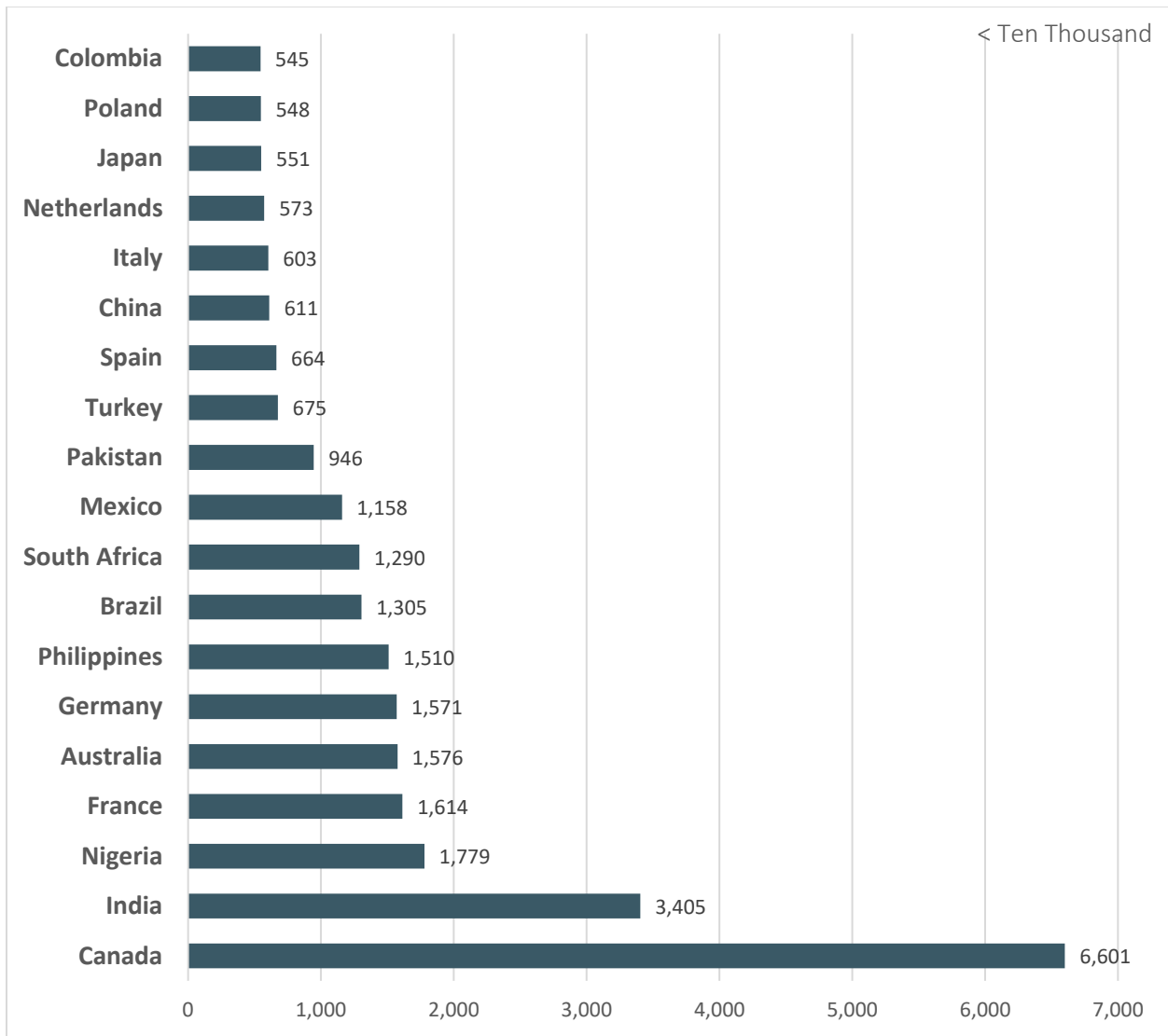
2023 - COMPLAINANTS BY AGE GROUP ¹³



¹³ 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 Losses by Age Group. Under 20 18,174 Complaints, \$40.7 Million losses; 20-29 62,410 Complaints, \$360.7 Million losses; 30-39 88,138 Complaints, \$1.2 Billion losses; 40-49 84,052 Complaints, \$1.5 Billion losses; 50-59 65,924 Complaints, \$1.7 Billion losses; 60+ 101,068 Complaints, \$3.4 Billion losses.

