FEDERAL BUREAU of INVESTIGATION

Internet Crime Report

2022

INTERNET CRIME COMPLAINT CENTER

CONTENTS

INTRODUCTION

Dear Reader,

Today's cyber landscape has provided ample opportunities for criminals and adversaries to target U.S. networks, attack our critical infrastructure, hold our money and data for ransom, facilitate large-scale fraud schemes, and threaten our national security. At the FBI, we know "cyber risk is business risk" and "cyber security is national security." There is no shortage of recent examples showing the wide-ranging economic and national security effects of cyber crimes. We have seen cyber threats emanate from around the world and witnessed the scope and sophistication of these scams and attacks deepen. As these threats increase, we continue to encourage victims to report cyber incidents and cyber-enabled frauds to the FBI so that we may impose risks and consequences on malicious cyber actors.

Because cyberattacks and cyber-enabled frauds continue to affect our everyday lives, the FBI's Internet Crime Complaint Center (IC3) is critical to combatting the cyber threat. The IC3 serves as a public resource to submit reports of cyberattacks and incidents, which allows us to collect data, identify trends, and pursue the threat at hand. In 2022, the IC3 received 800,944 complaints, which is a 5 percent decrease from 2021. However, the potential total loss has grown from $6.9 billion in 2021 to more than $10.2 billion in 2022.

While the number of reported ransomware incidents has decreased, we know not everyone who has experienced a ransomware incident has reported to the IC3. As such, we assess ransomware remains a serious threat to the public and to our economy, and the FBI and our partners will remain focused on disrupting ransomware actors and increasing the risks of engaging in this activity. In concert, the public can play a crucial role by taking proactive measures to prevent and prepare for a potential cyber attack and, if there is an incident, by reporting it to the FBI through the IC3. Though cybercriminals are continuously seeking to make their attacks more resilient, more disruptive, and harder to counter, public reporting to the IC3 helps us gain a better understanding of the threats we face daily.

The FBI's commitment to assisting victims of cyber crimes and cyber-enabled frauds, as well as our dedication to working with partners to combat these crimes, allows for 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 2022, RAT initiated the Financial Fraud Kill Chain (FFKC) on 2,838 Business Email Compromise (BEC) complaints involving domestic-to-domestic transactions with potential losses of over $590 million. A monetary hold was placed on approximately $433 million, which represents a 73 percent success rate. In 2022, RAT saw a 64 percent increase in FFKCs initiated compared to 2021.

While the cyber threat is ever-growing, the FBI remains appreciative of those individuals and entities who report cyber incidents to the IC3, as that valuable information helps fill in gaps that are crucial to advancing our investigations. Your efforts are critical to our ability to pursue the perpetrators and share intelligence to protect your fellow citizens. Cyber is the ultimate team sport, and we are in this fight together. The FBI is relentlessly focused on promoting safety, security, and confidence into our digitally connected world, and we are eager to continue working with the American public to bring cybercriminals to justice around the globe.

Timothy Langan
Executive Assistant Director
Federal Bureau of Investigation

THE IC3

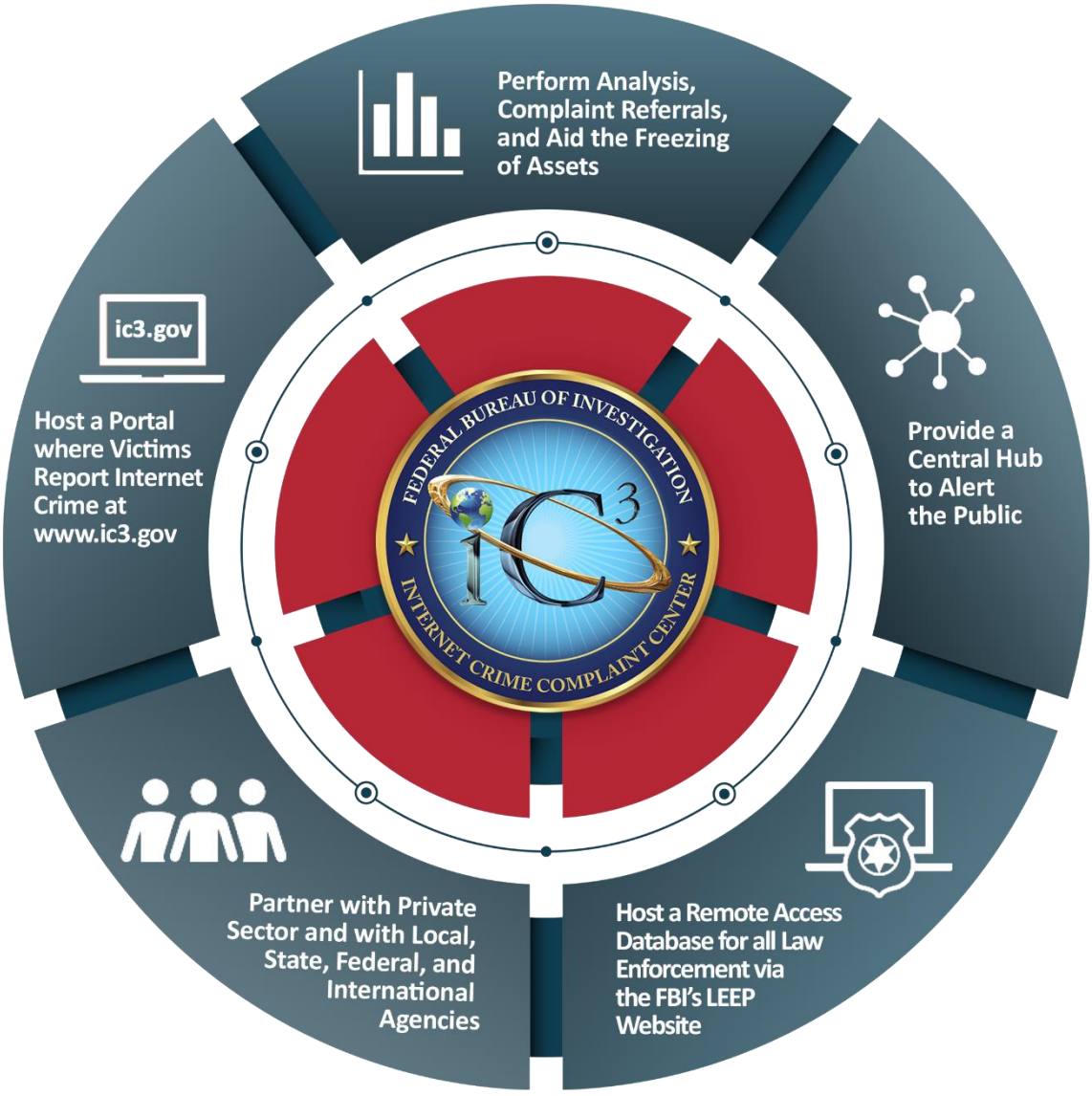
Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities. We are focused on protecting the American people from terrorism, espionage, cyber-attacks, and major criminal threats which are increasingly emanating from our digitally connected world. To do that, the FBI leverages the IC3 as a mechanism to gather intelligence and internet crime so that we can support 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, 2022, the IC3 has received over seven million complaints. The IC3 mission 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 and in the aggregate. That is, when these 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.

