



Login: ●●●●●●●●



Password: ●●●●●●●●●●

Confidential Data



# Federal Bureau of Investigation Internet Crime Report



# 2025

INTERNET CRIME COMPLAINT CENTER

**CONTENTS**

A QUARTER-CENTURY OF CYBERCRIME REPORTING .....	3
OUR ROLE IN COMBATING CYBERCRIME .....	5
IC3 COMPLAINTS IN 2025 .....	6
CYBER-ENABLED FRAUD IN 2025.....	9
CYBER THREATS IN 2025.....	13
IC3 RECOVERY ASSET TEAM - FINANCIAL FRAUD KILL CHAIN.....	17
POSITIVE IMPACTS .....	19
INTERNATIONAL COMPLAINT COUNTRIES .....	24
THREE YEAR COMPLAINT COUNT COMPARISON .....	25
COMPLAINTS BY STATE.....	27
CRIME TYPES BY AGE GROUPS.....	32
COMPLAINANTS 17 YEARS OLD OR YOUNGER.....	34
ARTIFICIAL INTELLIGENCE (AI) USED IN CYBERCRIME.....	39
IC3 ELDER FRAUD – COMPLAINTS FILED BY INDIVIDUALS 60+.....	44
COMPLAINTS INVOLVING CRYPTOCURRENCY .....	52
APPENDIX A: ABOUT IC3 .....	58
APPENDIX B: DEFINITIONS AND DESCRIPTORS .....	59
APPENDIX C: ADDITIONAL INFORMATION ABOUT IC3 DATA.....	62
APPENDIX D: PUBLIC SERVICE ANNOUNCEMENTS PUBLISHED IN 2025 .....	63
APPENDIX E: INDUSTRY ALERTS PUBLISHED IN 2025 .....	65
APPENDIX F: IC3 QR CODES.....	66

# A Quarter-Century of Cybercrime Reporting

In 2025, the FBI Internet Crime Complaint Center (IC3) celebrated its 25th anniversary as the central hub for reporting cyber-enabled crime. This milestone signifies the FBI's enduring commitment to fighting the ever-evolving cyber threat. Our success in protecting individuals and organizations is driven by public participation and robust data analysis.

For the past quarter-century, IC3 has been the primary connection between the FBI and the public for information related to cyber-enabled criminal activity. Since our founding, reporting to IC3 has surged. We received a few thousand complaints per month in our early days. We now average almost 3,000 complaints per day. IC3 produces annual reports (like the one you are reading) based on the information we receive, publishes public awareness campaigns, and provides industry alerts to the private sector. IC3 remains an essential resource for our law enforcement colleagues in combating cyber-enabled crime.

In 2025, losses reported to IC3 continued to climb, surpassing the \$20 billion mark. Investment-related fraud was once again the largest component of these losses, followed by business email compromises and tech support scams. The FBI continues to disrupt and deter malicious cyber actors -- and shift the cost from victims to our adversaries. One example was Operation Level Up, which countered crypto investment scams. This FBI-led initiative has reduced potential losses by more than \$500 million since 2024.

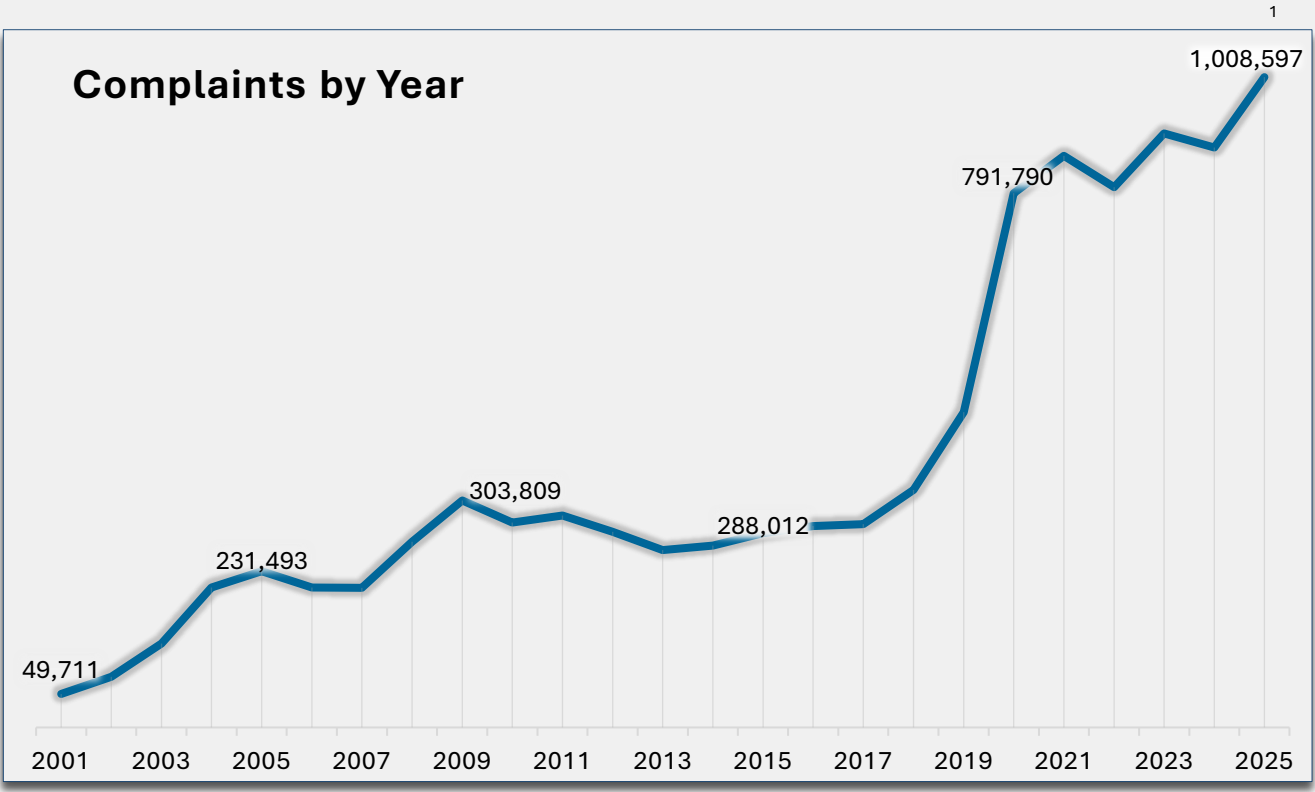
It has never been more important to be diligent with your cybersecurity, social media footprint, and electronic interactions. Cyber threats and cyber-enabled crime will continue to evolve as the world embraces emerging technologies such as artificial intelligence. At the time of publication, the FBI was engaged in Operation Winter Shield, which highlights concrete steps for organizations to bolster their digital security. The FBI remains fully committed to ensuring Americans' safety online and reinforcing the recent Executive Order targeting cybercrime, fraud, and foreign scam centers, to hold those accountable who exploit the internet for nefarious purposes.