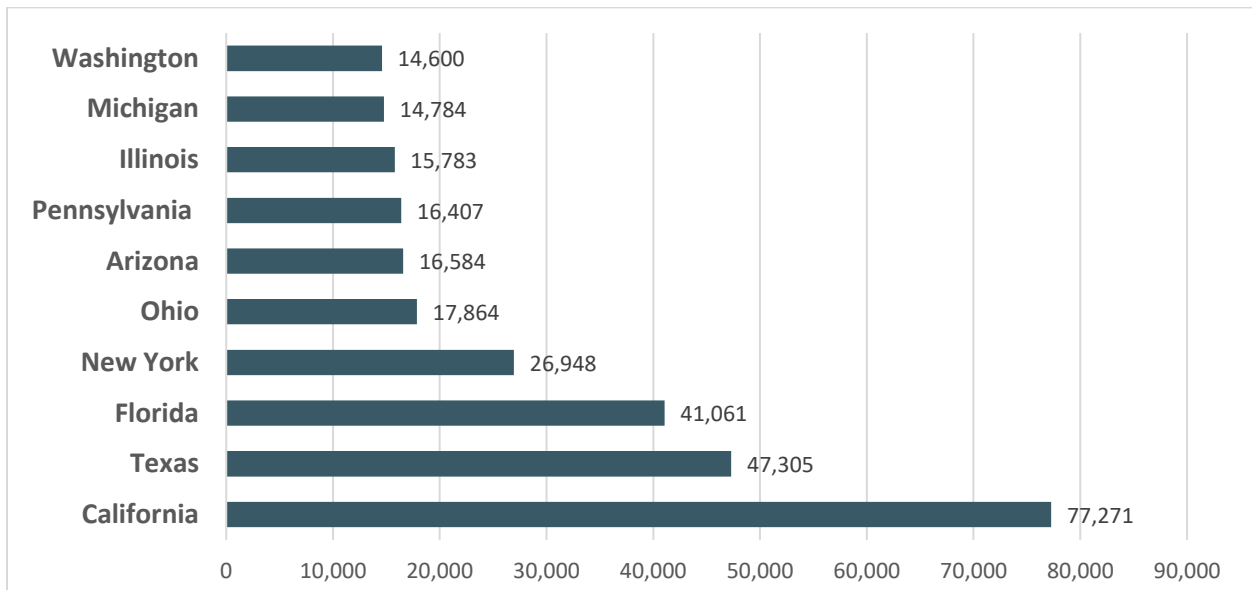
2023 - TOP 20 INTERNATIONAL COMPLAINT COUNTRIES ¹⁴

Compared to the United States

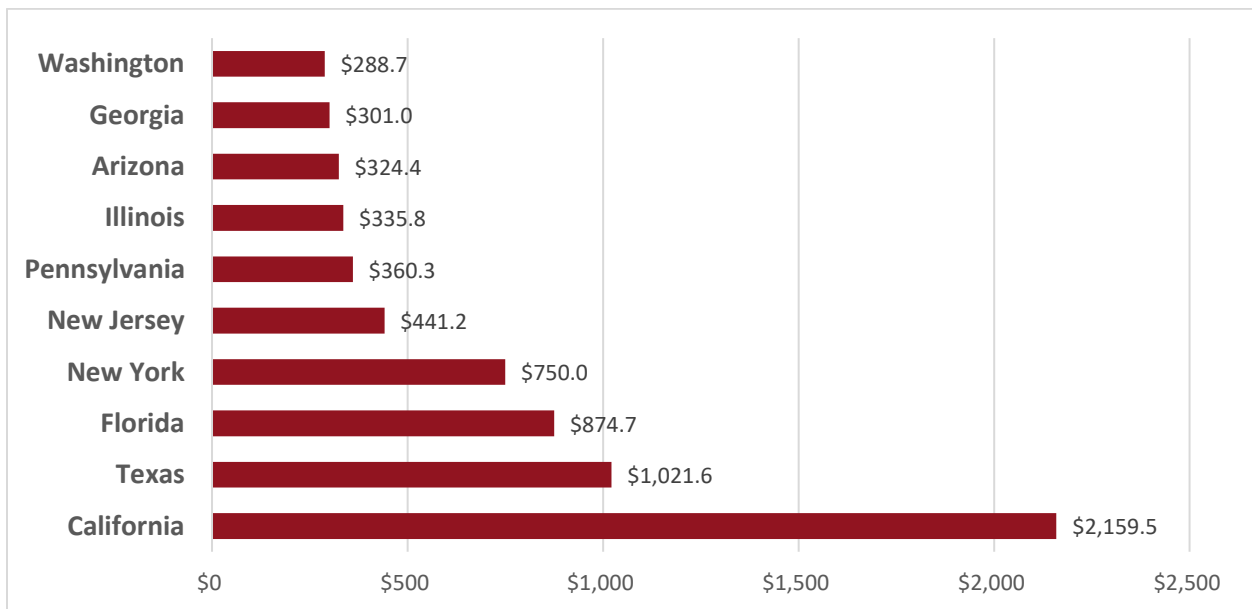


¹⁴ Accessibility description: the charts list the top 20 countries by number of total complaints as compared to the United States and United Kingdom. The specific number of complaints for each country are listed in ascending order to the right of the graph. Please see Appendix B for more information regarding IC3 data.

2023 - TOP 10 STATES BY NUMBER OF COMPLAINTS ¹⁵



2023 - TOP 10 STATES BY LOSS (IN MILLIONS) ¹⁶



¹⁵ Accessibility description: Chart depicts the top 10 states based on number of complaints are labeled. These include California, Texas, Florida, New York, Ohio, Arizona, Pennsylvania, Illinois, Michigan, and Washington. Please see Appendix B for more information regarding IC3 data.

¹⁶ Accessibility description: Chart depicts the top 10 states based on reported losses are labeled. These include California, Texas, Florida, New York, New Jersey, Pennsylvania, Illinois, Arizona, Georgia, and Washington. Please see Appendix B for more information regarding IC3 data.