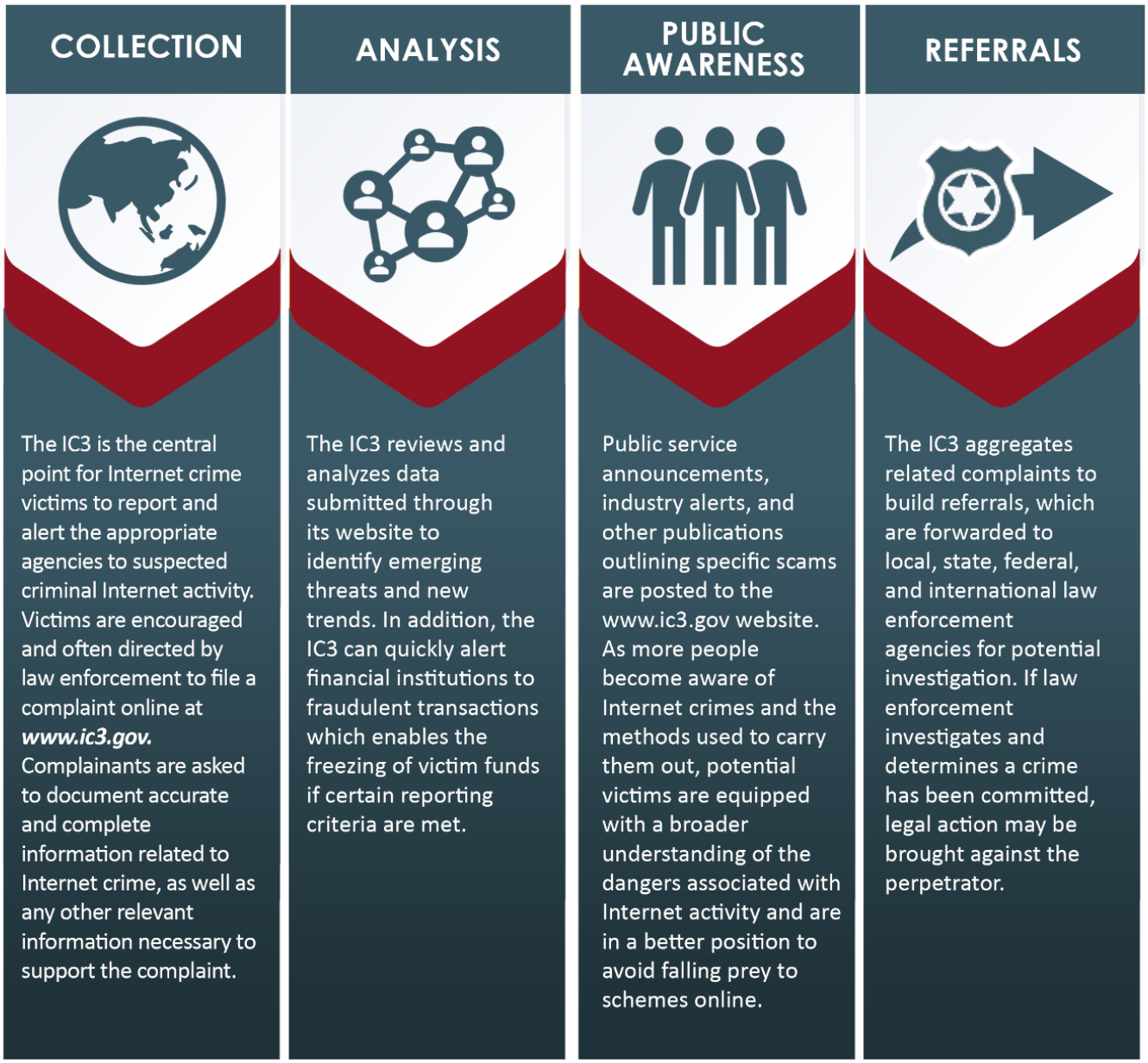
To promote public awareness and as part of its prevention mission, the IC3 aggregates the submitted data and produces an annual report on the trends impacting the public as well as routinely providing intelligence reports about trends. The success of these efforts is directly related to the quality of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

THE IC3'S ROLE IN COMBATTING CYBER CRIME[1]



[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 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 FUNCTIONS[2]

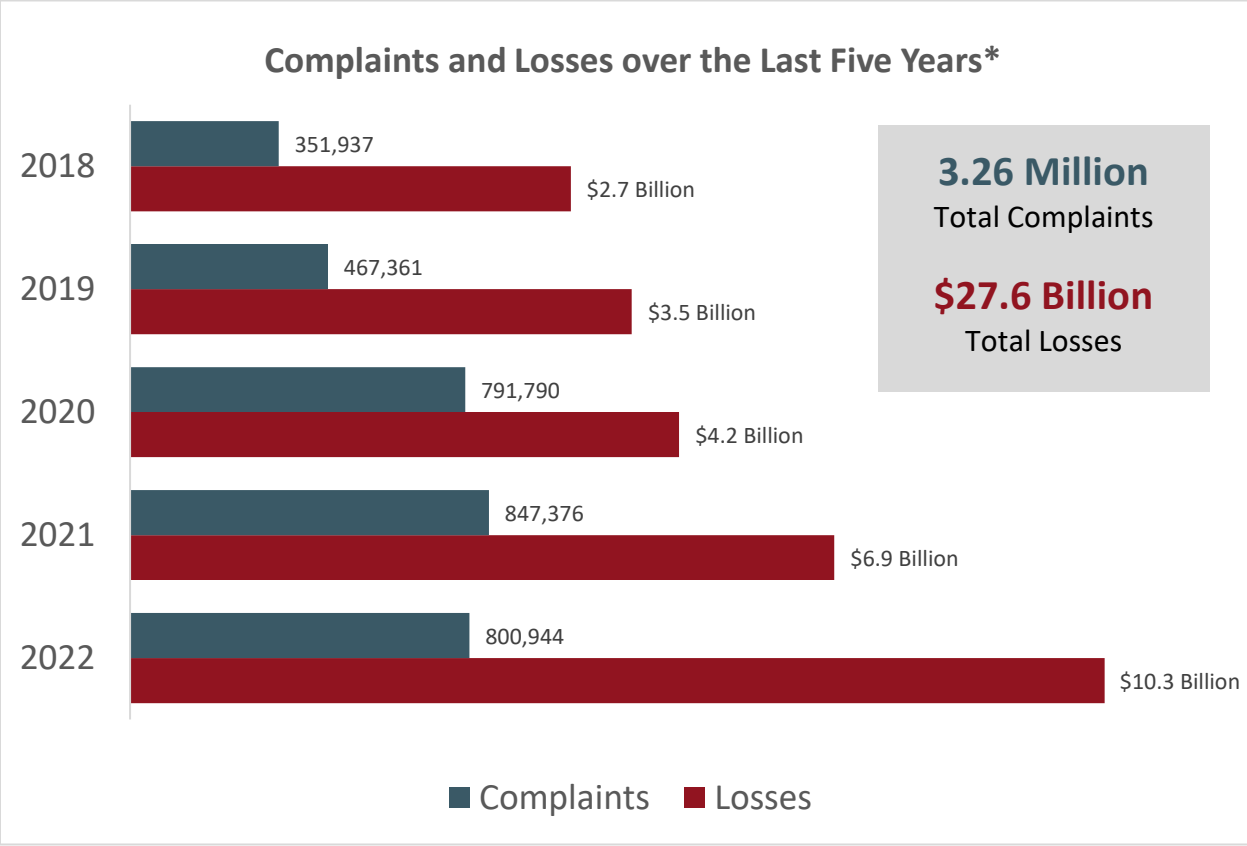


[2] Accessibility description: Image contains icons with the core functions. Core functions - Collection, Analysis, Public Awareness, and Referrals - are listed in individual blocks as components of an ongoing process.

