



Federal Bureau of Investigation Internet Crime Report



2024

INTERNET CRIME COMPLAINT CENTER

CONTENTS

INTRODUCTION	3
2024 BY THE NUMBERS	4
IC3's ROLE IN COMBATTING CYBER CRIME	5
IC3 CORE FUNCTIONS	6
IC3 COMPLAINT STATISTICS	7
PAST FIVE YEARS.....	7
2024 COMPLAINTS BY AGE GROUP	8
2024 CRIME TYPES.....	9
CYBER-ENABLED FRAUD.....	11
CYBER THREATS.....	12
IC3 RECOVERY ASSET TEAM	13
POSITIVE IMPACT	14
INTERNATIONAL COMPLAINT COUNTRIES.....	16
TOP 10 STATES	17
THREE YEAR COMPLAINT COUNT COMPARISON	18
OVERALL STATE STATISTICS.....	20
CRIME TYPES BY AGE GROUPS	24
2024 IC3 ELDER FRAUD	26
COMPLAINTS FILED BY INDIVIDUALS 60+	27
CRIME TYPES REPORTED BY 60+	28
THREE YEAR COMPARISON.....	30
OVERALL STATE STATISTICS.....	32
2024 IC3 CRYPTOCURRENCY FRAUD	34
2024 IC3 CRYPTOCURRENCY FRAUD.....	35
CRIME TYPES WITH CRYPTOCURRENCY NEXUS	37
OVERALL STATE STATISTICS.....	39
APPENDIX A: ABOUT IC3	41
APPENDIX B: DEFINITIONS	42
APPENDIX C: ADDITIONAL INFORMATION ABOUT IC3 DATA	44
APPENDIX D: PUBLIC SERVICE ANNOUNCEMENTS PUBLISHED	45
APPENDIX E: EDUCATIONAL MATERIALS PUBLISHED	47

Dear Reader:

This year marks the 25th anniversary of the FBI's Internet Crime Complaint Center, or IC3. Originally intended to serve the law enforcement community, IC3 has evolved to become the primary destination for the public to report cyber-enabled crime and fraud as well as a key source for information on scams and cyber threats. Since its founding, IC3 has received over 9 million complaints of malicious activity. During its infancy, IC3 received roughly 2,000 complaints every month. For the past five years, IC3 has averaged more than 2,000 complaints every day.

As nearly all aspects of our lives have become digitally connected, the attack surface for cyber actors has grown exponentially. Scammers are increasingly using the Internet to steal Americans' hard-earned savings. And with today's technology, it can take mere taps on a keyboard to hijack networks, cripple water systems, or even rob virtual exchanges. Cryptocurrency has become an enticing means to cheat investors, launder proceeds, and engage in other illicit schemes.

Last year saw a new record for losses reported to IC3, totaling a staggering \$16.6 billion. Fraud represented the bulk of reported losses in 2024, and ransomware was again the most pervasive threat to critical infrastructure, with complaints rising 9% from 2023. As a group, those over the age of 60 suffered the most losses and submitted the most complaints.

These rising losses are even more concerning because last year, the FBI took significant actions to make it harder, and more costly, for malicious actors to succeed. We dealt a serious blow to LockBit, one of the world's most active ransomware groups. Since 2022, we have offered up thousands of decryption keys to victims of ransomware, avoiding over \$800 million in payments.

Also in 2024, we worked proactively to prevent losses and minimize victim harm through private sector collaboration and initiatives like Operation Level Up. We disbanded fraud and laundering syndicates, shut down scam call centers, shuttered illicit marketplaces, dissolved nefarious "botnets," and put hundreds of other actors behind bars. Our partnerships across the intelligence, law enforcement, and private sector communities have never been stronger.

The criminals Americans face today may look different than in years past, but they still want the same thing: to harm Americans for their own benefit. This brings me back to IC3's quarter-century milestone. While the top threats facing our country have certainly shifted over the decades, protecting American citizens—whether that means your safety, your money, or your data—remains a cornerstone of the FBI's mission.

And in the fight against increasingly savvy criminals, the FBI also relies on *you*. Without the information you report to us through IC3 or your local FBI Field Office, we simply cannot piece together the puzzle of this ever-shifting threat landscape. If ever you suspect you're a victim of cyber-enabled crime, do not hesitate to let us know. We want to be there for you, and what you report will help us help others.



B. Chad Yarbrough
Operations Director for Criminal and Cyber
Federal Bureau of Investigation

2024 BY THE NUMBERS¹



859,532

Total Complaints in 2024



**\$16.6
Billion**

Losses in 2024



33%

Increase in Losses from 2023



256,256

Complaints with Actual Loss



\$19,372

Average Loss

¹ Accessibility description: Image depicts key statistics regarding complaints and losses. In 2024, complaints totaled 859,532, with losses of \$16.6 billion, representing a 33 percent increase from 2023. 256,256 complaints reported an actual loss. For complaints, the average reported loss was \$19,372.

IC3's ROLE IN COMBATTING CYBER CRIME²



² Accessibility description: Image lists 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 FBI's LEEP website.

IC3 CORE FUNCTIONS³



COLLECTION

IC3 is the central point for Internet crime victims to report and alert the appropriate agencies to suspected cybercriminal activity. Victims are encouraged and often directed by law enforcement to file a complaint online at www.ic3.gov. Complainants are asked to document accurate and complete information related to suspected cyber-enabled crime, as well as any other relevant information.



ANALYSIS

IC3 reviews and analyzes data submitted through its website to identify emerging threats and new trends. In addition, IC3 can quickly alert financial institutions to fraudulent transactions which enables the freezing of victim funds if certain reporting criteria are met.



PUBLIC AWARENESS

Public service announcements, industry alerts, and other publications outlining specific scams are posted to the www.ic3.gov website. As more people become aware of cyber-enabled crimes and the methods used to carry them out, potential victims are equipped with a broader understanding of the dangers associated with Internet activity and are in a better position to avoid falling prey to schemes online.



REFERRALS

IC3 aggregates related complaints to build referrals, which are forwarded to local, state, federal, and international law enforcement agencies for potential investigation. If law enforcement investigates and determines a crime has been committed, legal action may be brought against the perpetrator.

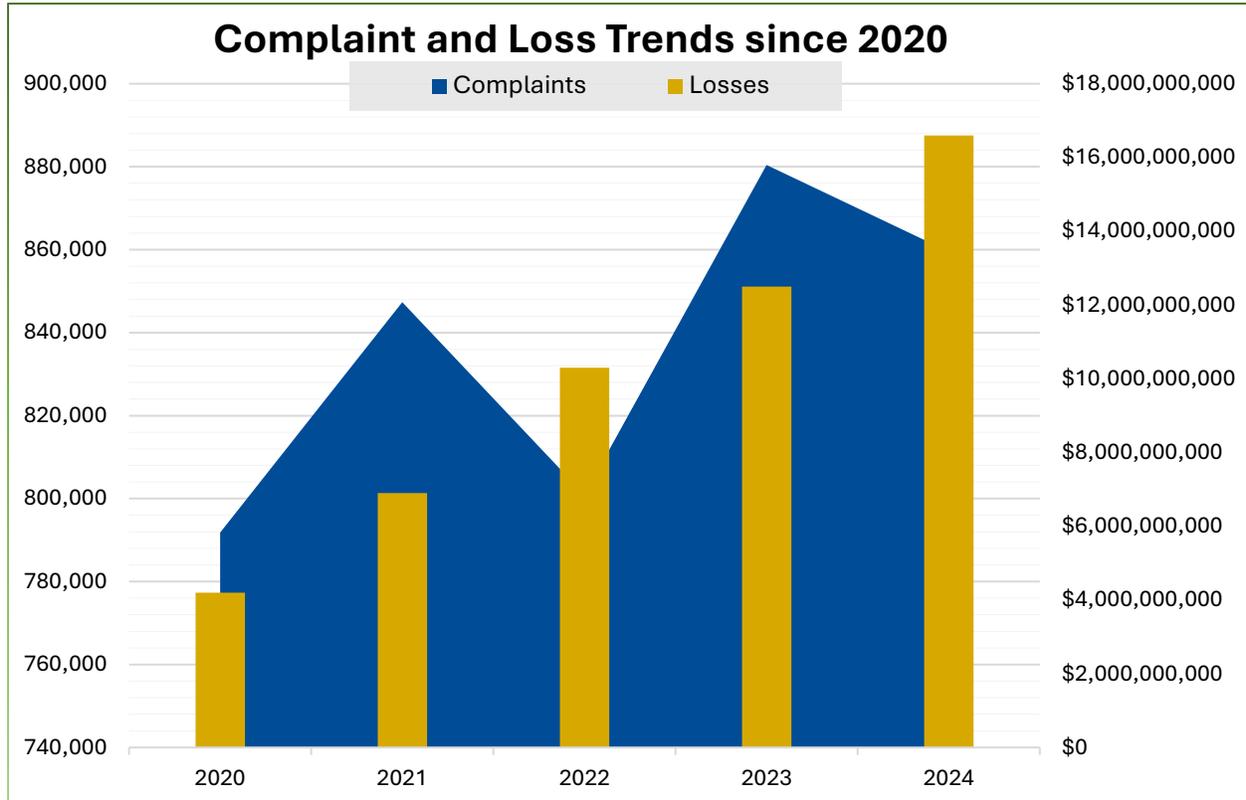
³ Accessibility description: Image contains icons with the core functions. Core functions - Collection, Analysis, Public Awareness, and Referrals - are listed in individual blocks as components of an ongoing process.

IC3 COMPLAINT STATISTICS

PAST FIVE YEARS

IC3 has received an average of 836,000 complaints per year. These complaints address a wide array of Internet scams affecting individuals around the globe.