2023 CRIME TYPES

| By Complaint Count | | | |
|--------------------------|-------------------|---------------------------------|-------------------|
| <i>Crime Type</i> | <i>Complaints</i> | <i>Crime Type</i> | <i>Complaints</i> |
| Phishing/Spoofing | 298,878 | Other | 8,808 |
| Personal Data Breach | 55,851 | Advanced Fee | 8,045 |
| Non-payment/Non-Delivery | 50,523 | Lottery/Sweepstakes/Inheritance | 4,168 |
| Extortion | 48,223 | Overpayment | 4,144 |
| Investment | 39,570 | Data Breach | 3,727 |
| Tech Support | 37,560 | Ransomware | 2,825 |
| BEC | 21,489 | Crimes Against Children | 2,361 |
| Identity Theft | 19,778 | Threats of Violence | 1,697 |
| Confidence/Romance | 17,823 | IPR/Copyright and Counterfeit | 1,498 |
| Employment | 15,443 | SIM Swap | 1,075 |
| Government Impersonation | 14,190 | Malware | 659 |
| Credit Card/Check Fraud | 13,718 | Botnet | 540 |
| Harassment/Stalking | 9,587 | | |
| Real Estate | 9,521 | | |
| <i>Descriptors*</i> | | | |
| Cryptocurrency | 43,653 | Cryptocurrency Wallet | 25,815 |

*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.

2023 CRIME TYPES continued

| By Complaint Loss | | | |
|---------------------------------|-----------------|-------------------------------|--------------|
| Crime Type | Loss | Crime Type | Loss |
| Investment | \$4,570,275,683 | Extortion | \$74,821,835 |
| BEC | \$2,946,830,270 | Employment | \$70,234,079 |
| Tech Support | \$924,512,658 | Ransomware* | \$59,641,384 |
| Personal Data Breach | \$744,219,879 | SIM Swap | \$48,798,103 |
| Confidence/Romance | \$652,544,805 | Overpayment | \$27,955,195 |
| Data Breach | \$534,397,222 | Botnet | \$22,422,708 |
| Government Impersonation | \$394,050,518 | Phishing/Spoofing | \$18,728,550 |
| Non-payment/Non-Delivery | \$309,648,416 | Threats of Violence | \$13,531,178 |
| Other | \$240,053,059 | Harassment/Stalking | \$9,677,332 |
| Credit Card/Check Fraud | \$173,627,614 | IPR/Copyright and Counterfeit | \$7,555,329 |
| Real Estate | \$145,243,348 | Crimes Against Children | \$2,031,485 |
| Advanced Fee | \$134,516,577 | Malware | \$1,213,317 |
| Identity Theft | \$126,203,809 | | |
| Lottery/Sweepstakes/Inheritance | \$94,502,836 | | |

| Descriptors** | | | |
|----------------|-----------------|-----------------------|-----------------|
| Cryptocurrency | \$3,809,090,856 | Cryptocurrency Wallet | \$1,778,399,729 |

*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 an entity. In some cases, entities do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to the FBI via the IC3 and does not account for the entity 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-THREE-YEAR COMPLAINT COUNT COMPARISON

| By Complaint Count | | ▼ ▲ = Trend from previous Year | | |
|---------------------------------|-----------|--------------------------------|-----------|--|
| Crime Type | 2023 | 2022 | 2021 | |
| Advanced Fee | 8,045 ▼ | 11,264 ▲ | 11,034 ▼ | |
| BEC | 21,489 ▼ | 21,832 ▲ | 19,954 ▲ | |
| Botnet | 540 ▼ | 568 | N/A | |
| Confidence Fraud/Romance | 17,823 ▼ | 19,021 ▼ | 24,299 ▲ | |
| Credit Card/Check Fraud | 13,718 ▼ | 22,985 ▲ | 16,750 ▼ | |
| Crimes Against Children | 2,361 ▼ | 2,587 ▲ | 2,167 ▼ | |
| Data Breach | 3,727 ▲ | 2,795 ▲ | 1,287 ▼ | |
| Employment | 15,443 ▲ | 14,946 ▼ | 15,253 ▼ | |
| Extortion | 48,223 ▲ | 39,416 ▲ | 39,360 ▼ | |
| Government Impersonation | 14,190 ▲ | 11,554 ▲ | 11,335 ▼ | |
| Harassment/Stalking | 9,587 ▼ | 11,779 | N/A | |
| Identity Theft | 19,778 ▼ | 27,922 ▼ | 51,629 ▲ | |
| Investment | 39,570 ▲ | 30,529 ▲ | 20,561 ▲ | |
| IPR/Copyright and Counterfeit | 1,498 ▼ | 2,183 ▼ | 4,270 ▲ | |
| Lottery/Sweepstakes/Inheritance | 4,168 ▼ | 5,650 ▼ | 5,991 ▼ | |
| Malware | 659 ▼ | 762 ▼ | 810 ▼ | |
| Non-Payment/Non-Delivery | 50,523 ▼ | 51,679 ▼ | 82,478 ▼ | |
| Other | 8,808 ▼ | 9,966 ▼ | 12,346 ▲ | |
| Overpayment | 4,144 ▼ | 6,183 ▲ | 6,108 ▼ | |
| Personal Data Breach | 55,851 ▼ | 58,859 ▲ | 51,829 ▲ | |
| Phishing/Spoofing | 298,878 ▼ | 321,136 ▼ | 342,494 ▲ | |
| Ransomware | 2,825 ▲ | 2,385 ▼ | 3,729 ▲ | |
| Real Estate | 9,521 ▼ | 11,727 ▲ | 11,578 ▼ | |
| SIM Swap | 1,075 ▼ | 2,026 | N/A | |
| Tech Support | 37,560 ▲ | 32,538 ▲ | 23,903 ▲ | |
| Threats of Violence | 1,697 ▼ | 2,224 | N/A | |