IC3 COMPLAINT STATISTICS

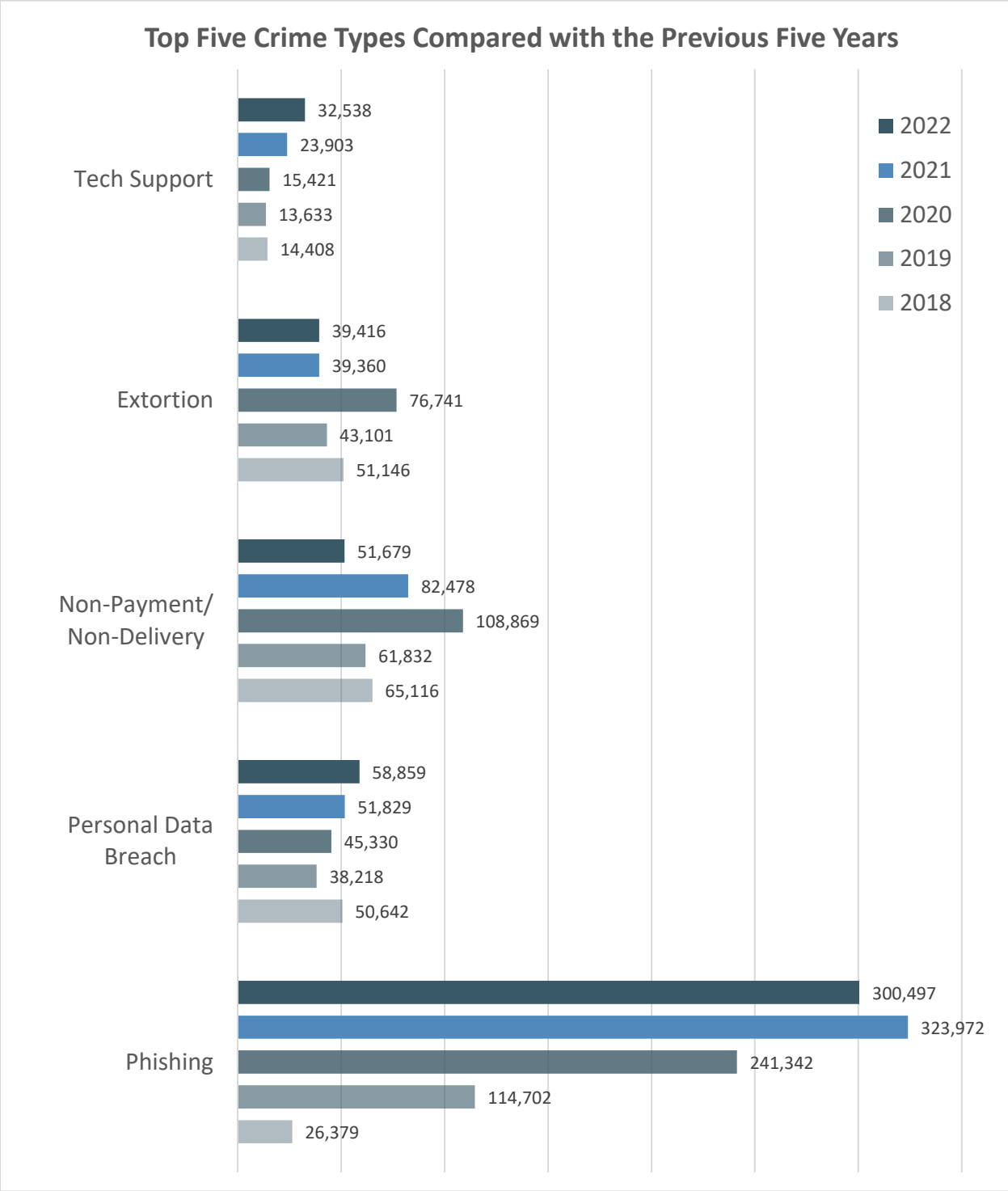
LAST FIVE YEARS

Over the last five years, the IC3 has received an average of 652,000 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 2018 to 2022. Over this time, the IC3 received a total of 3.26 million complaints, reporting a loss of $27.6 billion. * Please see Appendix B for more information regarding IC3 data.

TOP FIVE CRIME TYPE COMPARISON[4]

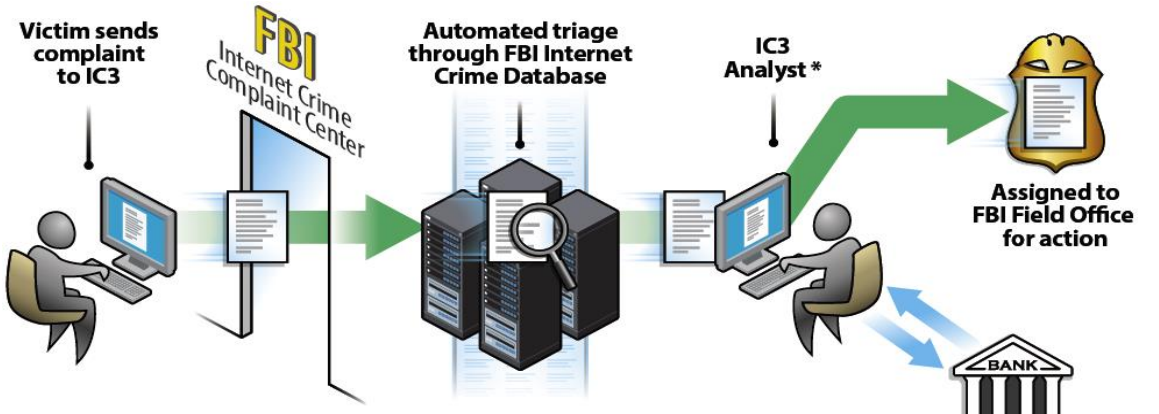


[4] Accessibility description: Chart includes a victim loss comparison for the top five reported crime types for the years of 2018 to 2022.

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 victims who made transfers to domestic accounts under fraudulent pretenses.

RAT Process[5]



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

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

Goals of RAT-Financial Institution Partnership

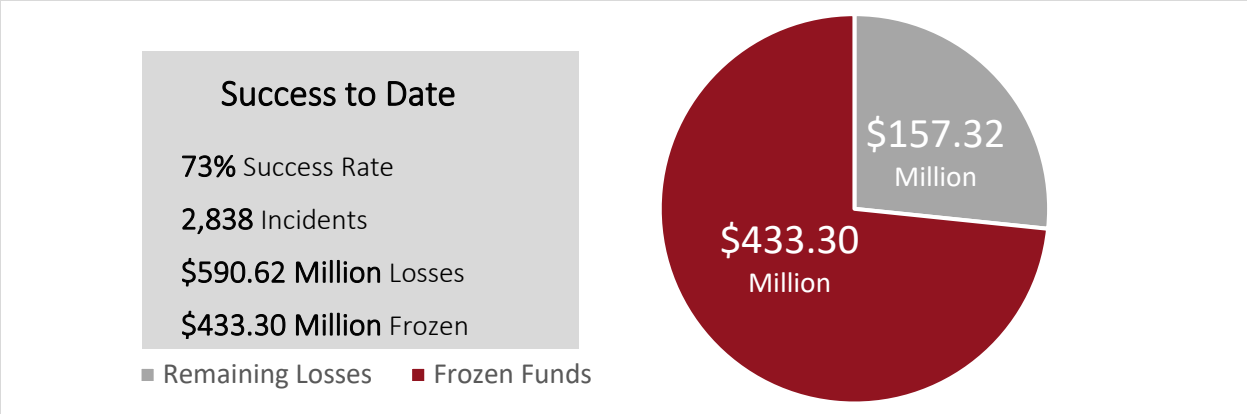
- Assist in the identification of potentially fraudulent accounts across the sector.
- Remain at the forefront of emerging trends among financial fraud schemes.
- Foster a symbiotic relationship in which information is appropriately shared.

Guidance for BEC Victims

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

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

RAT SUCCESSES[6]



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:

Seattle

In September 2022, the IC3 received a complaint filed by a victim located in the Seattle, Washington area of a BEC who intended a wire of $650,000.00 be sent to an investor, not realizing their email account was intercepted by a hacker providing fraudulent bank account instructions. The IC3 RAT immediately initiated the Financial Fraud Kill Chain (FFKC) process to freeze the fraudulent financial bank account. Further collaboration with the domestic financial institution enabled a full return to the business of approximately $645,000.00. The RAT team walked the victim through the recovery process which enabled the return of funds.

Charlotte

In July 2022, the IC3 received notice from the Charlotte field office of an IC3 complaint filed by an attorney seeking assistance with a FFKC on behalf of his clients. The clients were in the process of purchasing a home and received a spoofed email from their supposed realtor instructing them to wire $400,000.00 to a financial institution for an escrow payment. Once the wire was initiated, it was realized the instructions came from a spoofed email. Upon notification, the IC3 requested a FFKC to the recipient bank. Further collaboration between the attorney and the Charlotte field office confirmed the full amount of $400,000.00 was returned to the victim, making a full recovery possible due to the FFKC process taken by RAT and the legitimate purchase of the home was able to be made.

[6] Accessibility description: Image shows Success to Date to include 73% Success Rate; 2,838 Incidents; $590.62 Million in Losses; and $433.30 Million Frozen.