4



5

IC3 COMPLAINTS - PAST FIVE YEARS

**4.2 Million
Complaints**

**\$50.5 Billion
in Losses**

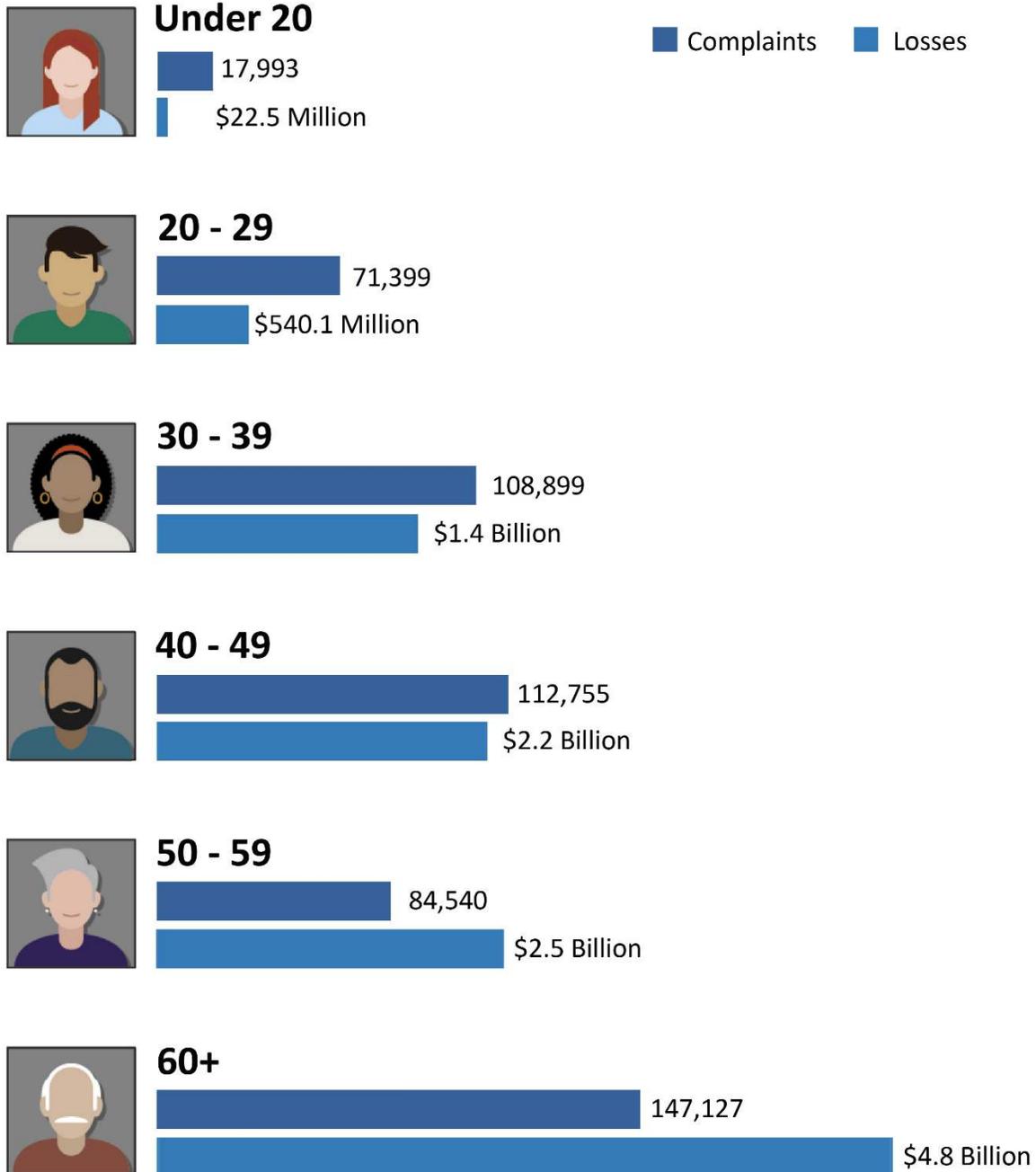
836,000 Average

Since 2000, the IC3 has received more than 9 million complaints.

⁴ Accessibility description: Chart describes complaint counts and losses over a 5-year period.

⁵ Accessibility description: Chart includes yearly and aggregate data for complaints and losses over the years 2020 to 2024. Over this time, IC3 received a total of 4.2 million complaints, a reported loss of \$50.5 billion, and an average of 836,000 complaints received per year. Since 2000, IC3 has received more than 9 million complaints. * Please see Appendix C for more information regarding IC3 data.

2024 COMPLAINTS BY AGE GROUP ⁶



⁶ Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix C for more information regarding IC3 data. Accessibility description: Chart shows number of complaints and losses by age group. Under 20: 17,993 complaints, \$22.5 million in losses; 20-29: 71,399 complaints, \$540.1 million in losses; 30-39: 108,899 complaints, \$1.4 billion in losses; 40-49: 112,755 complaints, \$2.2 billion in losses; 50-59: 84,540 complaints, \$2.5 billion in losses; 60+: 147,127 complaints, \$4.8 billion in losses.

2024 CRIME TYPES

BY COMPLAINT COUNT			
Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441
<i>Descriptor**</i>			
Cryptocurrency	149,686		

*IPR: Intellectual Property Rights

** This descriptor relates to the medium or tool used to facilitate the crime and used by IC3 for tracking purposes only. It is available as a descriptor only after a crime type has been selected.

Please see Appendix C for more information regarding IC3 data.

2024 CRIME TYPES *continued***BY COMPLAINT LOSS**

Crime Type	Loss	Crime Type	Loss
Investment	\$6,570,639,864	Extortion	\$143,185,736
Business Email Compromise	\$2,770,151,146	Lottery/Sweepstakes/ Inheritance	\$102,212,250
Tech Support	\$1,464,755,976	Advanced Fee	\$102,074,512
Personal Data Breach	\$1,453,296,303	Phishing/Spoofing	\$70,013,036
Non-Payment/Non-Delivery	\$785,436,888	SIM Swap	\$25,983,946
Confidence/Romance	\$672,009,052	Overpayment	\$21,452,521
Government Impersonation	\$405,624,084	Ransomware *	\$12,473,156
Data Breach	\$364,855,818	Harassment/Stalking	\$10,611,223
Other	\$280,278,325	Botnet	\$8,860,202
Employment	\$264,223,271	IPR/Copyright and Counterfeit	\$8,715,512
Credit Card/Check Fraud	\$199,889,841	Threats of Violence	\$1,842,186
Identity Theft	\$174,354,745	Malware	\$1,365,945
Real Estate	\$173,586,820	Crimes Against Children	\$519,424

*Descriptor***

Cryptocurrency \$9,322,335,911

* 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 FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to FBI via IC3 and does not account for the entity directly reporting to FBI field offices/agents.

** This descriptor relates to the medium or tool used to facilitate the crime and is used by IC3 for tracking purposes only. It is available as a descriptor only after a crime type has been selected.

Please see Appendix C for more information regarding IC3 data.

CYBER-ENABLED FRAUD

Cyber-enabled fraud includes complaints where criminals use the Internet or other technology to commit fraudulent activities, often involving the theft of money, data, or identity, or the creation of counterfeit goods or services. Cyber-enabled fraud is responsible for almost 83% of all losses reported to IC3 in 2024. ⁷

CYBER-ENABLED FRAUD in 2024

333,981 Complaints	\$13.7 Billion Losses	38% of 2024 Complaints	83% of 2024 Losses
------------------------------	---------------------------------	----------------------------------	------------------------------



8

TRENDS

<p>Call Center Scams 53,369 complaints; \$1.9 billion in losses FBI Warns of Scammers Impersonating Cryptocurrency Exchanges Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash...</p>	<p>Emergency Scams 357 complaints; \$2.7 million in losses FBI Warns of Scammers Targeting Senior Citizens in Grandparent Scams... Telephone Scam Alleging a Relative is in a Financial or Legal Crisis</p>
<p>Toll Scams 59,271 complaints; \$129,624 in losses Smishing Scam Regarding Debt for Road Toll Services</p>	<p>Gold Courier Scams 525 complaints; \$219 million in losses Scammers Use Couriers to Retrieve Cash and Precious Metals...</p>

⁷Accessibility description: Chart describes totals for crime types generally considered to be cyber-enabled fraud: 333,981 complaints; \$13.7 billion in losses; 38% of 2024 complaints received; 83% of 2024 losses. * Please see Appendix C for more information regarding IC3 data.

⁸ Accessibility description: Chart describes counts and losses for crime types generally considered to be cyber-enabled fraud.

CYBER THREATS

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include ransomware, viruses and malware, data breaches, Denial of Service (DoS) attacks, and other attack vectors. IC3 received more than 4,800 complaints from organizations belonging to a critical infrastructure sector that were affected by a cyber threat. The most reported cyber threats among critical infrastructure organizations were ransomware and data breaches.

CYBER THREATS in 2024

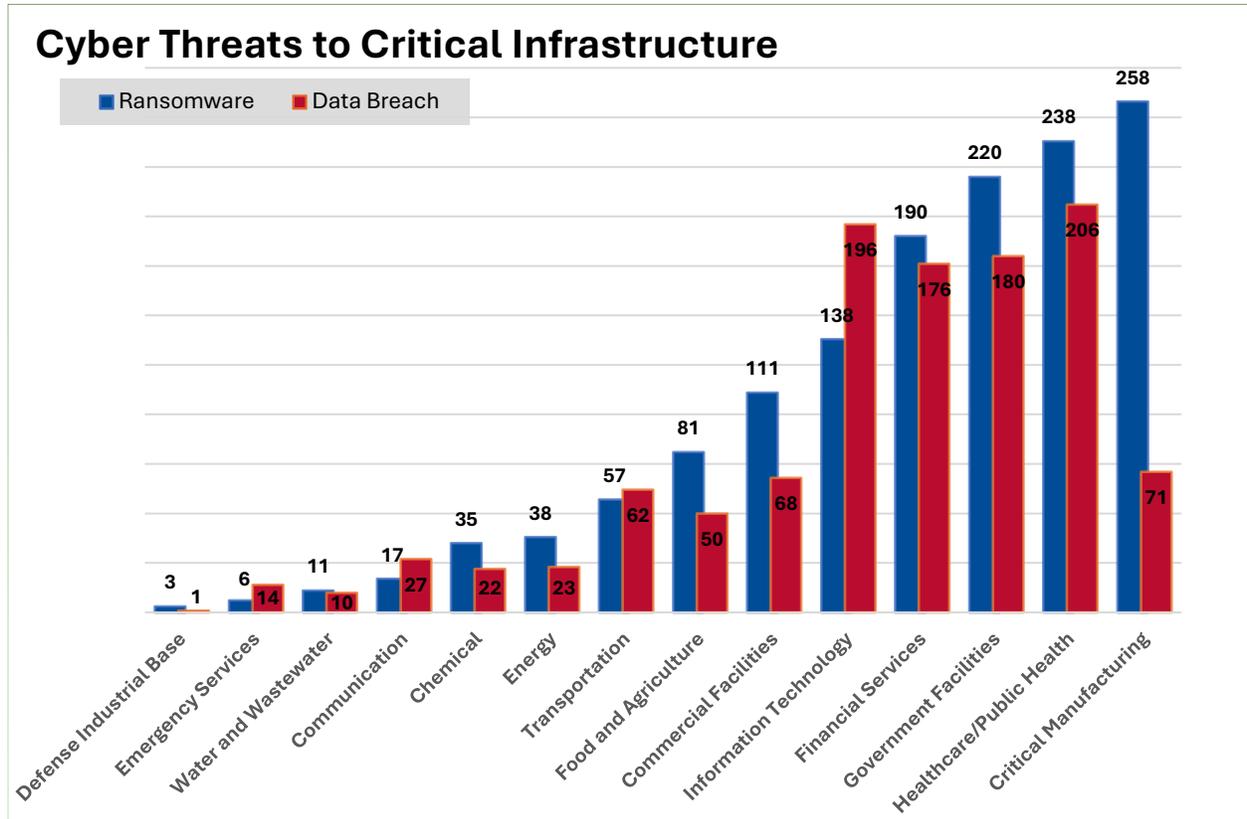
263,455
Complaints

\$1.571 billion
in Losses

Critical Infrastructure
4,878 Complaints

Top Five Ransomware Variants by IC3 Complaints

1. Akira
2. LockBit
3. RansomHub
4. FOG
5. PLAY



⁹ Accessibility description: This chart outlines cyber threat complaints in 2024: 263,455 complaints; \$1.571 billion in losses; 4,878 complaints from critical infrastructure. The five most reported ransomware variants: Akira, LockBit, RansomHub, FOG, and PLAY.

¹⁰ Accessibility description: This chart outlines the number of ransomware and data breach complaints filed by the critical infrastructure sectors.