LAST-THREE-YEAR COMPLAINT LOSS COMPARISON

| By Complaint Loss | | ▼ ▲ = Trend from previous Year | | |
|---------------------------------|-------------------|--------------------------------|-------------------|--|
| Crime Type | 2023 | 2022 | 2021 | |
| Advanced Fee | \$134,516,577 ▲ | \$104,325,444 ▲ | \$98,694,137 ▲ | |
| BEC | \$2,946,830,270 ▲ | \$2,742,354,049 ▲ | \$2,395,953,296 ▲ | |
| Botnet | \$22,422,708 ▲ | \$17,099,378 ▲ | N/A | |
| Confidence Fraud/Romance | \$652,544,805 ▼ | \$735,882,192 ▼ | \$956,039,739 ▲ | |
| Credit Card/Check Fraud | \$173,627,614 ▼ | 264,148,905 ▲ | \$172,998,385 ▲ | |
| Crimes Against Children | \$2,031,485 ▲ | \$577,464 ▲ | \$198,950 ▼ | |
| Data Breach | \$534,397,222 ▲ | \$459,321,859 ▲ | \$151,568,225 ▲ | |
| Employment | \$70,234,079 ▲ | \$52,204,269 ▲ | \$47,231,023 ▼ | |
| Extortion | \$74,821,835 ▲ | \$54,335,128 ▼ | \$60,577,741 ▼ | |
| Government Impersonation | \$394,050,518 ▲ | \$240,553,091 ▲ | \$142,643,253 ▲ | |
| Harassment/Stalking | \$9,677,332 ▲ | \$5,621,402 | N/A | |
| Identity Theft | \$126,203,809 ▼ | 189,205,793 ▼ | \$278,267,918 ▲ | |
| Investment | \$4,570,275,683 ▲ | \$3,311,742,206 ▲ | \$1,455,943,193 ▲ | |
| IPR/Copyright and Counterfeit | \$7,555,329 ▲ | \$4,591,177 ▼ | \$16,365,011 ▲ | |
| Lottery/Sweepstakes/Inheritance | \$94,502,836 ▲ | \$83,602,376 ▲ | \$71,289,089 ▲ | |
| Malware | \$1,213,317 ▼ | \$9,326,482 ▲ | \$5,596,889 ▼ | |
| Non-Payment/Non-Delivery | \$309,648,416 ▲ | \$281,770,073 ▼ | \$337,493,071 ▲ | |
| Other | \$240,053,059 ▲ | \$117,686,789 ▲ | \$75,837,524 ▼ | |
| Overpayment | \$27,955,195 ▼ | \$38,335,772 ▲ | \$33,407,671 ▼ | |
| Personal Data Breach | \$744,219,879 ▲ | \$742,438,136 ▲ | \$517,021,289 ▲ | |
| Phishing/Spoofing | \$18,728,550 ▼ | \$160,015,411 ▲ | \$126,383,513 ▼ | |
| Ransomware | \$59,641,384 ▲ | \$34,353,237 ▼ | \$49,207,908 ▲ | |
| Real Estate | \$145,243,348 ▼ | \$396,932,821 ▲ | \$350,328,166 ▲ | |
| SIM Swap | \$48,798,103 ▼ | \$72,652,571 | N/A | |
| Tech Support | \$924,512,658 ▲ | \$806,551,993 ▲ | \$347,657,432 ▲ | |
| Threats of Violence | \$13,531,178 ▲ | \$4,972,099 | N/A | |