THREAT OVERVIEWS FOR 2022

BUSINESS EMAIL COMPROMISE (BEC)

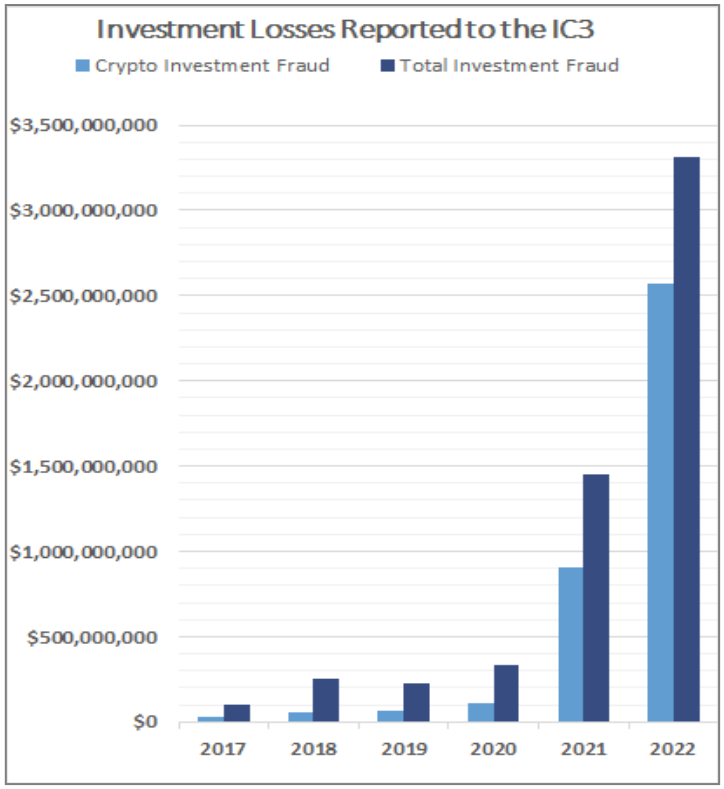
In 2022, the IC3 received 21,832 BEC complaints with adjusted losses over $2.7 billion. BEC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

As fraudsters have become more sophisticated and preventative measures have been put in place, the BEC 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. More recently, fraudsters are more frequently utilizing custodial accounts held at financial institutions for cryptocurrency exchanges, or having victims send funds directly to cryptocurrency platforms where funds are quickly dispersed.

In 2022, the IC3 also saw a slight increase of targeting victims' investment accounts instead of the traditional banking accounts. There was also an increasingly prevalent tactic by BEC bad actors of spoofing legitimate business phone numbers to confirm fraudulent banking details with victims. For one example, the victims report they have called a title company, realtor, etc., using a known phone number, and then find later the phone number has been spoofed. With this increased tactic of "spoofed" phone numbers 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 e-mail communication and can include direct phone calls but to a known verified number and not relying on information or phone numbers included in the e-mail 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[7]

In 2022, investment scam losses were the most (common or dollar amount) scheme reported to the IC3. Investment fraud complaints increased from $1.45 billion in 2021 to $3.31 billion in 2022, which is a 127%. Within those complaints, cryptocurrency investment fraud rose from $907 million in 2021 to $2.57 billion in 2022, an increase of 183%.



Crypto-investment scams saw unprecedented increases in the number of victims and the dollar losses to these investors. Many victims have assumed massive debt to cover losses from these fraudulent investments and the most targeted age group reporting this type of scam are victims ages 30 to 49. Some variations of crypto-investment scams reported in 2022 are:

- Liquidity Mining: victims are enticed to link their cryptocurrency wallet to a fraudulent liquidity mining application. Scammers then wipe out the victims' funds without notification or permission from the victim. (PSA I-072122-PSA[8]).
- Hacked Social Media: scammers used hacked social media accounts to perpetrate a fraudulent investment opportunity using cryptocurrency, targeting existing friends of the hacked user.
- Celebrity Impersonation: impersonating a well-known celebrity or social figure, the scammers feign a friendship with the targeted victim who is eventually enticed to learn how to invest in cryptocurrency or is given the opportunity to invest by the scammer.
- Real Estate Professionals: the scammer contacts a real estate agent, usually offering to buy a very expensive property for cash or cryptocurrency. Once engaged, the fraudster will expose their control of fictitious accounts with purported value of millions of dollars to entice them to engage in their investment scheme.
- Employment: victims apply for fake positions online at an investment firm or company supposedly affiliated with investing. Instead of a job, the victims are instead offered advice investment advice. The investment is fraudulent and designed to retrieve as much money from the target as possible.

[7] Accessibility description: Chart shows Investment Fraud Losses Reported to the IC3 by Year for 2017 to 2022.
[8] Internet Crime Complaint Center (IC3) | Scammers Target and Exploit Owners of Cryptocurrencies in Liquidity Mining Scam

RANSOMWARE[9]

In 2022, the IC3 received 2,385 complaints identified as ransomware with adjusted losses of more than $34.3 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 victim's data remains unavailable.

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 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. In 2022, the IC3 has seen an increase in an additional extortion tactic used to facilitate ransomware. The threat actors pressure victims to pay by threatening to publish the stolen data if they do not pay the ransom.

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.

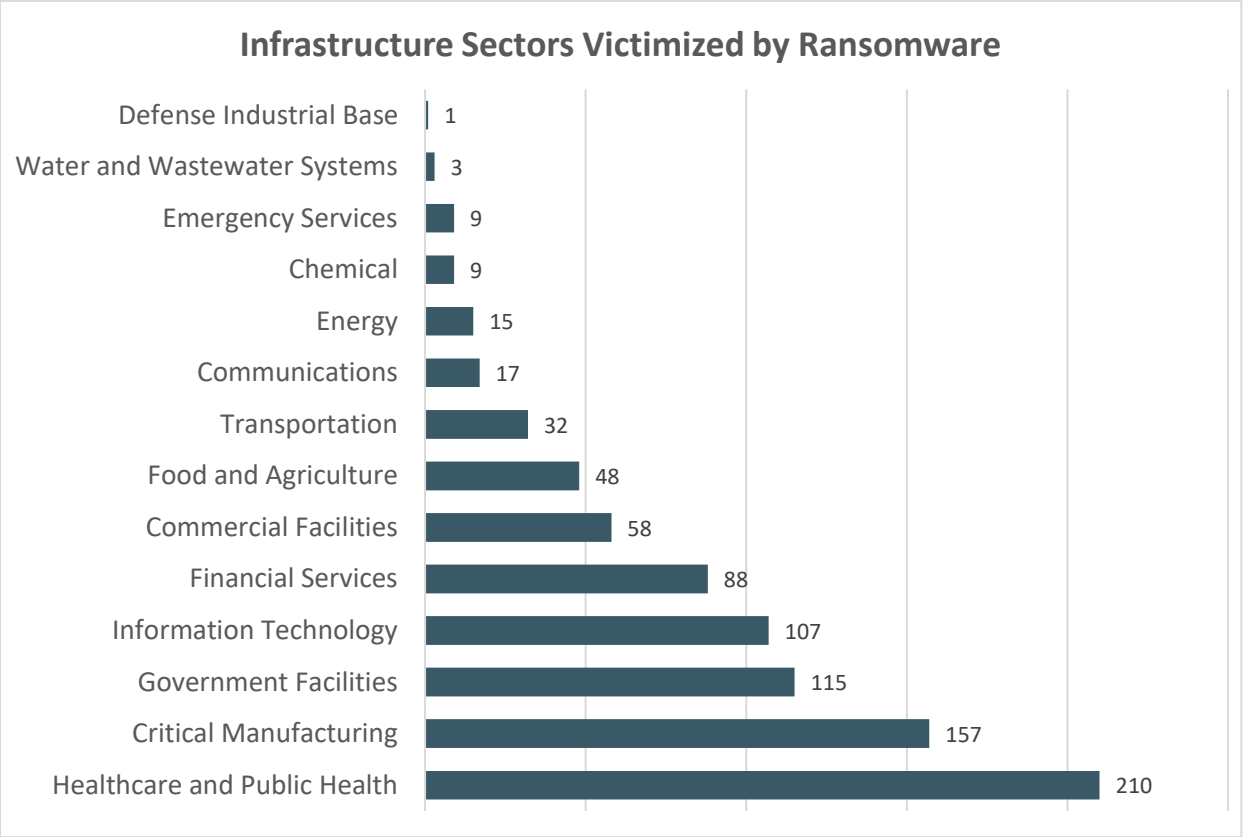
Incident reporting

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, possible seizure/recovery of ransom payments, and gain insight on adversary tactics. Ultimately, the information you provide will lead us to bring the perpetrators to justice.

[9] 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 your data.