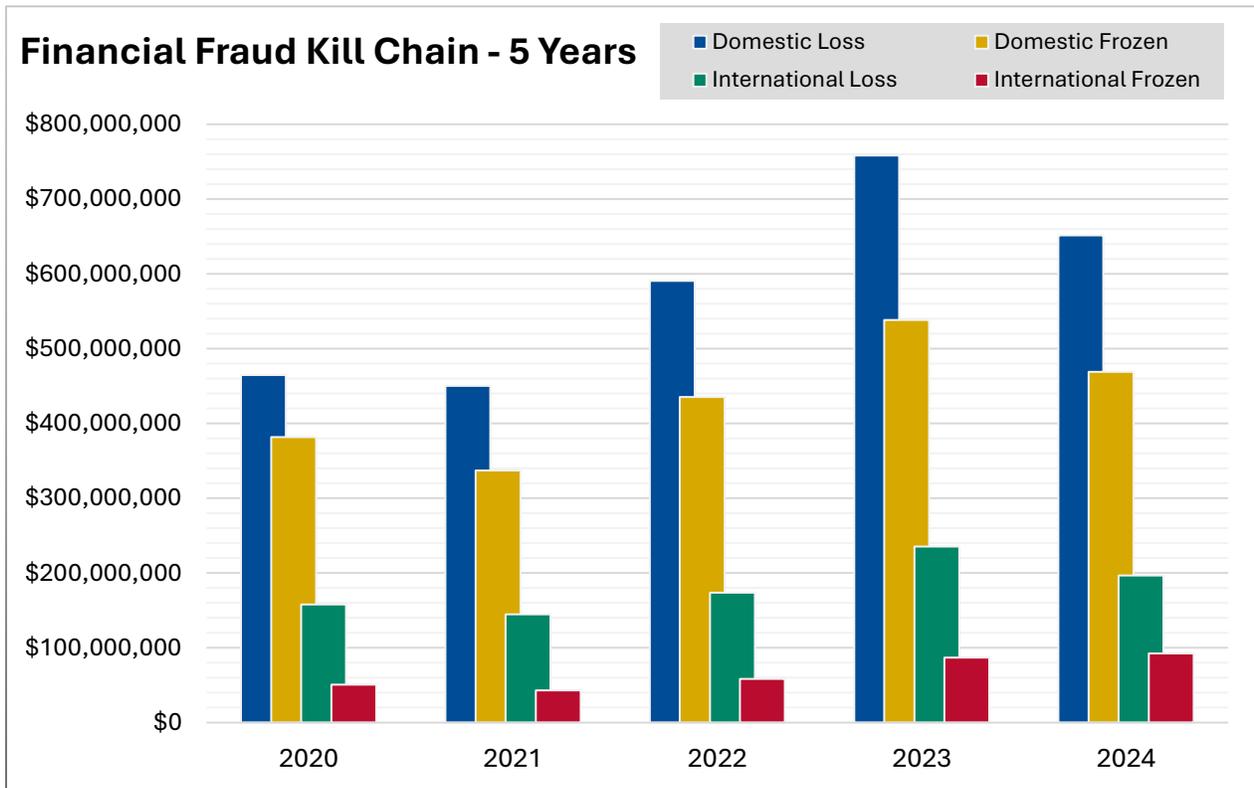
IC3 RECOVERY ASSET TEAM



11

Established in 2018, the IC3 Recovery Asset Team streamlines communications with financial institutions and FBI field offices to assist in the freezing of funds for victims of fraudulent domestic and international transactions via the Financial Fraud Kill Chain. Most Financial Fraud Kill Chain incidents initiated by the IC3 RAT are Business Email Compromise (BEC). The Financial Fraud Kill Chain can also be initiated for Tech Support Fraud, Romance Scams, and Data Breaches. The Recovery Asset Team assumed responsibility for domestic-to-international transactions in April 2024. The International Financial Fraud Kill Chain is a partnership between federal law enforcement and financial entities whose purpose is to freeze fraudulent funds wired by victims. International requests are coordinated through the Financial Crimes Enforcement Network Rapid Response Team and law enforcement entities, including FBI LEGAT offices and international law enforcement partners.

12



¹¹ Accessibility description: Chart describes FFKC activity in 2024: 3,020 complaints attempted for \$848.4 million. Domestic: 2,651 complaints, \$469.1 million frozen; International: 369 complaints, \$92.5 million frozen; 66% success rate.

¹² Accessibility description: Chart describes FFKC domestic and international frozen and loss amounts from 2020 to 2024.

POSITIVE IMPACT

Operation Level Up

Launched in January 2024, Operation Level Up identified victims of cryptocurrency investment fraud and notified them of the scam. The operation was initiated with the support of agents from FBI and the U.S. Secret Service. Cryptocurrency investment fraud, also known as "pig butchering," is a confidence-based scam. Subjects target victims online and develop a relationship before introducing a fraudulent investment opportunity in cryptocurrency. Victims are coached to invest more and more money into what appears to be an extremely profitable platform, only to be unable to withdraw their funds.

Success Stories

Utilizing IC3 complaint data, Operation Level Up reported:

- 4,323 victims of cryptocurrency investment fraud were notified.
- 76% of those victims were unaware they were being scammed.
- Estimated savings to victims of \$285,639,989.
- 42 victims referred to an FBI victim specialist for suicide intervention.

Read More About It

[Operation Level-Up: How the FBI Is Saving Victims from Cryptocurrency Investment Fraud](#)
[Operation Level Up — FBI](#)

Call Center Fraud

Illegal call centers defraud thousands of victims each year. Two categories of call center fraud reported to the IC3 are Tech/Customer Support and Government Impersonation.

DOJ, FBI, and Central Bureau of Investigation:

Since 2022, the DOJ, FBI, and IC3 have collaborated with law enforcement in India, such as the Central Bureau of Investigation (CBI) in New Delhi and local Indian states, to combat cyber-enabled financial crimes and transnational call center fraud.

In 2024, law enforcement in India conducted multiple call center raids, disruptions, seizures, and arrests of the individuals alleged to be involved in perpetrating these crimes.

FBI Washington Field Office participated in two media series aimed at bringing awareness to call center fraud.

Success Stories

FBI responded to over 38 requests from law enforcement in India and provided approximately 60 actionable leads. FBI enabled over 215 arrests through 11 joint operations with the CBI and other local law enforcement in 2024. This represented a 700% increase in arrests from 2023, the first full year of the collaboration. FBI conducted hundreds of interviews and continues to support Indian law enforcement efforts and prosecution of call centers perpetrating these frauds.

Read More About It

[Tech/Customer Support and Government Impersonation](#)

POSITIVE IMPACT

Ransomware

IC3 recognized 67 new ransomware variants in 2024. The most reported of these new variants were:

- FOG
- Lynx
- Cicada 3301
- Dragonforce
- Frag

IC3 provides this information to FBI Field Offices to help identify new ransomware variants, discover the enterprises the threat actors are targeting, and determine whether critical infrastructure is being targeted.

Success Story

FBI Boston, February 2024: Authorities seized www.warzone.ws and three related domains, which together offered for sale the Warzone RAT malware — a sophisticated remote access trojan capable of enabling cybercriminals to surreptitiously connect to victims' computers for malicious purposes. The Warzone RAT provided cybercriminals the ability to browse victim file systems, take screenshots, record keystrokes, steal victim usernames and passwords, and watch victims through web cameras, all without the victims' knowledge or permission.

Read More About It

[International Cybercrime Malware Service Dismantled by Federal Authorities: Key Malware Sales and Support Actors in Malta and Nigeria Charged in Federal Indictments | United States Department of Justice Charged in Federal Indictments](#)

Financial Fraud Kill Chain

The IC3 Recovery Asset Team streamlines communications with financial institutions and FBI field offices to assist in the freezing of funds for victims of fraudulent domestic and international transactions.

FBI Denver, March 2024: The Recovery Asset Team received a complaint reporting a BEC involving a real estate transaction. The individuals were in the process of purchasing property and received a spoofed email from their supposed real estate agents requesting that they wire \$956,342 to a U.S. domestic bank to finalize the closing. Two days after the wire was initiated, the victims realized the instructions came from a spoofed email. Upon notification, the Recovery Asset Team immediately initiated the process to freeze the fraudulent recipient bank account. The transfer of \$955,060 was stopped and the money was returned to the individuals.

Success Story

LEGAT Singapore, September 2024: The Recovery Asset Team received a request from LEGAT Singapore regarding a transaction sent to a U.S. domestic recipient bank in the amount of \$6,661,650 due to a BEC incident. The Recovery Asset Team initiated the Financial Fraud Kill Chain request to the domestic recipient bank, who blocked the account and froze a total of \$5,100,000 for recovery. Funds not available were wired out immediately upon deposit to accounts located in Spain and China. Efforts by the domestic recipient bank were made to potentially recover those wires as well.

Read More About It

[SPF | International Cooperation Leading To The Interception Of Over USD 5 Million Linked To Business Email Compromise Scam](#)

INTERNATIONAL COMPLAINT COUNTRIES

13

IC3 received complaints from more than 200 countries in 2024.

TOP 20 FOREIGN COUNTRIES WITH CITIZENS SUBMITTING COMPLAINTS TO IC3			
Country	Complaints	Country	Complaints
United Kingdom	102,692	Mexico	1,116
Canada	6,951	South Africa	1,075
India	4,189	Pakistan	979
France	2,223	Indonesia	895
Philippines	1,790	Italy	761
Australia	1,533	Sweden	732
Germany	1,524	China	651
Japan	1,492	Turkey	649
Brazil	1,472	Spain	639
Honduras	1,352	Netherlands	598

Transactional information provided in IC3 complaints also helps identify where funds are going when victims are directed to send funds overseas.

14



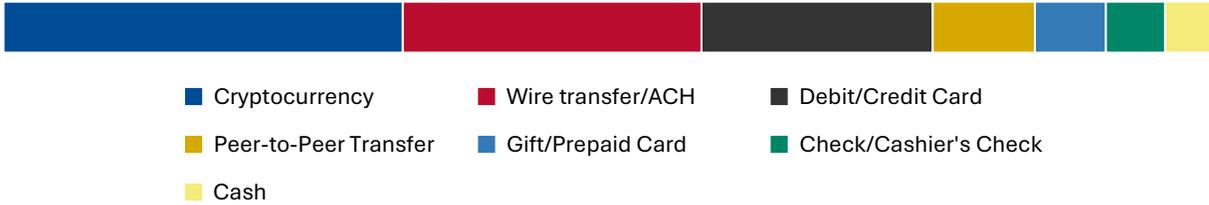
¹³ Accessibility description: Charts list the top 20 countries by number of total complaints submitted to IC3, aside from the U.S. Please see Appendix C for more information regarding IC3 data.

¹⁴ Accessibility description: Chart shows the countries with the highest number of reported fraudulent wire transactions in 2024.

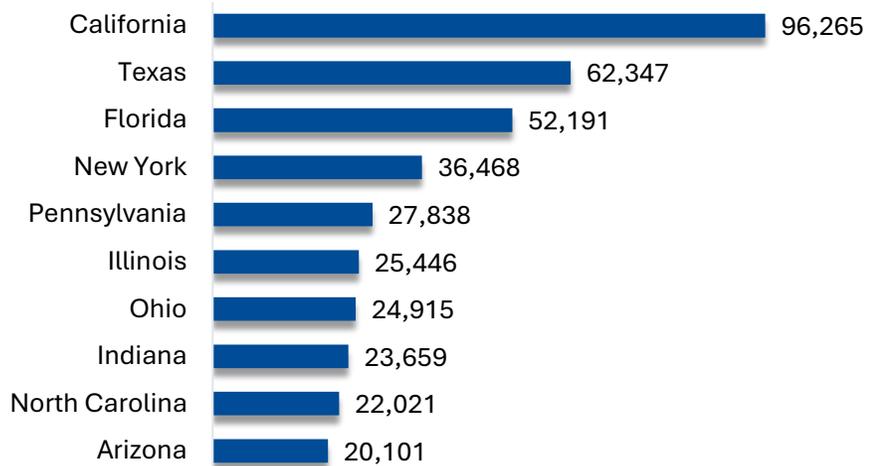
TOP REPORTED TRANSACTION TYPES¹⁵

Transaction information provided in IC3 complaints helps FBI understand how victims are losing funds to fraud and assists the Recovery Asset Team Financial Fraud Kill Chain process when complaints are filed as quickly as possible. This chart identifies the top ways complainants reported financial loss in fraud.