OVERALL STATE STATISTICS

| Complaints per State* | | | | | |
|-----------------------|----------------|------------|------|-----------------------------|------------|
| Rank | State | Complaints | Rank | State | Complaints |
| 1 | California | 77,271 | 30 | Louisiana | 4,890 |
| 2 | Texas | 47,305 | 31 | Kentucky | 4,641 |
| 3 | Florida | 41,061 | 32 | District of Columbia | 3,769 |
| 4 | New York | 26,948 | 33 | Iowa | 3,723 |
| 5 | Ohio | 17,864 | 34 | Arkansas | 3,220 |
| 6 | Arizona | 16,584 | 35 | Mississippi | 2,983 |
| 7 | Pennsylvania | 16,407 | 36 | New Mexico | 2,944 |
| 8 | Illinois | 15,783 | 37 | Kansas | 2,894 |
| 9 | Michigan | 14,784 | 38 | Delaware | 2,687 |
| 10 | Washington | 14,600 | 39 | Puerto Rico | 2,678 |
| 11 | Georgia | 13,917 | 40 | West Virginia | 2,365 |
| 12 | Virginia | 12,711 | 41 | Alaska | 2,338 |
| 13 | North Carolina | 12,282 | 42 | Idaho | 2,240 |
| 14 | New Jersey | 12,253 | 43 | Nebraska | 2,195 |
| 15 | Colorado | 11,475 | 44 | Hawaii | 1,954 |
| 16 | Indiana | 11,097 | 45 | South Dakota | 1,688 |
| 17 | Massachusetts | 9,915 | 46 | New Hampshire | 1,650 |
| 18 | Nevada | 9,893 | 47 | Maine | 1,626 |
| 19 | South Carolina | 9,736 | 48 | Montana | 1,571 |
| 20 | Maryland | 9,717 | 49 | Rhode Island | 1,425 |
| 21 | Tennessee | 8,484 | 50 | Wyoming | 828 |
| 22 | Missouri | 8,108 | 51 | North Dakota | 764 |
| 23 | Wisconsin | 7,683 | 52 | Vermont | 698 |
| 24 | Minnesota | 7,049 | 53 | U.S. Minor Outlying Islands | 145 |
| 25 | Oregon | 6,724 | 54 | Virgin Islands, U.S. | 126 |
| 26 | Alabama | 5,763 | 55 | Guam | 90 |
| 27 | Connecticut | 5,216 | 56 | American Samoa | 33 |
| 28 | Utah | 5,061 | 57 | Northern Mariana Islands | 16 |
| 29 | Oklahoma | 4,987 | | | |

*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*

| Losses by State* | | | | | |
|------------------|----------------|-----------------|------|-----------------------------|--------------|
| Rank | State | Loss | Rank | State | Loss |
| 1 | California | \$2,159,454,513 | 30 | Louisiana | \$78,286,085 |
| 2 | Texas | \$1,021,547,286 | 31 | Oklahoma | \$66,967,060 |
| 3 | Florida | \$874,725,493 | 32 | Iowa | \$59,829,482 |
| 4 | New York | \$749,955,480 | 33 | Hawaii | \$51,722,052 |
| 5 | New Jersey | \$441,151,263 | 34 | Idaho | \$50,631,580 |
| 6 | Pennsylvania | \$360,334,651 | 35 | Kentucky | \$48,746,051 |
| 7 | Illinois | \$335,764,223 | 36 | Arkansas | \$46,585,087 |
| 8 | Arizona | \$324,352,644 | 37 | District of Columbia | \$46,142,350 |
| 9 | Georgia | \$301,001,997 | 38 | Montana | \$45,554,368 |
| 10 | Washington | \$288,691,091 | 39 | New Mexico | \$45,127,386 |
| 11 | Virginia | \$265,073,590 | 40 | Nebraska | \$40,581,244 |
| 12 | Massachusetts | \$235,890,173 | 41 | South Dakota | \$35,855,494 |
| 13 | North Carolina | \$234,972,238 | 42 | Delaware | \$35,376,770 |
| 14 | Maryland | \$221,520,527 | 43 | Mississippi | \$32,144,078 |
| 15 | Michigan | \$203,445,988 | 44 | Alaska | \$31,771,278 |
| 16 | Nevada | \$200,995,121 | 45 | Rhode Island | \$31,586,831 |
| 17 | Ohio | \$197,365,326 | 46 | Puerto Rico | \$30,102,231 |
| 18 | Minnesota | \$193,949,414 | 47 | New Hampshire | \$27,178,268 |
| 19 | Colorado | \$187,621,731 | 48 | West Virginia | \$21,445,942 |
| 20 | Indiana | \$162,259,036 | 49 | Maine | \$18,968,567 |
| 21 | Tennessee | \$161,195,036 | 50 | Wyoming | \$13,746,109 |
| 22 | Oregon | \$136,052,036 | 51 | North Dakota | \$13,532,443 |
| 23 | Utah | \$132,257,035 | 52 | Vermont | \$ 8,818,181 |
| 24 | Missouri | \$123,405,404 | 53 | U.S. Minor Outlying Islands | \$3,588,797 |
| 25 | Connecticut | \$120,767,349 | 54 | Virgin Islands, U.S. | \$2,637,004 |
| 26 | South Carolina | \$119,950,630 | 55 | Guam | \$747,876 |
| 27 | Alabama | \$96,479,649 | 56 | American Samoa | \$327,467 |
| 28 | Kansas | \$94,158,337 | 57 | Northern Mariana Islands | \$25,917 |
| 29 | Wisconsin | \$92,084,459 | | | |