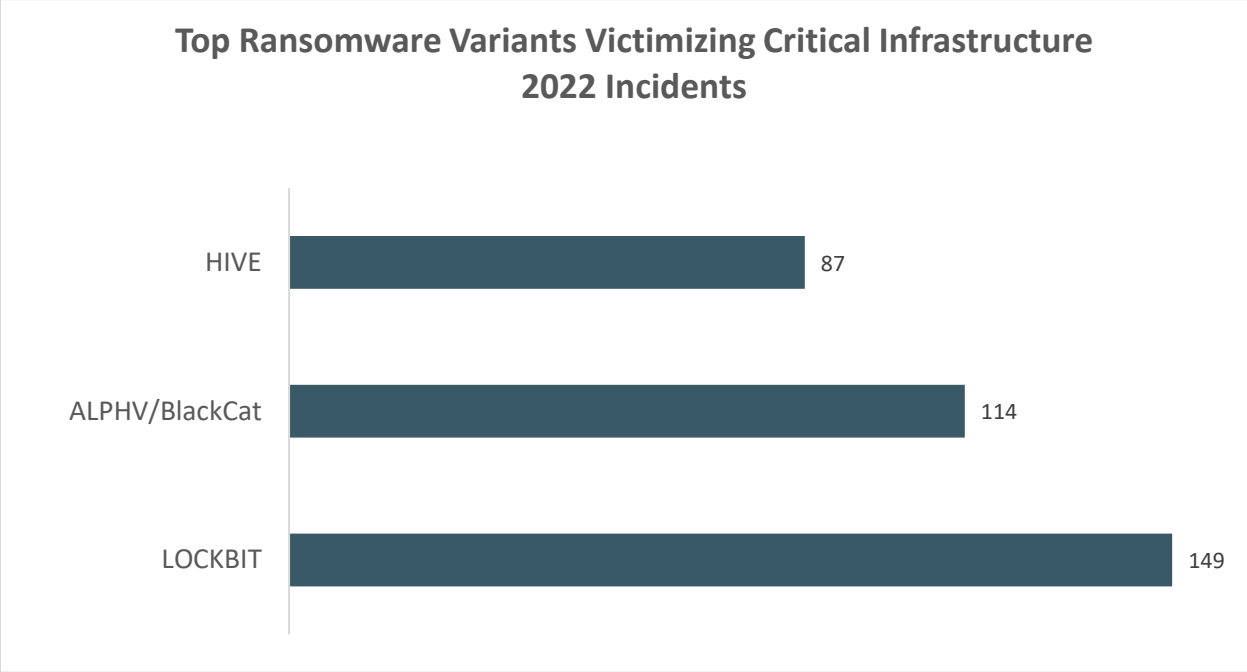
Ransomware and Critical Infrastructure Sectors

The IC3 received 870 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 2022.[10]



[10] Accessibility description: Chart shows Infrastructure Sectors Victimized by Ransomware. Healthcare and Public Health was highest with 210; followed by Critical Manufacturing 157; Government Facilities 115; Information Technology 107; Financial Services 88; Commercial Facilities 58; Food and Agriculture 48; Transportation 32; Communications 17; Energy 15; Chemical 9; Emergency Services 9; Water and Wastewater Systems 3; Defense Industrial Base 1.

The three top ransomware variants reported to the IC3 that victimized a member of a critical infrastructure sector were Lock bit, ALPHV/Blackcoats, and Hive.[11]



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 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.

[11] Accessibility description: Chart shows Top Ransomware Variants Victimizing Critical Infrastructure 2022 Incidents. lock bit, ALPHV/BlackCat, and Hive.

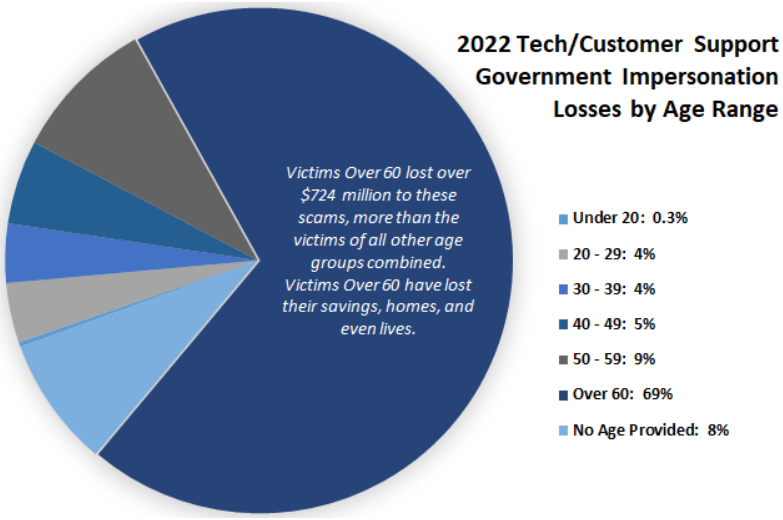
CALL CENTER FRAUD[12]

TECH AND CUSTOMER SUPPORT/GOVERNMENT IMPERSONATION

Illegal call centers defraud thousands of victims each year. Two categories of fraud reported to the IC3, Tech/Customer Support and Government Impersonation, are responsible for over $1 billion in losses to victims.

	Victims	Losses	Trend
Government Impersonation	11,554	$240,553,091	▲ 68%
Tech and Customer Support	32,538	$806,551,993	▲ 132%
TOTAL	**44,092**	**$1,047,105,083**	

Call centers overwhelmingly target the elderly, with devastating effects. Almost half the victims report to be over 60 (46%), and experience 69% of the losses (over $724 million). To learn more about these types of scams, please see these 2022-published Public Service Announcements on the IC3 website [13] and recently published podcast[14] on FBI.gov [15]



The scams primarily emanate from call centers in South Asia, mainly India. In response to the increasing victimization, the Department of Justice (DOJ) and the FBI are collaborating 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. The cooperation has secured the testimony of U.S. victims of call center fraud for use in enforcement proceedings against the alleged perpetrators.

In 2022, with the assistance of U.S. law enforcement, Indian law enforcement accomplished multiple call center raids, disruptions, seizures, and arrests of the individuals alleged to be involved in perpetrating these cyber-enabled financial crimes and global telemarketing frauds.

---

[12] Accessibility description: Chart shows number of Government Impersonation and Tech and Customer Support victims and losses for 2022.

[13] Internet Crime Complaint Center (IC3) | Technical and Customer Support Fraud; Internet Crime Complaint Center (IC3) | Scammers Using Computer-Technical Support Impersonation Scams to Target Victims and Conduct Wire Transfers; Internet Crime Complaint Center (IC3) | FBI Warns of the Impersonation of Law Enforcement and Government Officials

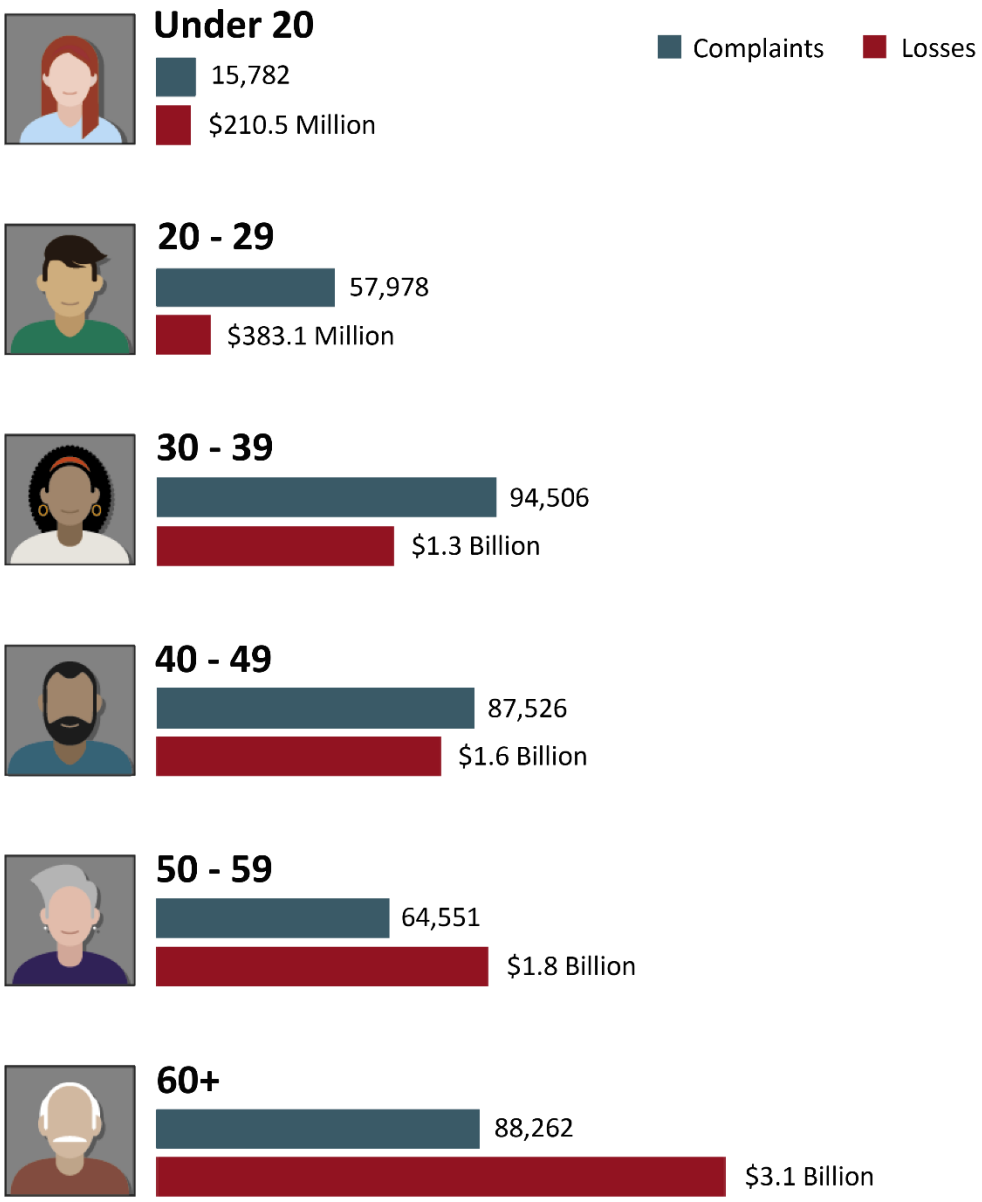
[14] https://www.fbi.gov/news/podcasts/inside-the-fbi-tech-support-scams