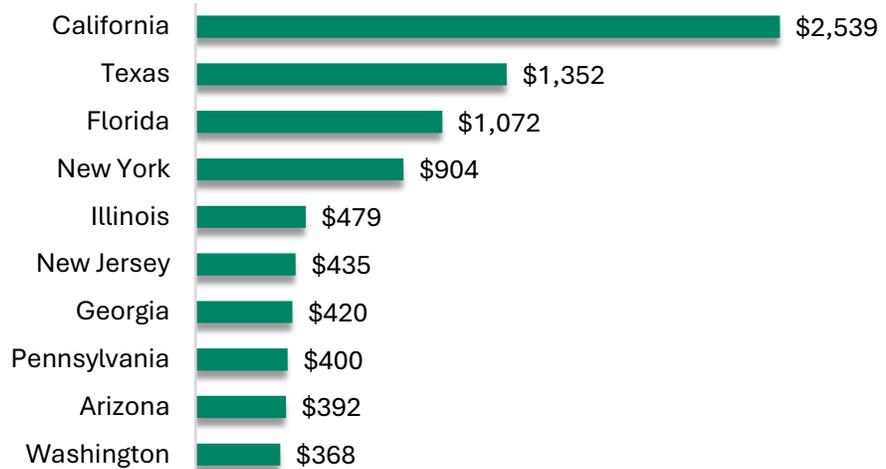
Top Ways Funds Are Lost in Fraud



TOP 10 STATES BY NUMBER OF COMPLAINTS¹⁶



TOP 10 STATES BY LOSS (IN MILLIONS)¹⁷



¹⁵ Accessibility description: Chart depicts the top reported transaction types: Cryptocurrency, Wire transfer/ACH, Debit/Credit Card, Peer-to-Peer, Check/Cashier's Check, Gift/Prepaid Card, and Cash.

¹⁶ Accessibility description: Chart depicts the top 10 states based on number of complaints. These include California, Texas, Florida, New York, Pennsylvania, Illinois, Ohio, Indiana, North Carolina, and Arizona. Please see Appendix C for more information regarding IC3 data.

¹⁷ Accessibility description: Chart depicts the top 10 states based on reported losses are labeled. These include California, Texas, Florida, New York, Illinois, New Jersey, Georgia, Pennsylvania, Arizona, and Washington. Please see Appendix C for more information regarding IC3 data.

THREE YEAR COMPLAINT COUNT COMPARISON

BY COMPLAINT COUNT			
Crime Type	2024	2023	2022
Advanced Fee	7,097	8,045	11,264
Business Email Compromise	21,442	21,489	21,832
Botnet	587	540	568
Confidence Fraud/Romance	17,910	17,823	19,021
Credit Card/Check Fraud	12,876	13,718	22,985
Crimes Against Children	4,472	2,361	2,587
Data Breach	3,204	3,727	2,795
Employment	20,044	15,443	14,946
Extortion	86,415	48,223	39,416
Government Impersonation	17,367	14,190	11,554
Harassment/Stalking	11,672	9,587	11,779
Identity Theft	21,403	19,778	27,922
Investment	47,919	39,570	30,529
IPR/Copyright and Counterfeit	1,583	1,498	2,183
Lottery/Sweepstakes/Inheritance	3,690	4,168	5,650
Malware	441	659	762
Non-Payment/Non-Delivery	49,572	50,523	51,679
Other	12,318	8,808	9,966
Overpayment	2,705	4,144	6,183
Personal Data Breach	64,882	55,851	58,859
Phishing/Spoofing	193,407	298,878	321,136
Ransomware	3,156	2,825	2,385
Real Estate	9,359	9,521	11,727
SIM Swap	982	1,075	2,026
Tech Support	36,002	37,560	32,538
Threats of Violence	1,360	1,697	2,224

THREE YEAR COMPLAINT LOSS COMPARISON

BY COMPLAINT LOSS			
Crime Type	2024	2023	2022
Advanced Fee	\$102,074,512	\$134,516,577	\$104,325,444
Business Email Compromise	\$2,770,151,146	\$2,946,830,270	\$2,742,354,049
Botnet	\$8,860,202	\$22,422,708	\$17,099,378
Confidence Fraud/Romance	\$672,009,052	\$652,544,805	\$735,882,192
Credit Card/Check Fraud	\$199,889,841	\$173,627,614	264,148,905
Crimes Against Children	\$519,424	\$2,031,485	\$577,464
Data Breach	\$364,855,818	\$534,397,222	\$459,321,859
Employment	\$264,223,271	\$70,234,079	\$52,204,269
Extortion	\$143,185,736	\$74,821,835	\$54,335,128
Government Impersonation	\$405,624,084	\$394,050,518	\$240,553,091
Harassment/Stalking	\$10,611,223	\$9,677,332	\$5,621,402
Identity Theft	\$174,354,745	\$126,203,809	189,205,793
Investment	\$6,570,639,864	\$4,570,275,683	\$3,311,742,206
IPR/Copyright and Counterfeit	\$8,715,512	\$7,555,329	\$4,591,177
Lottery/Sweepstakes/Inheritance	\$102,212,250	\$94,502,836	\$83,602,376
Malware	\$1,365,945	\$1,213,317	\$9,326,482
Non-Payment/Non-Delivery	\$785,436,888	\$309,648,416	\$281,770,073
Other	\$280,278,325	\$240,053,059	\$117,686,789
Overpayment	\$21,452,521	\$27,955,195	\$38,335,772
Personal Data Breach	\$1,453,296,303	\$744,219,879	\$742,438,136
Phishing/Spoofing	\$70,013,036	\$18,728,550	\$160,015,411
Ransomware	\$12,473,156	\$59,641,384	\$34,353,237
Real Estate	\$173,586,820	\$145,243,348	\$396,932,821
SIM Swap	\$25,983,946	\$48,798,103	\$72,652,571
Tech Support	\$1,464,755,976	\$924,512,658	\$806,551,993
Threats of Violence	\$1,842,186	\$13,531,178	\$4,972,099

OVERALL STATE STATISTICS

COMPLAINTS BY STATE*					
Rank	State	Complaints	Rank	State	Complaints
1	California	96,265	30	Alaska	6,770
2	Texas	62,347	31	Louisiana	6,455
3	Florida	52,191	32	Kentucky	6,165
4	New York	36,468	33	Connecticut	5,695
5	Pennsylvania	27,838	34	Kansas	4,797
6	Illinois	25,446	35	Arkansas	4,240
7	Ohio	24,915	36	New Mexico	3,884
8	Indiana	23,659	37	District of Columbia	3,856
9	North Carolina	22,021	38	Idaho	3,081
10	Arizona	20,101	39	Mississippi	3,068
11	Georgia	19,797	40	Delaware	2,806
12	Washington	18,009	41	Hawaii	2,603
13	Virginia	17,466	42	Nebraska	2,603
14	Michigan	16,302	43	West Virginia	2,594
15	New Jersey	15,701	44	New Hampshire	2,340
16	Maryland	14,996	45	Puerto Rico	2,241
17	Colorado	14,848	46	Maine	2,137
18	Massachusetts	14,254	47	Montana	1,854
19	Tennessee	11,411	48	Rhode Island	1,642
20	Nevada	10,716	49	Wyoming	1,377
21	Missouri	10,028	50	South Dakota	1,298
22	South Carolina	9,661	51	Vermont	937
23	Wisconsin	9,619	52	North Dakota	885
24	Minnesota	9,264	53	U.S. Minor Outlying Islands	170
25	Oregon	9,011	54	Guam	96
26	Alabama	7,840	55	American Samoa	91
27	Oklahoma	7,479	56	Virgin Islands, U.S.	87
28	Iowa	7,193	57	Northern Mariana Islands	21
29	Utah	6,877			

* Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia for which the complainant provided state information. Please see Appendix C for more information regarding IC3 data.

OVERALL STATE STATISTICS *CONTINUED*

LOSSES BY STATE*					
Rank	State	Loss	Rank	State	Loss
1	California	\$2,539,041,635	30	Alabama	\$103,771,880
2	Texas	\$1,351,598,183	31	Puerto Rico	\$91,363,707
3	Florida	\$1,071,909,632	32	Louisiana	\$87,411,457
4	New York	\$903,975,003	33	Kansas	\$80,300,908
5	Illinois	\$479,054,271	34	New Mexico	\$76,621,670
6	New Jersey	\$434,856,424	35	Kentucky	\$73,919,940
7	Georgia	\$420,454,472	36	Iowa	\$72,860,333
8	Pennsylvania	\$400,082,312	37	Mississippi	\$65,613,936
9	Arizona	\$392,441,717	38	Idaho	\$63,035,342
10	Washington	\$368,203,209	39	Hawaii	\$55,180,901
11	Massachusetts	\$338,872,378	40	New Hampshire	\$52,811,455
12	North Carolina	\$324,287,947	41	Arkansas	\$51,714,039
13	Virginia	\$317,406,595	42	Nebraska	\$46,730,894
14	District of Columbia	\$291,531,458	43	Wyoming	\$43,502,744
15	Ohio	\$278,038,028	44	Delaware	\$37,611,598
16	Nevada	\$268,769,310	45	Montana	\$31,603,407
17	Colorado	\$243,517,403	46	Maine	\$31,455,797
18	Michigan	\$241,737,979	47	Alaska	\$26,296,803
19	Maryland	\$238,976,904	48	South Dakota	\$24,957,446
20	Minnesota	\$203,352,530	49	West Virginia	\$24,196,661
21	Tennessee	\$190,271,310	50	Rhode Island	\$23,597,036
22	Missouri	\$183,751,987	51	North Dakota	\$21,831,953
23	Wisconsin	\$169,942,495	52	Vermont	\$11,285,112
24	South Carolina	\$146,468,765	53	Guam	\$2,532,544
25	Oregon	\$144,160,344	54	Virgin Islands, U.S.	\$1,441,830
26	Connecticut	\$143,884,002	55	U.S. Minor Outlying Islands	\$1,107,380
27	Utah	\$129,414,310	56	American Samoa	\$195,182
28	Indiana	\$125,093,323	57	Northern Mariana Islands	\$121,874
29	Oklahoma	\$113,724,886			

* Note: This information is based on the total losses from complaints in each state, American Territory, and the District of Columbia for which the complainant provided state information. Please see Appendix C for more information regarding IC3 data.