*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 of Subjects per State* | | | | | |
|------------------------------|----------------------|----------|------|--------------------------------------|----------|
| Rank | State | Subjects | Rank | State | Subjects |
| 1 | California | 42,590 | 30 | Kentucky | 1,760 |
| 2 | Texas | 18,194 | 31 | Mississippi | 1,738 |
| 3 | Florida | 17,174 | 32 | Nebraska | 1,696 |
| 4 | New York | 14,824 | 33 | Wisconsin | 1,621 |
| 5 | Georgia | 6,083 | 34 | Arkansas | 1,587 |
| 6 | Ohio | 5,728 | 35 | Utah | 1,440 |
| 7 | Illinois | 5,550 | 36 | New Mexico | 1,035 |
| 8 | Washington | 5,523 | 37 | Delaware | 1,027 |
| 9 | Pennsylvania | 5,359 | 38 | Kansas | 989 |
| 10 | Arizona | 5,029 | 39 | Iowa | 915 |
| 11 | North Carolina | 4,973 | 40 | West Virginia | 736 |
| 12 | Michigan | 4,839 | 41 | Idaho | 694 |
| 13 | New Jersey | 4,633 | 42 | South Dakota | 615 |
| 14 | Connecticut | 4,297 | 43 | Hawaii | 602 |
| 15 | Virginia | 4,202 | 44 | Montana | 600 |
| 16 | Colorado | 4,178 | 45 | Vermont | 598 |
| 17 | Maryland | 3,598 | 46 | Wyoming | 573 |
| 18 | Nevada | 3,402 | 47 | Rhode Island | 525 |
| 19 | Massachusetts | 3,263 | 48 | Alaska | 487 |
| 20 | Tennessee | 3,127 | 49 | New Hampshire | 474 |
| 21 | South Carolina | 2,893 | 50 | Maine | 446 |
| 22 | Indiana | 2,624 | 51 | Puerto Rico | 326 |
| 23 | Minnesota | 2,549 | 52 | North Dakota | 303 |
| 24 | Missouri | 2,470 | 53 | Virgin Islands, U.S. | 60 |
| 25 | Alabama | 2,408 | 54 | United States Minor Outlying Islands | 58 |
| 26 | Oregon | 2,253 | 55 | Guam | 32 |
| 27 | Louisiana | 2,128 | 56 | American Samoa | 10 |
| 28 | Oklahoma | 2,066 | 57 | Northern Mariana Islands | 6 |
| 29 | District of Columbia | 1,952 | | | |

*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*

| Losses Attributed to Subjects per Destination State* | | | | | |
|--|----------------------|-----------------|------|---|--------------|
| Rank | State | Loss | Rank | State | Loss |
| 1 | California | \$1,450,468,117 | 30 | Delaware | \$26,679,171 |
| 2 | New York | \$659,190,424 | 31 | Oklahoma | \$25,955,810 |
| 3 | Florida | \$460,557,456 | 32 | Alabama | \$24,130,582 |
| 4 | Texas | \$436,917,629 | 33 | Iowa | \$22,875,411 |
| 5 | Washington | \$197,573,721 | 34 | Wisconsin | \$21,885,467 |
| 6 | New Jersey | \$162,556,627 | 35 | Kentucky | \$18,985,386 |
| 7 | Pennsylvania | \$161,290,998 | 36 | New Hampshire | \$16,725,453 |
| 8 | Illinois | \$160,429,405 | 37 | South Dakota | \$16,664,530 |
| 9 | Arizona | \$143,931,864 | 38 | Idaho | \$16,259,172 |
| 10 | Georgia | \$138,867,559 | 39 | New Mexico | \$15,968,662 |
| 11 | Utah | \$136,063,240 | 40 | Arkansas | \$13,170,026 |
| 12 | Colorado | \$123,104,339 | 41 | Montana | \$12,196,983 |
| 13 | Massachusetts | \$115,059,569 | 42 | West Virginia | \$11,423,197 |
| 14 | North Carolina | \$100,992,438 | 43 | Mississippi | \$11,309,747 |
| 15 | Minnesota | \$76,391,448 | 44 | Nebraska | \$11,260,461 |
| 16 | Louisiana | \$76,222,392 | 45 | Hawaii | \$11,086,273 |
| 17 | Maryland | \$72,488,154 | 46 | Kansas | \$10,734,529 |
| 18 | Nevada | \$72,469,793 | 47 | Rhode Island | \$9,446,947 |
| 19 | Virginia | \$69,306,635 | 48 | Maine | \$7,468,102 |
| 20 | District of Columbia | \$65,746,127 | 49 | Alaska | \$6,534,122 |
| 21 | Ohio | \$64,966,735 | 50 | Puerto Rico | \$3,260,842 |
| 22 | Michigan | \$52,994,817 | 51 | North Dakota | \$2,714,457 |
| 23 | Tennessee | \$49,887,333 | 52 | Vermont | \$2,003,750 |
| 24 | Indiana | \$49,381,324 | 53 | United States Minor Outlying Islands | \$947,386 |
| 25 | Missouri | \$46,655,163 | 54 | Northern Mariana Islands | \$237,597 |
| 26 | Connecticut | \$40,616,316 | 55 | Virgin Islands, U.S. | \$123,269 |
| 27 | Oregon | \$38,230,223 | 56 | Guam | \$113,518 |
| 28 | South Carolina | \$31,866,254 | 57 | American Samoa | \$21,420 |
| 29 | Wyoming | \$30,627,210 | | | |