[15] Accessibility description: Chart shows 2022 Tech/Customer Support and Government Impersonation Losses by age range.

IC3 BY THE NUMBERS[16]

[16] Accessibility description: Image depicts key statistics regarding complaints and victim loss. Total losses of $10.3 billion were reported in 2022. The total number of complaints received since the year 2000 is over 7.3 million. The IC3 has received approximately 651,800 complaints per year on average over the last five years, or more than 2,175 complaints per day.

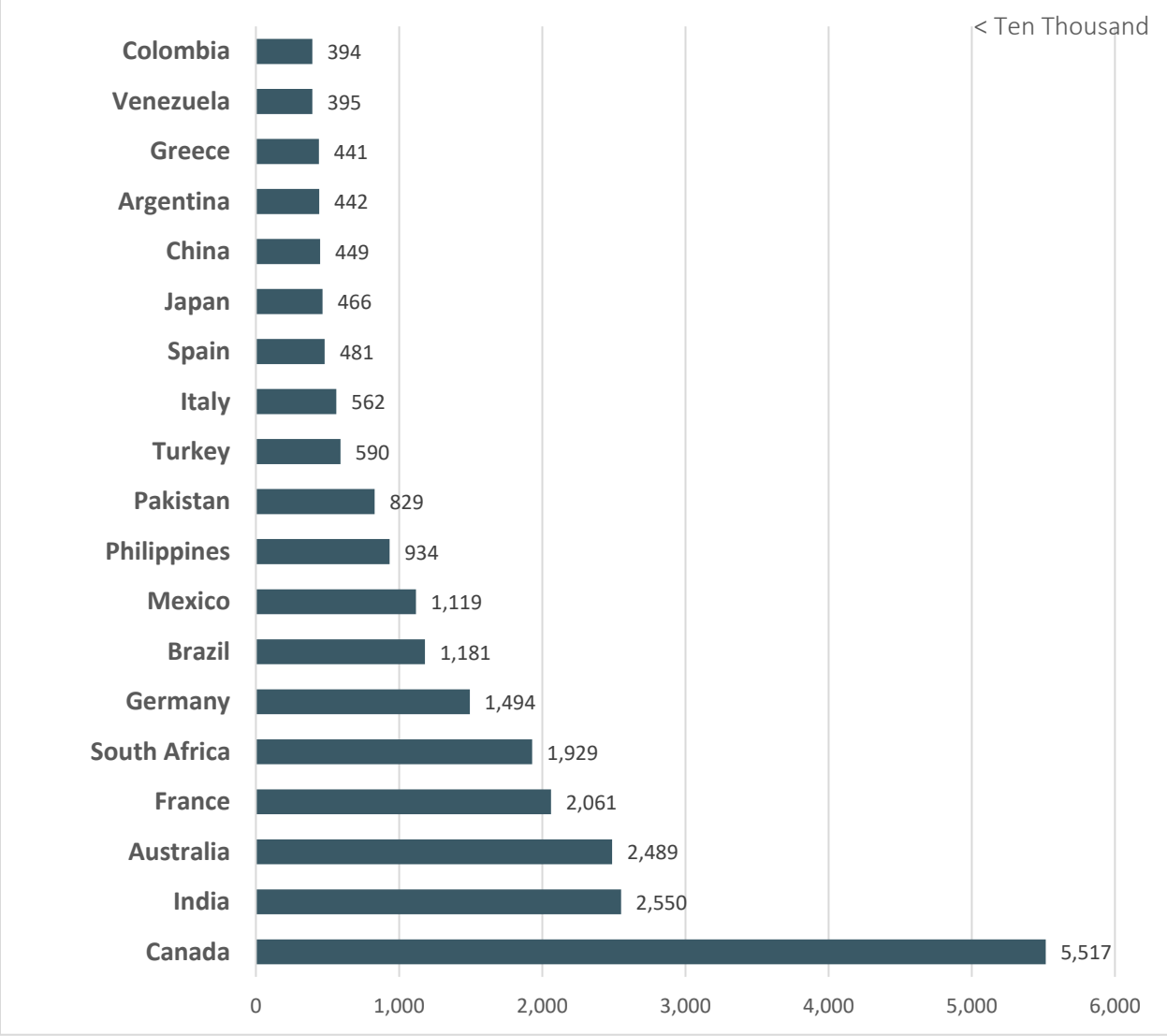
2022 - VICTIMS BY AGE GROUP[17]



[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 15,782 victims $210.5 Million losses; 20-29 57,978 Victims $383.1 Million losses; 30-39 94,506 Victims $1.3 Billion losses; 40-49 87,526 victims $1.6 Billion losses; 50-59 64,551 Victims $1.8 Billion losses; 60+ 88,262 Victims $3.1 Billion losses.

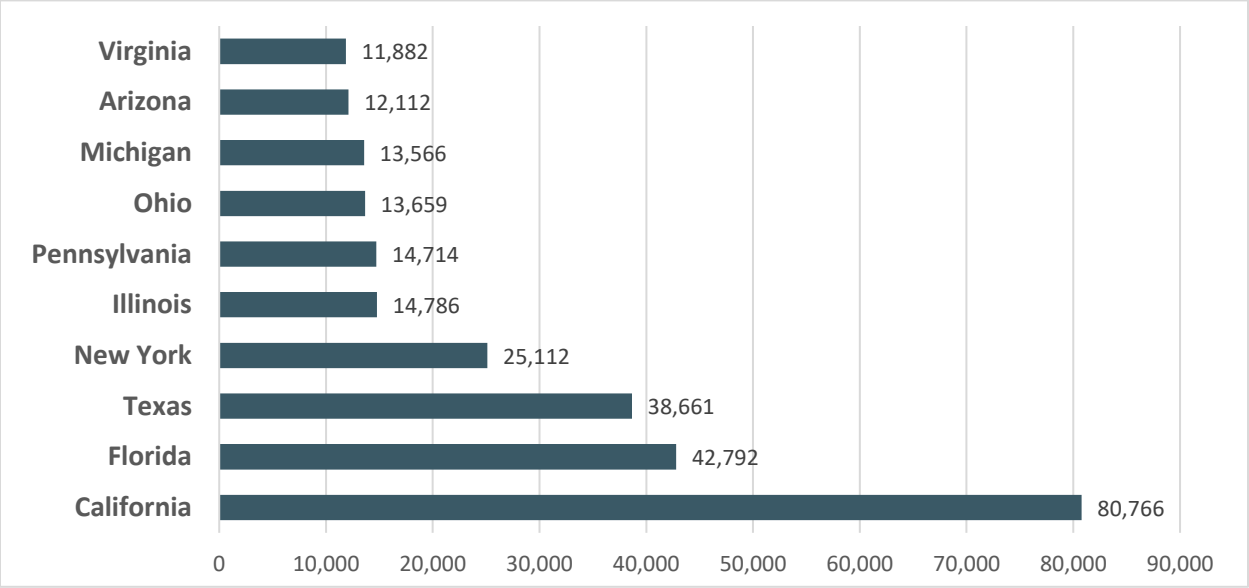
2022 - TOP 20 INTERNATIONAL VICTIM COUNTRIES[18]