OVERALL STATE STATISTICS *CONTINUED***COMPLAINTS PER 100K CITIZENS***

Rank	State	Count	Rank	State	Count
1	Alaska	914.7	27	Georgia	177.1
2	District of Columbia	549.1	28	South Carolina	176.3
3	Indiana	341.7	29	New Hampshire	166.1
4	Nevada	328.0	30	New Jersey	165.3
5	Delaware	266.8	31	Montana	163.0
6	Arizona	265.1	32	Kansas	161.5
7	Colorado	249.2	33	Wisconsin	161.4
8	California	244.1	34	Michigan	160.8
9	Maryland	239.4	35	Missouri	160.6
10	Wyoming	234.3	36	Minnesota	159.9
11	Washington	226.3	37	Tennessee	157.9
12	Florida	223.3	38	Connecticut	155.0
13	Iowa	221.9	39	Idaho	153.9
14	Pennsylvania	212.8	40	Maine	152.1
15	Oregon	210.9	41	Alabama	152.0
16	Ohio	209.7	42	Rhode Island	147.6
17	Illinois	200.2	43	West Virginia	146.6
18	Massachusetts	199.7	44	Vermont	144.5
19	North Carolina	199.4	45	Louisiana	140.4
20	Texas	199.3	46	South Dakota	140.4
21	Virginia	198.2	47	Arkansas	137.3
22	Utah	196.3	48	Kentucky	134.4
23	New York	183.6	49	Nebraska	129.8
24	Oklahoma	182.6	50	North Dakota	111.1
25	New Mexico	182.3	51	Mississippi	104.2
26	Hawaii	180.0	52	Puerto Rico	70.0

* Note: This information is based on the estimated 2024 Census estimated data and the total number of complaints from each state, the District of Columbia, and Puerto Rico for which the complainant provided state information. Please see Appendix C for more information regarding IC3 data. <https://www.census.gov/data/tables/time-series/demo/pepstat/2020s-state-total.html#v2024>

OVERALL STATE STATISTICS *CONTINUED*

LOSSES PER 100K CITIZENS*					
Rank	State	Loss	Rank	State	Loss
1	District of Columbia	\$41,513,914	27	Pennsylvania	\$3,059,025
2	Nevada	\$8,225,617	28	Missouri	\$2,942,166
3	Wyoming	\$7,403,235	29	North Carolina	\$2,935,789
4	California	\$6,439,159	30	Puerto Rico	\$2,852,179
5	Arizona	\$5,175,704	31	Wisconsin	\$2,850,918
6	Massachusetts	\$4,748,658	32	Montana	\$2,778,974
7	Washington	\$4,626,726	33	Oklahoma	\$2,776,898
8	Florida	\$4,586,256	34	North Dakota	\$2,740,752
9	New Jersey	\$4,577,026	35	Kansas	\$2,703,183
10	New York	\$4,550,077	36	South Dakota	\$2,699,068
11	Texas	\$4,319,470	37	South Carolina	\$2,673,358
12	Colorado	\$4,087,582	38	Tennessee	\$2,632,511
13	Connecticut	\$3,915,137	39	Michigan	\$2,383,896
14	Hawaii	\$3,815,721	40	Ohio	\$2,339,737
15	Maryland	\$3,815,560	41	Nebraska	\$2,330,178
16	Illinois	\$3,769,066	42	Iowa	\$2,247,743
17	Georgia	\$3,760,478	43	Maine	\$2,238,828
18	New Hampshire	\$3,748,066	44	Mississippi	\$2,229,457
19	Utah	\$3,693,739	45	Rhode Island	\$2,121,448
20	Virginia	\$3,602,310	46	Alabama	\$2,011,980
21	New Mexico	\$3,596,829	47	Louisiana	\$1,901,183
22	Delaware	\$3,575,529	48	Indiana	\$1,806,591
23	Alaska	\$3,552,983	49	Vermont	\$1,740,206
24	Minnesota	\$3,510,223	50	Arkansas	\$1,674,485
25	Oregon	\$3,374,247	51	Kentucky	\$1,611,028
26	Idaho	\$3,149,218	52	West Virginia	\$1,367,059

* Note: This information is based on the estimated 2024 Census estimated data and the total number of complaints from each state, the District of Columbia, and Puerto Rico for which the complainant provided state information. Please see Appendix C for more information regarding IC3 data. <https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html#v2024>

CRIME TYPES BY AGE GROUPS

COUNTS	UNDER 20	20 - 29	30 - 39	40 - 49	50 - 59
Advanced Fee	220	971	1,102	968	1,009
Business Email Compromise	90	800	2,058	2,934	3,047
Botnet	74	99	79	55	42
Confidence/Romance	272	1,219	1,814	2,056	2,365
Credit Card/Check Fraud	295	1,206	1,690	1,641	1,642
Crimes Against Children	1,367	140	73	58	28
Data Breach	33	147	358	523	402
Employment	604	3,674	2,916	2,003	1,516
Extortion	6,540	13,811	6,180	4,305	3,620
Government Impersonation	161	1,462	1,894	1,818	1,711
Harassment/Stalking	548	1,667	1,998	1,619	990
Identity Theft	288	1,922	3,550	3,163	2,688
Investment	399	3,453	6,822	6,873	5,797
IPR/Copyright and Counterfeit	24	146	216	198	168
Lottery/Sweepstakes/ Inheritance	31	168	298	343	708
Malware	47	86	113	89	66
Non-Payment/ Non-Delivery	1,691	7,644	8,436	7,466	5,848
Other	318	883	1,375	1,187	909
Overpayment	314	776	507	456	449
Personal Data Breach	1,335	6,312	10,756	9,870	7,008
Phishing/Spoofing	203	1,088	1,532	1,701	2,060
Ransomware	12	62	120	211	253
Real Estate	150	1,749	1,407	1,088	1,011
SIM Swap	7	58	185	213	172
Spoofing	127	615	955	902	1,045
Tech Support	279	1,928	2,537	2,794	3,584
Threats of Violence	118	254	326	249	168
Cryptocurrency	858	6,277	10,885	10,338	8,953

* 60+ crime type information is available in the 2024 IC3 Elder Fraud Report.

CRIME TYPES BY AGE GROUPS

LOSSES	UNDER 20	20 - 29	30 - 39	40 - 49	50 - 59
Advanced Fee	\$289,546	\$4,479,321	\$9,638,362	\$16,770,456	\$12,970,490
Business Email Compromise	\$11,067,986	\$30,611,039	\$207,186,022	\$302,370,195	\$361,651,832
Botnet	\$60	\$30,718	\$2,691	\$17,303,168	\$2,001
Confidence/Romance	\$759,616	\$11,016,901	\$31,008,972	\$46,027,157	\$82,466,829
Credit Card/Check Fraud	\$687,043	\$4,581,387	\$9,861,167	\$25,602,871	\$21,660,432
Crimes Against Children	\$95,862	\$4,292	\$45,366	\$29,655	\$499,469
Data Breach	\$970,279	\$3,251,108	\$64,898,844	\$43,983,317	\$15,586,514
Employment	\$1,971,457	\$13,138,194	\$15,419,807	\$9,874,429	\$10,102,359
Extortion	\$2,080,479	\$11,799,104	\$8,777,342	\$8,984,024	\$7,784,643
Government Impersonation	\$2,008,033	\$34,354,239	\$30,281,258	\$20,880,418	\$18,727,179
Harassment/Stalking	\$51,719	\$676,809	\$2,185,563	\$2,699,273	\$649,797
Identity Theft	\$269,690	\$4,522,239	\$13,036,661	\$17,427,975	\$12,879,363
Investment	\$13,571,240	\$154,183,205	\$540,646,646	\$616,072,673	\$871,842,750
IPR/Copyright and Counterfeit	\$4,302	\$61,107	\$780,863	\$1,662,760	\$2,851,670
Lottery/Sweepstakes/Inheritance	\$28,558	\$732,222	\$2,118,356	\$3,512,077	\$3,856,993
Malware	\$18,056	\$43,693	\$59,168	\$202,908	\$135,302
Non-Payment/Non-Delivery	\$1,578,742	\$19,895,195	\$40,383,092	\$54,348,415	\$49,535,571
Other	\$1,366,980	\$11,369,781	\$22,380,525	\$15,665,583	\$16,411,270
Overpayment	\$1,006,792	\$2,055,986	\$2,799,535	\$2,737,512	\$2,570,057
Personal Data Breach	\$635,038	\$20,180,645	\$115,301,927	\$224,444,555	\$108,826,649
Phishing/Spoofing	\$35,368	\$1,229,413	\$2,726,832	\$2,612,598	\$2,751,552
Ransomware	\$0	\$12,548	\$37,660	\$187,680	\$517,222
Real Estate	\$413,752	\$4,784,750	\$6,623,054	\$9,331,733	\$22,466,504
SIM Swap	\$0	\$800,617	\$6,752,902	\$6,250,788	\$5,080,192
Spoofing	\$780,878	\$876,082	\$2,624,922	\$3,054,743	\$3,665,661
Tech Support	\$1,007,672	\$14,019,656	\$25,573,715	\$48,163,755	\$48,548,923
Threats of Violence	\$4,181	\$7,908	\$6,063,974	\$65,817	\$331,395
Cryptocurrency	\$14,745,598	\$169,240,044	\$695,761,773	\$851,201,069	\$904,569,789

* 60+ crime type information is available in the 2024 IC3 Elder Fraud Report.

2024 Elder Fraud



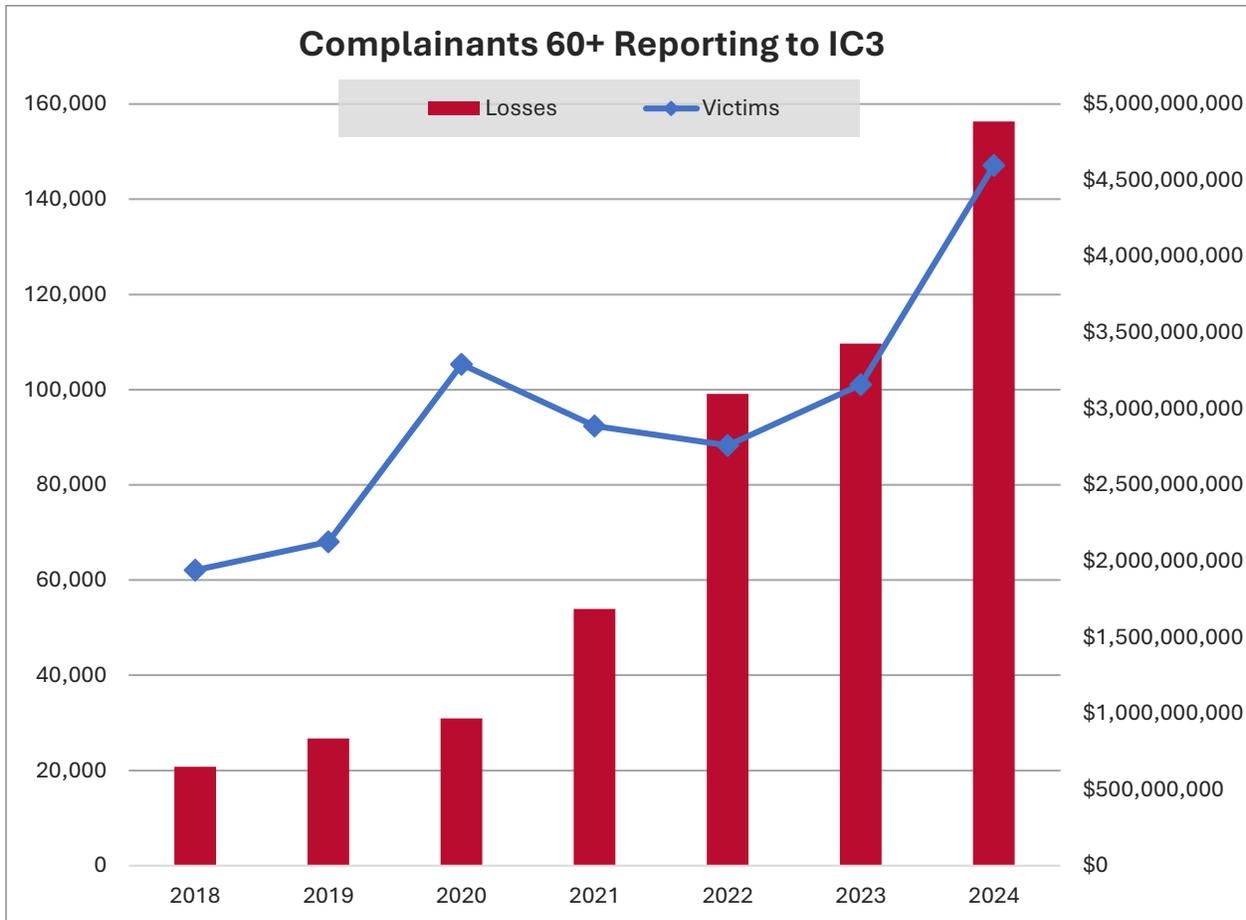
INTERNET CRIME COMPLAINT CENTER

COMPLAINTS FILED BY INDIVIDUALS 60+

18



19



¹⁸ Charts describe count and loss trends for those 60+ from 2018 to 2024.