*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*

| Complaints per Capita* | | | <i>per 100,000 citizens</i> | | |
|------------------------|----------------------|----------|-----------------------------|----------------|----------|
| Rank | State | Subjects | Rank | State | Subjects |
| 1 | District of Columbia | 555.1 | 27 | West Virginia | 133.6 |
| 2 | Alaska | 318.8 | 28 | New Jersey | 131.9 |
| 3 | Nevada | 309.7 | 29 | Missouri | 130.9 |
| 4 | Delaware | 260.4 | 30 | Rhode Island | 130.0 |
| 5 | Arizona | 223.2 | 31 | Wisconsin | 130.0 |
| 6 | California | 198.3 | 32 | Pennsylvania | 126.6 |
| 7 | Colorado | 195.2 | 33 | Georgia | 126.2 |
| 8 | Washington | 186.9 | 34 | Illinois | 125.8 |
| 9 | South Dakota | 183.6 | 35 | Oklahoma | 123.0 |
| 10 | Florida | 181.6 | 36 | Minnesota | 122.8 |
| 11 | South Carolina | 181.2 | 37 | Tennessee | 119.0 |
| 12 | Indiana | 161.7 | 38 | New Hampshire | 117.7 |
| 13 | Oregon | 158.8 | 39 | Maine | 116.5 |
| 14 | Maryland | 157.2 | 40 | Iowa | 116.1 |
| 15 | Texas | 155.1 | 41 | Idaho | 114.0 |
| 16 | Ohio | 151.6 | 42 | North Carolina | 113.3 |
| 17 | Utah | 148.1 | 43 | Alabama | 112.8 |
| 18 | Michigan | 147.3 | 44 | Nebraska | 110.9 |
| 19 | Virginia | 145.8 | 45 | Vermont | 107.8 |
| 20 | Connecticut | 144.2 | 46 | Louisiana | 106.9 |
| 21 | Wyoming | 141.8 | 47 | Arkansas | 105.0 |
| 22 | Massachusetts | 141.6 | 48 | Kentucky | 102.5 |
| 23 | New Mexico | 139.2 | 49 | Mississippi | 101.5 |
| 24 | Montana | 138.7 | 50 | Kansas | 98.4 |
| 25 | New York | 137.7 | 51 | North Dakota | 97.5 |
| 26 | Hawaii | 136.2 | 52 | Puerto Rico | 83.5 |

*Note: This information is based on the estimated 2023 Census data and the total number of complaints from each state, the District of Columbia, and Puerto Rico when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

<https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html#v2023>

OVERALL STATE STATISTICS *continued*

| Losses per Capita* | | | <i>per 100,000 citizens</i> | | |
|--------------------|----------------------|-------------|-----------------------------|----------------|-------------|
| Rank | State | Loss | Rank | State | Loss |
| 1 | District of Columbia | \$6,795,914 | 27 | Illinois | \$2,675,478 |
| 2 | Nevada | \$6,292,550 | 28 | Idaho | \$2,577,030 |
| 3 | California | \$5,542,009 | 29 | Indiana | \$2,364,534 |
| 4 | New Jersey | \$4,748,238 | 30 | Wyoming | \$2,353,556 |
| 5 | Arizona | \$4,364,657 | 31 | Tennessee | \$2,261,914 |
| 6 | Alaska | \$4,332,018 | 32 | South Carolina | \$2,232,240 |
| 7 | Montana | \$4,021,353 | 33 | North Carolina | \$2,168,543 |
| 8 | South Dakota | \$3,900,228 | 34 | New Mexico | \$2,134,317 |
| 9 | Utah | \$3,869,729 | 35 | Nebraska | \$2,051,237 |
| 10 | Florida | \$3,868,631 | 36 | Michigan | \$2,026,907 |
| 11 | New York | \$3,831,931 | 37 | Missouri | \$1,991,645 |
| 12 | Washington | \$3,695,066 | 38 | New Hampshire | \$1,938,461 |
| 13 | Hawaii | \$3,603,978 | 39 | Alabama | \$1,888,622 |
| 14 | Maryland | \$3,584,328 | 40 | Iowa | \$1,865,588 |
| 15 | Delaware | \$3,428,347 | 41 | North Dakota | \$1,726,240 |
| 16 | Minnesota | \$3,380,137 | 42 | Louisiana | \$1,711,639 |
| 17 | Massachusetts | \$3,369,186 | 43 | Ohio | \$1,674,584 |
| 18 | Texas | \$3,348,973 | 44 | Oklahoma | \$1,651,948 |
| 19 | Connecticut | \$3,338,719 | 45 | Wisconsin | \$1,557,861 |
| 20 | Oregon | \$3,213,809 | 46 | Arkansas | \$1,518,551 |
| 21 | Kansas | \$3,202,070 | 47 | Puerto Rico | \$1,479,384 |
| 22 | Colorado | \$3,192,143 | 48 | Vermont | \$1,361,957 |
| 23 | Virginia | \$3,041,335 | 49 | Maine | \$1,359,051 |
| 24 | Rhode Island | \$2,882,110 | 50 | West Virginia | \$1,211,587 |
| 25 | Pennsylvania | \$2,779,999 | 51 | Mississippi | \$1,093,451 |
| 26 | Georgia | \$2,729,130 | 52 | Kentucky | \$1,076,986 |

*Note: This information is based on the estimated 2023 Census data and the total number of complaints from each state, the District of Columbia, and Puerto Rico when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

<https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html#v2023>

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 (BEC): BEC is a scam targeting businesses or individuals working with suppliers and/or businesses regularly performing wire transfer payments. These sophisticated scams are carried out by fraudsters by compromising email accounts and other forms of communication such as phone numbers and virtual meeting applications, through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Botnet: A botnet is a group of two or more computers controlled and updated remotely for an illegal purchase such as a Distributed Denial of Service or Telephony Denial of Service attack or other nefarious activity.