Compared to the United States

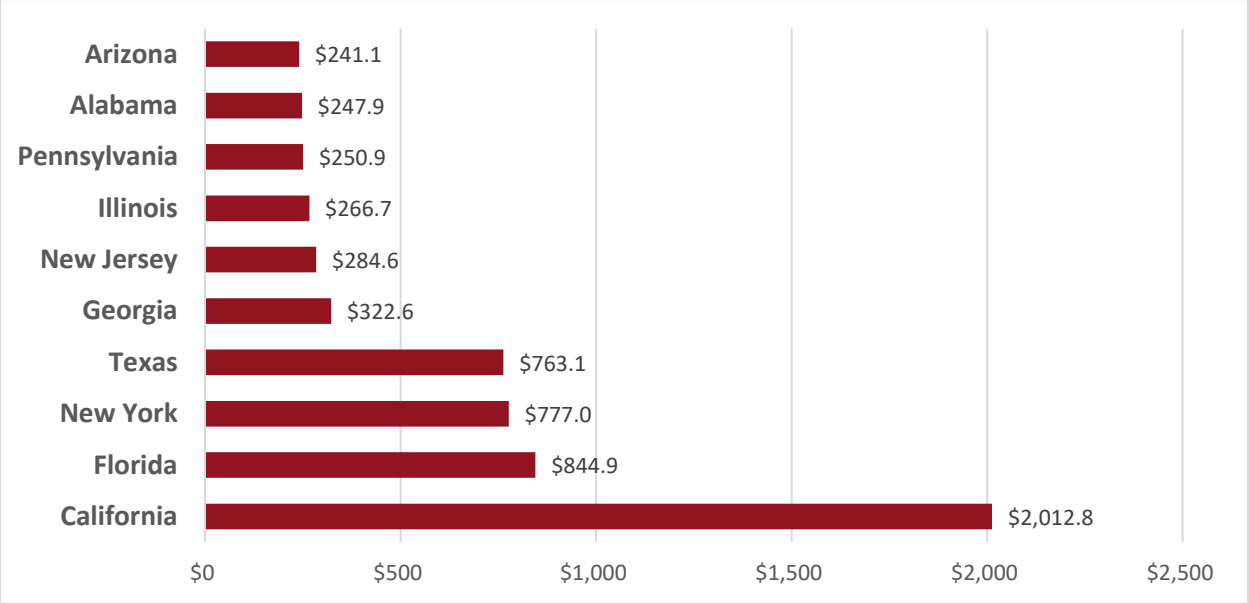


[18] Accessibility description: the charts list the top 20 countries by number of total victims as compared to the United States and United Kingdom. The specific number of victims for each country are listed in ascending order to the right of the graph. Please see Appendix B for more information regarding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

2022 - TOP 10 STATES BY NUMBER OF VICTIMS[19]



2022 - TOP 10 STATES BY VICTIM LOSS (IN MILLIONS)[20]



[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, Pennsylvania, Ohio, Michigan, Arizona, and Virginia. 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, Florida, New York, Texas, Georgia, New Jersey, Illinois, Pennsylvania, Alabama, and Arizona. Please see Appendix B for more information regarding IC3 data.

2022 CRIME TYPES

By Victim Count			
Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		
*Descriptors**			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

*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.

2022 CRIME TYPES continued

By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$3,311,742,206	Lottery/Sweepstakes/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Ransomware	*$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment/Stalking	$5,621,402
Identity Theft	$189,205,793	Threats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright/Counterfeit	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		

*Descriptors***			
Cryptocurrency	$2,496,196,530	Cryptocurrency Wallet	$1,349,090,883

* 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 THREE-YEAR COMPLAINT COUNT COMPARISON

By Victim Count			▼ ▲ = Trend from previous Year		
Crime Type	***2022***		*2021*		*2020*
Advanced Fee	**11,264**	▲	11,034	▼	13,020	▼
BEC	**21,832**	▲	19,954	▲	19,369	▼
*Botnet	**568**		N/A		N/A	
Confidence Fraud/Romance	**19,021**	▼	24,299	▲	23,751	▲
Credit Card/Check Fraud	**22,985**	▲	16,750	▼	17,614	▲
Crimes Against Children	**2,587**	▲	2,167	▼	3,202	▲
Data Breach	**2,795**	▲	1,287	▼	2,794	▲
Employment	**14,946**	▼	15,253	▼	16,879	▲
Extortion	**39,416**	▲	39,360	▼	76,741	▲
Government Impersonation	**11,554**	▲	11,335	▼	12,827	▼
*Harassment/Stalking	**11,779**		N/A		N/A	
Identity Theft	**27,922**	▼	51,629	▲	43,330	▲
Investment	**30,529**	▲	20,561	▲	8,788	▲
IPR/Copyright and Counterfeit	**2,183**	▼	4,270	▲	4,213	▲
Lottery/Sweepstakes/Inheritance	**5,650**	▼	5,991	▼	8,501	▲
Malware	**762**	▼	810	▼	1,423	▼
Non-Payment/Non-Delivery	**51,679**	▼	82,478	▼	108,869	▲
Other	**9,966**	▼	12,346	▲	10,372	▼
Overpayment	**6,183**	▲	6,108	▼	10,988	▼
Personal Data Breach	**58,859**	▲	51,829	▲	45,330	▲
Phishing	**300,497**	▼	323,972	▲	241,342	▲
Ransomware	**2,385**	▼	3,729	▲	2,474	▲
Real Estate	**11,727**	▲	11,578	▼	13,638	▲
*SIM Swap	**2,026**		N/A		N/A	
Spoofing	**20,649**	▲	18,522	▼	28,218	▲
Tech Support	**32,538**	▲	23,903	▲	15,421	▲
*Threats of Violence	**2,224**		N/A		N/A	

*New Crime Types added in 2022

LAST THREE-YEAR COMPLAINT LOSS COMPARISON

By Victim Loss						▼ ▲ = Trend from previous Year
Crime Type	***2022***		*2021*		*2020*	
Advanced Fee	**$104,325,444**	▲	$98,694,137	▲	$83,215,405	▼
BEC	**$2,742,354,049**	▲	$2,395,953,296	▲	$1,866,642,107	▲
*Botnet	**$17,099,378**	▲	N/A		N/A	
Confidence Fraud/Romance	**$735,882,192**	▼	$956,039,739	▲	$600,249,821	▲
Credit Card/Check Fraud	**264,148,905**	▲	$172,998,385	▲	$129,820,792	▲
Crimes Against Children	**$577,464**	▲	$198,950	▼	$660,044	▼
Data Breach	**$459,321,859**	▲	$151,568,225	▲	$128,916,648	▲
Employment	**$52,204,269**	▲	$47,231,023	▼	$62,314,015	▲
Extortion	**$54,335,128**	▼	$60,577,741	▼	$70,935,939	▼
Government Impersonation	**$240,553,091**	▲	$142,643,253	▲	$109,938,030	▼
*Harassment/Stalking	**$5,621,402**		N/A		N/A	
Identity Theft	**189,205,793**	▼	$278,267,918	▲	$219,484,699	▲
Investment	**$3,311,742,206**	▲	$1,455,943,193	▲	$336,469,000	▲
IPR/Copyright and Counterfeit	**$4,591,177**	▼	$16,365,011	▲	$5,910,617	▼
Lottery/Sweepstakes/Inheritance	**$83,602,376**	▲	$71,289,089	▲	$61,111,319	▲
Malware	**$9,326,482**	▲	$5,596,889	▼	$6,904,054	▲
Non-Payment/Non-Delivery	**$281,770,073**	▼	$337,493,071	▲	$265,011,249	▲
Other	**$117,686,789**	▲	$75,837,524	▼	$101,523,082	▲
Overpayment	**$38,335,772**	▲	$33,407,671	▼	$51,039,922	▼
Personal Data Breach	**$742,438,136**	▲	$517,021,289	▲	$194,473,055	▲
Phishing	**$52,089,159**	▲	$44,213,707	▼	$54,241,075	▼
Ransomware	**$34,353,237**	▼	$49,207,908	▲	$29,157,405	▲
Real Estate	**$396,932,821**	▲	$350,328,166	▲	$213,196,082	▼
*SIM Swap	**$72,652,571**		N/A		N/A	
Spoofing	**$107,926,252**	▲	$82,169,806	▼	$216,513,728	▼
Tech Support	**$806,551,993**	▲	$347,657,432	▲	$146,477,709	▲
*Threats of Violence	**$4,972,099**		N/A		N/A	