¹⁹ Accessibility Description: Chart describes counts and losses for those reporting as 60+ from 2018 to 2024.

CRIME TYPES REPORTED BY 60+

COMPLAINANTS 60+			
Crime Type	Count	Crime Type	Count
Phishing/Spoofing	23,252	Advanced Fee	1,897
Tech Support	16,777	Real Estate	1,765
Extortion	12,618	Lottery/Sweepstakes/Inheritance	1,711
Personal Data Breach	9,827	Harassment/Stalking	696
Investment	9,448	Overpayment	527
Non-Payment/Non-Delivery	7,646	Data Breach	300
Confidence/Romance	7,626	Ransomware	208
Government Impersonation	4,521	SIM Swap	205
Identity Theft	4,064	IPR/Copyright and Counterfeit	163
Business Email Compromise*	3,300	Threats of Violence	111
Credit Card/Check Fraud	3,226	Malware	45
Other	2,017	Crimes Against Children	25
Employment	1,928	Botnet	23
Descriptor**			
Cryptocurrency	33,369		

*Regarding Business Email Compromise counts: A whole number is given to depict the overall complaint count and includes when a 60+ complainant may be reporting on behalf of a business or personally.

** This descriptor relates to the medium or tool used to facilitate the crime and are used by IC3 for tracking purposes only. It is available only after a crime type has been selected. Please see Appendix C for more information regarding IC3 data.

CRIME TYPES REPORTED BY 60+ *Continued*

COMPLAINANTS 60+ LOSSES			
Crime Type	Loss	Crime Type	Loss
Investment	\$1,834,242,515	Data Breach	\$28,546,213
Tech Support	\$982,440,006	Identity Theft	\$28,463,106
Confidence/Romance	\$389,312,356	Extortion	\$24,901,693
Business Email Compromise*	\$385,001,099	Phishing/Spoofing	\$20,202,521
Personal Data Breach	\$254,187,196	SIM Swap	\$6,342,329
Government Impersonation	\$208,096,366	Overpayment	\$5,900,921
Other	\$111,300,637	IPR/Copyright and Counterfeit	\$1,076,710
Non-Payment/Non-Delivery	\$76,794,753	Harassment/Stalking	\$713,693
Real Estate	\$76,324,236	Threats of Violence	\$300,488
Lottery/Sweepstakes/Inheritance	\$75,897,926	Crimes Against Children	\$231,600
Advanced Fee	\$41,622,868	Malware	\$187,911
Employment	\$37,882,347	Ransomware**	\$43,199
Credit Card/Check Fraud	\$33,813,267	Botnet	\$14,852
Descriptor***			
Cryptocurrency	\$2,839,333,197		

* Regarding Business Email Compromise losses: A whole number is given to depict the overall complaint count and includes when a 60+ complainant may be reporting on behalf of a business or personally.

** 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 FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to FBI via IC3 and does not account for the entity directly reporting to FBI field offices/agents.

*** This descriptor relates to the medium or tool used to facilitate the crime and used by IC3 for tracking purposes only. It is available only after a crime type has been selected. Please see Appendix C for more information regarding IC3 data.

THREE YEAR COMPARISON

60+ COMPLAINT COUNT			
Crime Type	2024	2023	2022
Advanced Fee	1,897	1,951	3,153
Business Email Compromise	3,300	3,080	3,938
Botnet	23	17	33
Confidence Fraud/Romance	7,626	6,740	7,166
Credit Card/Check Fraud	3,226	3,182	4,956
Crimes Against Children	25	26	84
Data Breach	300	336	333
Employment	1,928	1,079	1,286
Extortion	12,618	5,396	4,285
Government Impersonation	4,521	3,517	3,425
Harassment/Stalking	696	568	754
IPR/Copyright and Counterfeit	163	152	235
Identity Theft	4,064	3,010	4,825
Investment	9,448	6,443	4,661
Lottery/Sweepstakes/Inheritance	1,711	1,771	2,388
Malware	45	67	125
Non-Payment/Non-Delivery	7,646	6,693	7,985
Other	2,017	1,447	2,016
Overpayment	527	698	1,183
Personal Data Breach	9,827	7,333	7,849
Phishing/Spoofing	23,252	2,856	8,369
Ransomware	208	175	215
Real Estate	1,765	1,498	1,862
SIM Swap	205	174	301
Tech Support	16,777	17,696	17,810
Threats of Violence	111	115	166
Cryptocurrency	33,369	16,968	9,991

THREE YEAR COMPARISON, *Continued*

60+ COMPLAINT LOSSES			
Crime Type	2024	2023	2022
Advanced Fee	\$41,622,868	\$67,923,263	\$49,322,099
Business Email Compromise	\$385,001,099	\$382,372,731	\$477,342,728
Botnet	\$14,852	\$23,142	\$120,621
Confidence Fraud/Romance	\$389,312,356	\$356,888,968	\$419,768,142
Credit Card/Check Fraud	\$33,813,267	\$37,862,023	\$61,649,198
Crimes Against Children	\$231,600	\$1,159,939	\$48,373
Data Breach	\$28,546,213	\$23,913,130	\$17,681,749
Employment	\$37,882,347	\$6,835,684	\$6,403,021
Extortion	\$24,901,693	\$23,093,451	\$15,555,047
Government Impersonation	\$208,096,366	\$179,646,103	\$136,500,338
Harassment/Stalking	\$713,693	\$1,930,347	\$254,659
IPR/Copyright and Counterfeit	\$1,076,710	\$183,169	\$203,140
Identity Theft	\$28,463,106	\$34,551,900	\$42,653,578
Investment	\$1,834,242,515	\$1,243,010,600	\$990,235,119
Lottery/Sweepstakes/Inheritance	\$75,897,926	\$67,396,206	\$69,845,106
Malware	\$187,911	\$261,144	\$1,851,421
Non-Payment/Non-Delivery	\$76,794,753	\$59,018,965	\$51,531,615
Other	\$111,300,637	\$72,707,042	\$31,410,237
Overpayment	\$5,900,921	\$7,496,049	\$10,977,231
Personal Data Breach	\$254,187,196	\$109,724,027	\$127,736,607
Phishing/Spoofing	\$20,202,521	\$3,355,436	\$36,715,205
Ransomware	\$43,199	\$635,548	\$210,052
Real Estate	\$76,324,236	\$65,634,851	\$135,239,020
SIM Swap	\$6,342,329	\$15,148,072	\$19,515,629
Tech Support	\$982,440,006	\$589,759,770	\$587,831,698
Threats of Violence	\$300,488	\$5,128,768	\$376,458
Cryptocurrency	\$2,839,333,197	\$1,653,484,444	\$1,088,330,051

OVERALL STATE STATISTICS

COUNTS BY STATE FROM COMPLAINTS FILED BY INDIVIDUALS 60+*					
Rank	State	Count	Rank	State	Count
1	California	18,091	30	Kentucky	1,336
2	Florida	11,902	31	Connecticut	1,209
3	Texas	9,473	32	New Mexico	1,150
4	Arizona	6,683	33	Kansas	1,129
5	Pennsylvania	6,353	34	Arkansas	1,063
6	New York	6,225	35	Iowa	803
7	Illinois	6,064	36	Idaho	775
8	Ohio	5,388	37	Hawaii	647
9	Indiana	5,324	38	New Hampshire	633
10	North Carolina	5,031	39	Maine	608
11	Virginia	3,841	40	Mississippi	604
12	Washington	3,692	41	West Virginia	594
13	Georgia	3,622	42	Nebraska	551
14	Maryland	3,231	43	Delaware	514
15	Massachusetts	3,224	44	Alaska	466
16	Michigan	3,148	45	Montana	438
17	Colorado	3,128	46	Rhode Island	324
18	New Jersey	2,918	47	Puerto Rico	285
19	Tennessee	2,543	48	District of Columbia	267
20	Nevada	2,299	49	Wyoming	267
21	South Carolina	2,293	50	South Dakota	259
22	Oregon	2,288	51	Vermont	243
23	Missouri	2,199	52	North Dakota	174
24	Oklahoma	1,858	53	U.S. Minor Outlying Islands	39
25	Minnesota	1,836	54	Guam	20
26	Wisconsin	1,785	55	Virgin Islands, U.S.	17
27	Utah	1,762	56	Northern Mariana Islands	2
28	Alabama	1,567	57	American Samoa	1
29	Louisiana	1,372			

* Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia for which the complainant provided state information. Please see Appendix C for more information regarding IC3 data.

OVERALL STATE STATISTICS, *Continued*

LOSSES BY STATE FROM COMPLAINTS FILED BY INDIVIDUALS 60+*					
Rank	State	Loss	Rank	State	Loss
1	California	\$832,710,048	30	Iowa	\$34,991,114
2	Texas	\$489,790,386	31	Alabama	\$33,200,314
3	Florida	\$388,436,198	32	Connecticut	\$30,918,559
4	New York	\$257,658,301	33	New Mexico	\$30,034,919
5	District of	\$251,454,544	34	Mississippi	\$28,870,444
6	Arizona	\$190,686,835	35	Arkansas	\$27,253,501
7	Georgia	\$174,744,201	36	Kentucky	\$26,139,251
8	Pennsylvania	\$151,096,514	37	Kansas	\$23,511,153
9	Illinois	\$133,794,241	38	Nebraska	\$21,414,248
10	New Jersey	\$133,397,512	39	Puerto Rico	\$20,183,422
11	Washington	\$107,052,160	40	Hawaii	\$18,851,052
12	Virginia	\$106,575,141	41	Idaho	\$18,663,392
13	Massachusetts	\$99,804,762	42	New Hampshire	\$15,840,854
14	Ohio	\$95,441,773	43	Maine	\$12,980,616
15	Michigan	\$92,378,793	44	Delaware	\$12,293,619
16	North Carolina	\$87,449,567	45	Montana	\$12,056,193
17	Nevada	\$81,400,930	46	South Dakota	\$8,975,829
18	Maryland	\$80,128,654	47	Wyoming	\$8,648,675
19	Colorado	\$74,760,501	48	Alaska	\$8,173,395
20	Missouri	\$63,530,750	49	Rhode Island	\$6,309,411
21	Tennessee	\$61,882,884	50	West Virginia	\$5,790,489
22	South Carolina	\$58,581,997	51	North Dakota	\$5,781,845
23	Minnesota	\$52,262,721	52	Vermont	\$4,177,269
24	Wisconsin	\$50,525,457	53	U.S. Minor Outlying	\$670,314
25	Oklahoma	\$50,203,394	54	Guam	\$592,965
26	Oregon	\$48,116,839	55	Virgin Islands, U.S.	\$163,884
27	Utah	\$44,155,961	56	American Samoa	\$3,000
28	Louisiana	\$37,512,993	57	Northern Mariana Islands	\$120
29	Indiana	\$37,209,947			

* Note: This information is based on the total losses in each state, American Territory, and the District of Columbia for which the complainant provided state information. Please see Appendix C for more information regarding IC3 data.