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

Credit Card Fraud/Check 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.

Data Breach: A data breach in the cyber context is the use of a computer intrusion to acquire confidential or secured information. This does not include computer intrusions targeting personally owned computers, systems, devices, or personal accounts such as social media or financial accounts.

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.

Government Impersonation: A government official is impersonated in an attempt to collect money.

Harassment/Stalking: Repeated words, conduct, or action that serve no legitimate purpose and are directed at a specific person to annoy, alarm, or distress that person. Engaging in a course of conduct directed at a specific person that would cause a reasonable person to fear for his/her safety or the safety of others or suffer substantial emotional distress.

Identity Theft: Someone wrongfully obtains and uses personally identifiable information in some way that involves fraud or deception, typically for economic gain.

Investment: Deceptive practice that induces investors to make purchases based on false information. These scams usually offer those targeted large returns with minimal risk. (Retirement, 401K, Ponzi, Pyramid, etc.).

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.

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: 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/Spoofing: 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.

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

SIM Swap: The use of unsophisticated social engineering techniques against mobile service providers to transfer a victim's phone service to a mobile device in the criminal's possession.

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

Threats of Violence: An expression of an intention to inflict pain, injury, self-harm, or death not in the context of extortion.

APPENDIX B: ADDITIONAL INFORMATION ABOUT IC3 DATA

- As appropriate, complaints are reviewed by IC3 analysts, who apply a crime type and adjust the total loss.
- Crime Types and losses can be variable and can evolve based upon investigative or analytical proceedings. Statistics are an assessment taken at a point in time, which can change.
- Complainant/Entity is identified as the individual filing a complaint.
- 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.
- Subject is identified as the individual perpetrating the scam as reported by the complainant.
- “Count by Subjects per state” is the number of subjects per state, as reported by complainants.
- “Losses Attributed to Subjects per Destination State” is the amount swindled by the subject, as reported by the complainant, per state.

APPENDIX C: PUBLIC SERVICE ANNOUNCEMENTS PUBLISHED

| Title | Date |
|--|------------|
| <u>Scammers Targeting Owners of Timeshares in Mexico</u> | 3/3/2023 |
| <u>Criminals Steal Cryptocurrency through Play-to-Earn Games</u> | 3/9/2023 |
| <u>The FBI Warns of a Spike in Cryptocurrency Investment Schemes</u> | 3/14/2023 |
| <u>Business Email Compromise Tactics Used to Facilitate the Acquisition of Commodities and Defrauding Vendors</u> | 3/24/2023 |
| <u>For-Profit Companies Charging Sextortion Victims for Assistance and Using Deceptive Tactics to Elicit Payments</u> | 4/7/2023 |
| <u>Criminals Pose as Chinese Authorities to Target US-based Chinese Community</u> | 4/10/2023 |
| <u>Multinational Non-Governmental Organizations Potentially Exploited in Aftermath of Earthquakes Affecting Turkey and Syria</u> | 4/28/2023 |
| <u>The FBI Warns of False Job Advertisements Linked to Labor Trafficking at Scam Compounds</u> | 5/22/2023 |
| <u>Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes (ic3.gov)</u> | 7/5/2023 |
| <u>Business Email Compromise: The \$50 Billion Scam</u> | 7/9/2023 |
| <u>Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash through Shipping Companies</u> | 7/18/2023 |
| <u>Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition</u> | 8/4/2023 |
| <u>Increase in Companies Falsely Claiming an Ability to Recover Funds Lost in Cryptocurrency Investment Scams</u> | 8/11/2023 |
| <u>Cyber Criminals Targeting Victims through Mobile Beta-Testing Applications (ic3.gov)</u> | 8/14/2023 |
| <u>FBI Guidance for Cryptocurrency Scam Victims</u> | 8/24/2023 |
| <u>Violent Online Groups Extort Minors to Self-Harm and Produce Child Sexual Abuse Material</u> | 9/12/2023 |
| <u>"Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings</u> | 9/29/2023 |
| <u>Situation in Israel</u> | 10/10/2023 |
| <u>Cybercriminals are Targeting Plastic Surgery Offices and Patients</u> | 10/17/2023 |
| <u>Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers</u> | 10/18/2023 |
| <u>Scammers Solicit Fake Humanitarian Donations</u> | 10/24/2023 |
| <u>Threats Associated with the Israel-HAMAS Conflict</u> | 10/26/2023 |
| <u>2023 Holiday Shopping Scams</u> | 11/15/2023 |
| <u>FBI Warns of Scammers Targeting Senior Citizens in Grandparent Scams and Demanding Funds by Wire, Mail, or Couriers</u> | 11/17/2023 |
| <u>Threat of Violence Likely Heightened Throughout Winter</u> | 12/12/2023 |