*New Crime Types added in 2022

OVERALL STATE STATISTICS

Victim per State*					
Rank	*State*	*Victims*	*Rank*	*State*	*Victims*
1	California	80,766	30	Kentucky	4,256
2	Florida	42,792	31	Oklahoma	4,148
3	Texas	38,661	32	Iowa	2,959
4	New York	25,112	33	Arkansas	2,887
5	Illinois	14,786	34	Puerto Rico	2,720
6	Pennsylvania	14,714	35	New Mexico	2,589
7	Ohio	13,659	36	District of Columbia	2,460
8	Michigan	13,566	37	Kansas	2,399
9	Georgia	13,415	38	Delaware	2,327
10	Washington	12,432	39	Mississippi	2,043
11	Arizona	12,112	40	Idaho	2,001
12	Virginia	11,882	41	Nebraska	1,957
13	New Jersey	11,793	42	West Virginia	1,846
14	Colorado	11,683	43	Hawaii	1,703
15	Indiana	11,682	44	South Dakota	1,691
16	Maryland	11,644	45	Alaska	1,539
17	North Carolina	10,554	46	Maine	1,435
18	Nevada	9,090	47	New Hampshire	1,416
19	Wisconsin	7,863	48	Montana	1,170
20	South Carolina	7,861	49	Rhode Island	1,119
21	Massachusetts	7,805	50	Wyoming	863
22	Missouri	7,560	51	Vermont	707
23	Tennessee	7,161	52	North Dakota	703
24	Minnesota	5,845	53	Guam	161
25	Oregon	5,516	54	Virgin Islands, U.S.	158
26	Alabama	4,893	55	United States Minor Outlying Islands	134
27	Connecticut	4,683	56	American Samoa	38
28	Louisiana	4,335	57	Northern Mariana Islands	29
29	Utah	4,325			

*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	$2,012,806,866	30	Kansas	$58,149,297
2	Florida	$844,972,494	31	Kentucky	$57,045,801
3	New York	$777,099,358	32	Louisiana	$55,696,565
4	Texas	$763,140,903	33	South Dakota	$48,072,730
5	Georgia	$322,638,566	34	Puerto Rico	$47,424,485
6	New Jersey	$284,590,029	35	Arkansas	$46,230,114
7	Illinois	$266,742,489	36	Iowa	$42,806,846
8	Pennsylvania	$250,903,241	37	Delaware	$40,980,800
9	Alabama	$247,930,058	38	Idaho	$40,323,594
10	Arizona	$241,191,959	39	Hawaii	$35,776,983
11	Washington	$240,923,860	40	District of Columbia	$33,668,057
12	Massachusetts	$226,202,504	41	New Mexico	$32,941,959
13	Maryland	$217,880,447	42	New Hampshire	$29,322,824
14	Virginia	$205,462,224	43	Nebraska	$28,659,814
15	Ohio	$180,091,279	44	Mississippi	$28,213,583
16	Colorado	$178,389,862	45	Montana	$22,252,737
17	Michigan	$177,865,280	46	Rhode Island	$21,827,037
18	North Carolina	$175,454,536	47	Maine	$21,403,477
19	Nevada	$127,315,394	48	West Virginia	$18,200,401
20	Missouri	$118,365,728	49	Wyoming	$17,980,141
21	Tennessee	$113,713,897	50	Alaska	$16,826,999
22	Oregon	$109,917,253	51	Vermont	$15,664,834
23	Wisconsin	$108,909,445	52	North Dakota	$14,279,199
24	Minnesota	$103,771,677	53	Guam	$2,712,088
25	South Carolina	$100,256,530	54	Northern Mariana Islands	$1,950,513
26	Connecticut	$99,937,935	55	U.S. Minor Outlying Islands	$960,281
27	Utah	$98,840,388	56	Virgin Islands, U.S.	$826,913
28	Indiana	$73,678,120	57	American Samoa	$127,716
29	Oklahoma	$66,517,159			

*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	43,970	30	Alabama	1,449
2	Texas	14,449	31	Wisconsin	1,357
3	New York	12,633	32	Louisiana	1,346
4	Connecticut	12,460	33	Nebraska	1,162
5	Florida	12,080	34	Utah	1,141
6	Ohio	5,694	35	Arkansas	970
7	Virginia	5,178	36	Delaware	873
8	Maryland	4,941	37	New Mexico	825
9	Illinois	4,719	38	Kansas	777
10	North Carolina	4,670	39	Mississippi	709
11	Georgia	4,494	40	Iowa	703
12	Pennsylvania	4,273	41	West Virginia	669
13	Washington	3,923	42	Idaho	552
14	Arizona	3,824	43	Rhode Island	534
15	New Jersey	3,455	44	Alaska	502
16	District of Columbia	3,253	45	Hawaii	468
17	Colorado	3,240	46	Montana	461
18	Tennessee	2,814	47	Puerto Rico	449
19	Michigan	2,804	48	New Hampshire	366
20	Nevada	2,647	49	Maine	359
21	Massachusetts	2,419	50	Wyoming	270
22	Indiana	2,104	51	South Dakota	266
23	Vermont	2,049	52	North Dakota	216
24	South Carolina	2,031	53	Virgin Islands, U.S.	109
25	Oregon	1,927	54	U.S. Minor Outlying Islands	29
26	Oklahoma	1,763	55	Guam	18
27	Missouri	1,729	56	American Samoa	12
28	Kentucky	1,564	57	Northern Mariana Islands	8
29	Minnesota	1,450			

*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	$795,987,132	30	Minnesota	$16,941,659
2	New York	$381,303,551	31	Delaware	$14,959,552
3	Florida	$276,735,659	32	Connecticut	$13,615,568
4	Texas	$189,388,702	33	Louisiana	$12,838,337
5	Washington	$104,499,748	34	Kansas	$11,049,910
6	Georgia	$104,094,184	35	Iowa	$9,461,815
7	Massachusetts	$80,135,611	36	Arkansas	$9,230,579
8	New Jersey	$70,424,356	37	Idaho	$7,808,319
9	Illinois	$68,476,083	38	Nebraska	$7,299,573
10	Colorado	$66,916,782	39	Hawaii	$7,225,885
11	North Carolina	$59,954,187	40	Rhode Island	$6,968,585
12	Arizona	$58,156,147	41	Mississippi	$6,761,939
13	Pennsylvania	$53,459,595	42	New Mexico	$6,508,152
14	Ohio	$51,023,868	43	Wyoming	$6,394,075
15	Virginia	$50,963,875	44	New Hampshire	$6,117,893
16	Nevada	$50,922,508	45	South Dakota	$5,254,557
17	Maryland	$45,499,236	46	West Virginia	$4,271,984
18	Michigan	$37,344,490	47	Vermont	$4,171,374
19	Oklahoma	$32,362,595	48	Maine	$4,146,399
20	Alabama	$29,866,067	49	North Dakota	$3,872,298
21	Tennessee	$29,251,877	50	Montana	$3,797,256
22	Indiana	$27,604,995	51	Alaska	$3,022,295
23	Oregon	$26,368,487	52	Puerto Rico	$1,547,721
24	Wisconsin	$25,846,107	53	U.S. Minor Outlying Islands	$582,173
25	District of Columbia	$22,955,746	54	Virgin Islands, U.S.	$506,331
26	Kentucky	$22,871,600	55	Guam	$421,994
27	Missouri	$22,276,108	56	Northern Mariana Islands	$56,282
28	South Carolina	$18,583,604	57	American Samoa	$50,000
29	Utah	$17,980,983			

*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 (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 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."

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 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.).

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: 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.

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.

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

- 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.