2024 Cryptocurrency Fraud



INTERNET CRIME COMPLAINT CENTER

2024 IC3 CRYPTOCURRENCY FRAUD

CRYPTOCURRENCY FRAUD - 2024

20

149,686
Complaints

\$9.3 Billion in
Losses

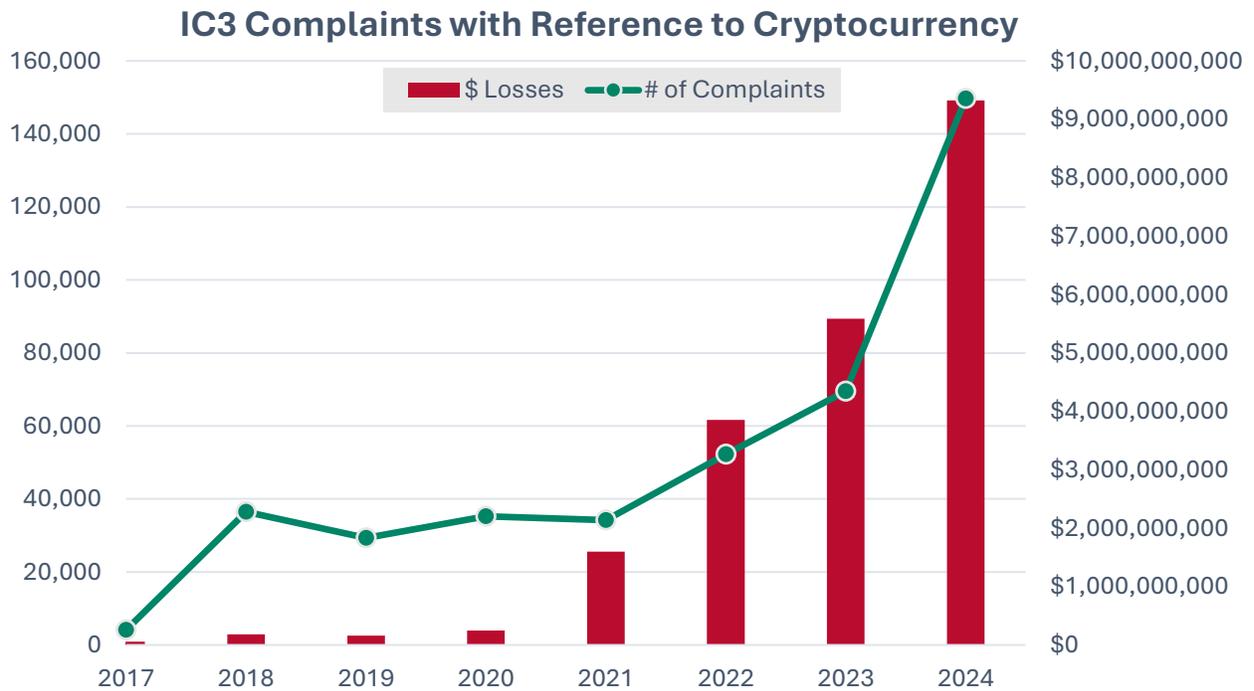
66% Increase
in Losses

Largest Age
Group: 60+

COMPLAINTS REFERENCING CRYPTOCURRENCY

AGE RANGE ²¹	COUNT	LOSS
Under 20	1,819	\$7,778,157
20 - 29	13,591	\$370,443,345
30 - 39	22,218	\$1,006,382,458
40 - 49	22,555	\$1,462,040,974
50 - 59	19,317	\$1,184,912,854
Over 60	33,369	\$2,839,333,197

22



²⁰ Accessibility description: Chart outlines cryptocurrency complaints in 2024: 149,686 complaints; \$9.3 billion in losses; 66% increase in loss; largest age group to report is 60+.

²¹ Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix C for more information regarding IC3 data.

²² Chart outlines the number of cryptocurrency related complaints from 2017 to 2024.

CRYPTOCURRENCY in FRAUD TRENDS

Cryptocurrency Investment	CRYPTO INVESTMENT FRAUD by AGE GROUP		
	Age Group	Count	Losses
41,557 Complaints; \$5.8 Billion in Losses -----	Under 20	303	\$3,307,216
29% Increase in Complaints from 2023	20 - 29	2,906	\$273,447,400
47% Increase in Losses from 2023 -----	30 - 39	6,217	\$373,696,736
The FBI Warns of a Spike in Cryptocurrency Investment Schemes	40 - 49	7,145	\$1,053,964,645
	50 - 59	6,364	\$811,298,119
	Over 60	8,043	\$1,600,353,509

Cryptocurrency ATMs/Kiosks	REPORTS of CRYPTO ATM/KIOSK USE by AGE GROUP		
	Age Group	Count	Losses
10,956 Complaints; \$246.7 Million in Losses -----	Under 20	7	\$51,913
99% Increase in Complaints from 2023	20 - 29	280	\$3,739,620
31% Increase in Losses from 2023 -----	30 - 39	361	\$4,241,387
The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment	40 - 49	319	\$3,621,774
	50 - 59	349	\$5,523,230
	Over 60	2,674	\$107,206,251

CRIME TYPES MOST ASSOCIATED WITH CRYPTO ATM USE					
	Count	Losses		Count	Losses
Extortion	4,189	\$5,601,953	Government Impersonation	1,786	\$44,587,335
Tech Support	3,037	\$107,429,709	Investment	606	\$38,090,269

Extortion/Sextortion	EXTORTION / SEXTORTION by AGE GROUP		
	Age Group	Count	Losses
54,936 Complaints; \$33.5 Million in Losses -----	Under 20	3,806	\$1,006,975
59% Increase in Complaints from 2023	20 - 29	13,302	\$5,471,516
9% Increase in Losses from 2023 -----	30 - 39	9,204	\$5,473,072
Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes	40 - 49	6,794	\$3,726,438
	50 - 59	4,940	\$2,899,089
	Over 60	5,903	\$7,821,886

CRIME TYPES WITH CRYPTOCURRENCY NEXUS

COMPLAINTS			
Crime Type	Count	Crime Type	Count
Extortion	47,054	Identity Theft	527
Investment	41,557	Credit Card/Check Fraud	389
Personal Data Breach	11,644	Ransomware	389
Tech Support	11,129	Lottery/Sweepstakes/Inheritance	329
Employment	6,533	Business Email Compromise	256
Phishing/Spoofing	3,938	Real Estate	256
Confidence/Romance	3,811	SIM Swap	215
Government Impersonation	3,585	Harassment/Stalking	211
Non-Payment/Non-Delivery	2,492	Overpayment	186
Advanced Fee	1,537	Malware	53
Other	1,315	Botnet	44
Data Breach	846	Crimes Against Children	42
Descriptor*			
Cryptocurrency	149,686		

* This descriptor relates to the medium or tool used to facilitate the crime and are used by IC3 for tracking purposes only. It is available only after a crime type has been selected. Please see Appendix C for more information regarding IC3 data.

CRIME TYPES WITH CRYPTOCURRENCY NEXUS *Continued*

LOSSES			
Crime Type	Loss	Crime Type	Loss
Investment	\$5,819,531,069	SIM Swap	\$28,463,106
Personal Data Breach	\$1,120,793,009	Credit Card/Check Fraud	\$24,901,693
Tech Support	\$961,998,313	Identity Theft	\$20,202,521
Confidence/Romance	\$237,151,771	Lottery/Sweepstakes/ Inheritance	\$6,342,329
Employment	\$197,224,612	Real Estate	\$5,900,921
Data Breach	\$167,874,424	Ransomware*	\$1,076,710
Government Impersonation	\$146,057,054	Botnet	\$713,693
Extortion	\$96,072,767	Overpayment	\$300,488
Business Email Compromise	\$63,882,699	Harassment/Stalking	\$231,600
Other	\$63,516,319	Malware	\$187,911
Non-Payment/Non-Delivery	\$55,139,529	IPR/Copyright and Counterfeit	\$43,199
Advanced Fee	\$36,436,824	Threats of Violence	\$289,288
Phishing/Spoofing	\$28,546,213	Crimes Against Children	\$19,174
Descriptor**			
Cryptocurrency	\$9,322,335,911		

* Regarding Ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, equipment, or any third-party remediation services acquired by a complainant. In some cases, complainants do not report any loss amount to FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what complainants report to FBI via IC3 and does not account for complainants directly reporting to FBI field offices/agents.

** This descriptor relates to the medium or tool used to facilitate the crime and are used by IC3 for tracking purposes only. It is available only after a crime type has been selected. Please see Appendix C for more information regarding IC3 data.

OVERALL STATE STATISTICS

CRYPTOCURRENCY COMPLAINTS BY STATE*					
Rank	State	Count	Rank	State	Count
1	California	19,508	30	Kentucky	1,196
2	Texas	11,270	31	Louisiana	1,165
3	Florida	10,698	32	New Mexico	885
4	New York	8,053	33	Kansas	862
5	Pennsylvania	4,355	34	Idaho	835
6	Illinois	4,319	35	Arkansas	775
7	New Jersey	4,259	36	Hawaii	709
8	Washington	4,169	37	Iowa	668
9	Arizona	4,145	38	Mississippi	582
10	Virginia	4,016	39	New Hampshire	547
11	North Carolina	3,684	40	Nebraska	541
12	Georgia	3,533	41	District of Columbia	534
13	Ohio	3,371	42	Alaska	453
14	Colorado	3,218	43	Maine	429
15	Maryland	3,158	44	Montana	421
16	Massachusetts	3,015	45	Delaware	406
17	Michigan	3,009	46	West Virginia	406
18	Tennessee	2,354	47	Rhode Island	329
19	Nevada	2,153	48	Puerto Rico	278
20	Oregon	2,070	49	South Dakota	254
21	Wisconsin	1,973	50	Wyoming	250
22	Missouri	1,951	51	Vermont	207
23	South Carolina	1,944	52	North Dakota	184
24	Indiana	1,880	53	U.S. Minor Outlying Islands	28
25	Minnesota	1,852	54	Guam	15
26	Utah	1,658	55	Virgin Islands, U.S.	13
27	Connecticut	1,361	56	American Samoa	5
28	Alabama	1,313	57	Northern Mariana Islands	3
29	Oklahoma	1,208			

* 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 C for more information regarding IC3 data.

OVERALL STATE STATISTICS, *Continued*

CRYPTOCURRENCY LOSSES BY STATE*					
Rank	State	Loss	Rank	State	Loss
1	California	\$1,393,628,996	30	Louisiana	\$49,306,020
2	Texas	\$738,583,341	31	Kansas	\$49,045,398
3	Florida	\$584,746,970	32	Indiana	\$48,009,883
4	New York	\$375,087,857	33	New Mexico	\$43,269,446
5	Illinois	\$272,633,678	34	Oklahoma	\$37,752,198
6	District of Columbia	\$262,640,821	35	Wyoming	\$36,386,737
7	New Jersey	\$236,721,074	36	Idaho	\$35,149,916
8	Pennsylvania	\$218,642,276	37	Kentucky	\$32,907,797
9	Washington	\$204,694,032	38	Hawaii	\$24,893,821
10	Massachusetts	\$201,530,349	39	Nebraska	\$23,094,744
11	Georgia	\$197,647,537	40	New Hampshire	\$22,699,416
12	Nevada	\$185,521,892	41	Arkansas	\$20,654,583
13	Arizona	\$177,578,809	42	Iowa	\$20,350,712
14	North Carolina	\$174,411,615	43	Delaware	\$19,973,180
15	Virginia	\$158,769,093	44	Maine	\$17,137,660
16	Maryland	\$132,730,401	45	Mississippi	\$14,505,794
17	Colorado	\$130,631,488	46	South Dakota	\$13,811,508
18	Michigan	\$126,330,606	47	Montana	\$12,900,561
19	Ohio	\$123,379,667	48	Rhode Island	\$12,556,877
20	Missouri	\$93,029,140	49	Alaska	\$11,780,664
21	Minnesota	\$91,614,693	50	North Dakota	\$7,700,246
22	Tennessee	\$82,748,140	51	West Virginia	\$7,686,156
23	Puerto Rico	\$71,185,851	52	Vermont	\$4,265,121
24	Oregon	\$68,159,115	53	U.S. Minor Outlying Islands	\$874,714
25	Utah	\$68,133,250	54	Guam	\$751,009
26	Wisconsin	\$67,513,795	55	Virgin Islands, U.S.	\$324,580
27	South Carolina	\$60,529,485	56	American Samoa	\$145,182
28	Connecticut	\$59,749,544	57	Northern Mariana Islands	\$16,946
29	Alabama	\$51,273,598			

* 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 C for more information regarding IC3 data.

APPENDIX A: ABOUT IC3

Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities. FBI is 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, FBI leverages IC3 as a mechanism to gather intelligence on cybercrime so that we can provide the public and our many partners with information, services, support, training, and leadership to stay ahead of the threat.

Every day, IC3 receives thousands of complaints reporting a wide array of scams, many of them targeting our most vulnerable populations. The information submitted to 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 FBI to connect complaints, investigate reported crimes, track trends and threats, and, in some cases, even freeze stolen funds. Just as importantly, 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.

IC3 was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include cyber threats and cyber-enabled fraud in their many forms including ransomware, intrusions (hacking), extortion, international money laundering, investment fraud, and a growing list of crimes. As of publication, IC3 has received over 9 million complaints. 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.

To promote public awareness and as part of its prevention mission, 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 IC3.gov interface. Their efforts help IC3 and FBI better protect their fellow citizens.

Frauds and scams will continue to evolve, but many characteristics of these schemes remain the same even as new trends develop. Review previous IC3 Annual Reports and Public Service Announcements (PSAs) to further educate and protect yourself, as well as your family, friends, and community.

APPENDIX B: DEFINITIONS

Advanced Fee Fraud: 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 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 Fraud: An individual believes they are legitimately employed and loses money, or launders money/items during 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 to collect or extort money.

Harassment/Stalking: Repeated words, conduct, and/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 Fraud: 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.).

Intellectual Property Rights (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 Fraud: 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 Fraud: 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).

Other: Criminal or civil matters not currently designated as an IC3 crime type.

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 Fraud: 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 Fraud: 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 C: ADDITIONAL INFORMATION ABOUT IC3 DATA

- As appropriate, complaints are reviewed by IC3 analysts, who apply descriptive data, such as crime type and adjusted loss.
- Descriptive data for complaints, such as crime type or loss, is variable and can evolve based upon investigative or analytical proceedings. Statistics are an assessment taken at a point in time, which may change.
- Complainants are not required to provide an age range.
- Each complaint will only have one crime type.
- Complainant 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.

APPENDIX D: PUBLIC SERVICE ANNOUNCEMENTS PUBLISHED

Title	Date
Chinese Police Imposters Incorporate Aggressive Tactics to Target U.S.-Based Chinese Community	1/3/2024
Malicious Actors Threaten U.S. Synagogues, Schools, Hospitals, and Other Institutions with Bomb Threats	1/12/2024
Scammers Use Couriers to Retrieve Cash and Precious Metals from Victims of Tech Support and Government Impersonation Scams	1/29/2024
IC3 Annual Report and Fraud Flyer	3/18/2024
Child Sexual Abuse Material Created by Generative AI and Similar Online Tools is Illegal	3/29/2024
Cyber Criminals Target Victims Using Social Engineering Techniques	4/11/2024
Smishing Scam Regarding Debt for Road Toll Services	4/12/2024
Alert on Cryptocurrency Money Services Businesses	4/25/2024
New Verification Schemes Target Users of Online Dating Platforms	4/26/2024
Foreign Terrorist Organizations and their Supporters Likely Heighten Threat Environment during 2024 Pride Month	5/10/2024
Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue	5/16/2024
Guidance on the 911 S5 Residential Proxy Service	5/29/2024
Scammers Defraud Individuals via Work-From-Home Scams	6/4/2024
Fictitious Law Firms Targeting Cryptocurrency Scam Victims Offering to Recover Funds	6/24/2024
Scammers Falsely Promise Significant Profit to Victims in Collectible Coin Scams	6/25/2024
DDoS Attacks: Could Hinder Access to Election Information, Would Not Prevent Voting	7/31/2024
FBI Warns of Scammers Impersonating Cryptocurrency Exchanges	8/1/2024
Safety Concern Related to Recent Trend in Financial Institution Customer Fraud Scheme	8/2/2024
Just So You Know: Ransomware Disruptions during Voting Periods Will Not Impact the Security and Resiliency of Vote Casting or Counting	8/15/2024
North Korea Aggressively Targeting Crypto Industry with Well-Disguised Social Engineering Attacks	9/3/2024
Business Email Compromise: The \$55 Billion Scam	9/11/2024

Just So You Know: False Claims of Hacked Voter Information Likely Intended to Sow Distrust of U.S. Elections	9/12/2024
Anniversary of October 7, 2023, HAMAS Attacks May Motivate Individuals to Violence in the United States	10/4/2024
Counterfeit Check Scam Targets Law Firms Via Debt Collection Scheme	10/8/2024
Just So You Know: Foreign Threat Actors Likely to Use a Variety of Tactics to Develop and Spread Disinformation During 2024 U.S. General Election Cycle	10/18/2024
Scammers Exploit 2024 US General Election to Perpetrate Multiple Fraud Schemes	10/29/2024
Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud	12/3/2024

APPENDIX E: EDUCATIONAL MATERIALS PUBLISHED



WARNING

Before you click on a link or make a payment, remember to **CHECK, CALL, WAIT**:

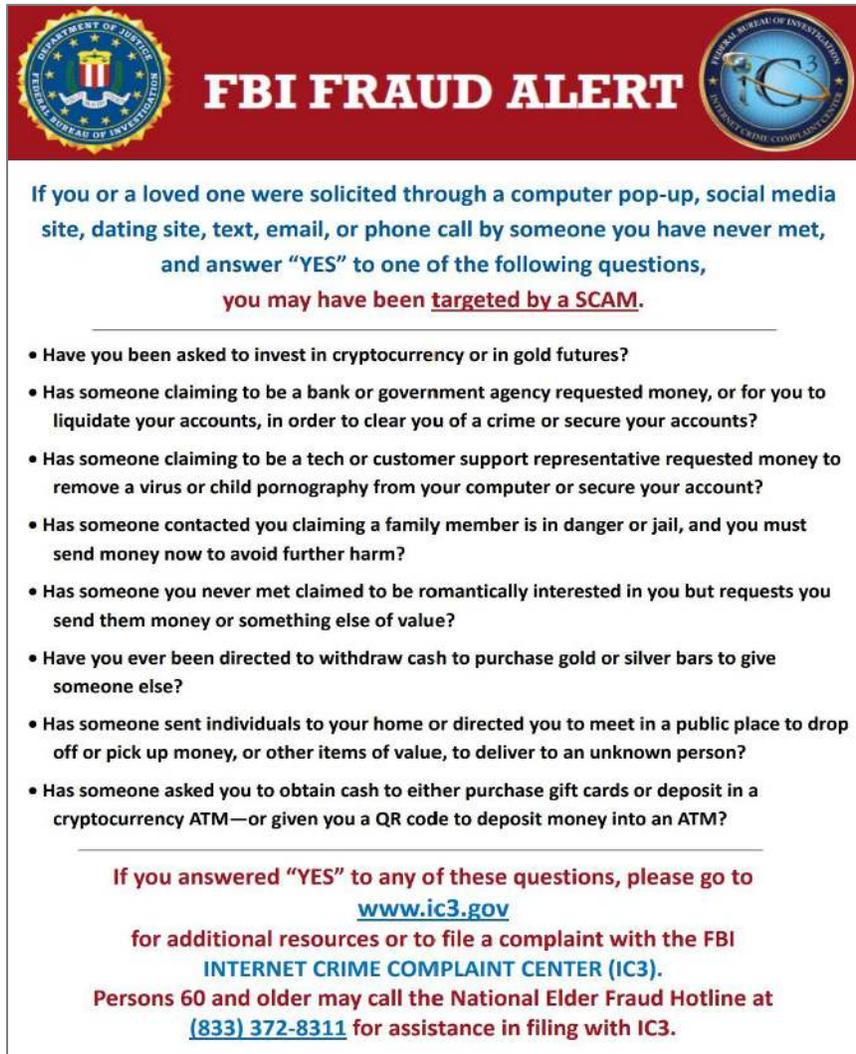
✓ Check	📞 Call	⌚ Wait
Email addresses and phone numbers to make sure they are correct.	A known number to ensure an email is authentic.	To verify that your money is going to the intended recipient.

Did a known client or vendor change payment or wire instructions? Make sure the request isn't coming from a spoofed email address.

🔍 If you suspect fraud, file a report via IC3.gov and call your local FBI office.

Check – Call – Wait
Avoid falling to a BEC scam.

IC3 Fraud Flyer



FBI FRAUD ALERT

If you or a loved one were solicited through a computer pop-up, social media site, dating site, text, email, or phone call by someone you have never met, and answer **"YES"** to one of the following questions, you may have been **targeted by a SCAM**.

- Have you been asked to invest in cryptocurrency or in gold futures?
- Has someone claiming to be a bank or government agency requested money, or for you to liquidate your accounts, in order to clear you of a crime or secure your accounts?
- Has someone claiming to be a tech or customer support representative requested money to remove a virus or child pornography from your computer or secure your account?
- Has someone contacted you claiming a family member is in danger or jail, and you must send money now to avoid further harm?
- Has someone you never met claimed to be romantically interested in you but requests you send them money or something else of value?
- Have you ever been directed to withdraw cash to purchase gold or silver bars to give someone else?
- Has someone sent individuals to your home or directed you to meet in a public place to drop off or pick up money, or other items of value, to deliver to an unknown person?
- Has someone asked you to obtain cash to either purchase gift cards or deposit in a cryptocurrency ATM—or given you a QR code to deposit money into an ATM?

If you answered **"YES"** to any of these questions, please go to www.ic3.gov for additional resources or to file a complaint with the FBI INTERNET CRIME COMPLAINT CENTER (IC3). Persons 60 and older may call the National Elder Fraud Hotline at [\(833\) 372-8311](tel:833-372-8311) for assistance in filing with IC3.