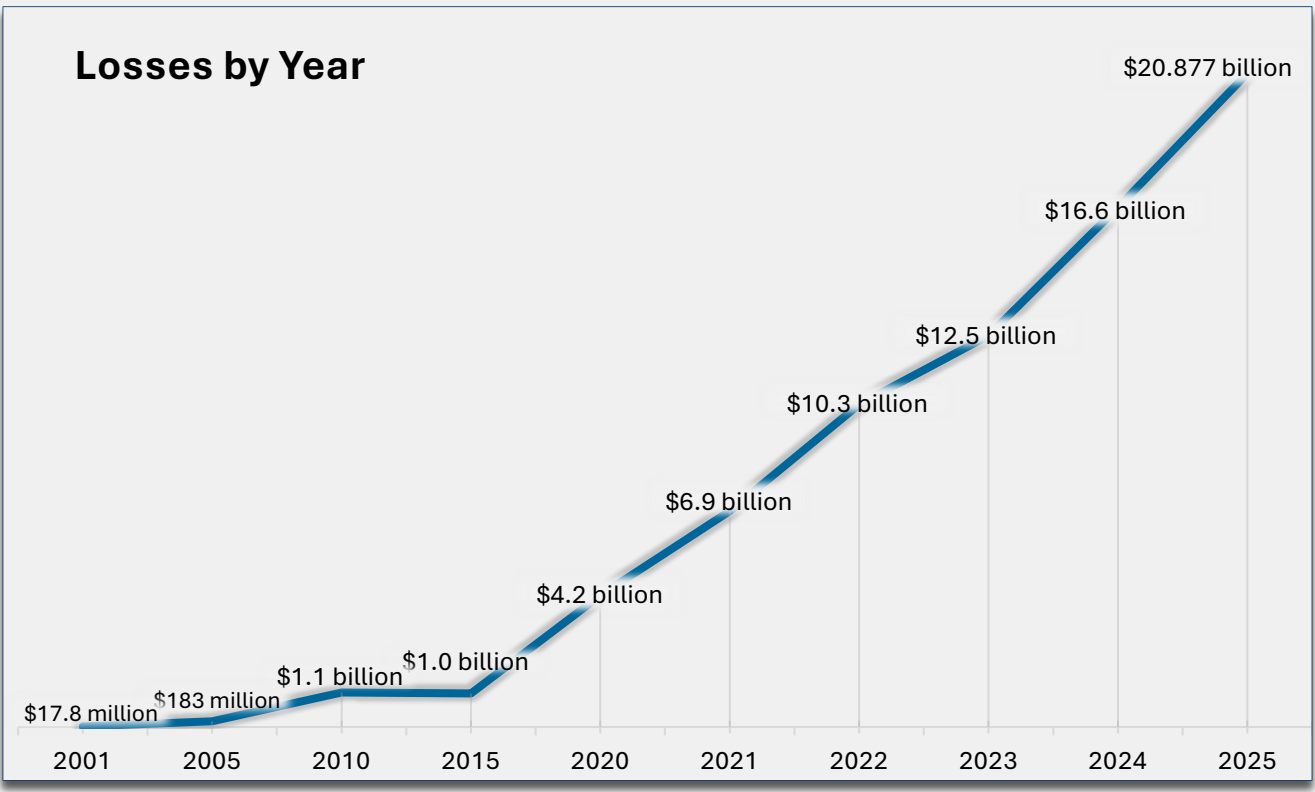
**Jose A. Perez**

**Operations Director for Criminal and Cyber Branch  
Federal Bureau of Investigation**

### A Quarter-Century of Cybercrime Reporting, *continued*



2



<sup>1</sup> Accessibility description: Chart describes the number of complaints filed with IC3.gov from 2001 – 2025.

<sup>2</sup> Accessibility description: Chart describes the losses of complaints filed with IC3.gov from 2001 – 2025.

# Our Role in Combating Cybercrime<sup>3</sup>

## Collection

IC3 is the primary connection between the FBI and the public for receiving and coordinating information related to cyber-enabled crimes, including intrusions, frauds, and scams. Victims are encouraged and often directed by law enforcement to file a complaint online at [www.ic3.gov](http://www.ic3.gov). Complainants should 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 [www.ic3.gov](http://www.ic3.gov) to identify emerging threats and new trends. IC3 can quickly alert financial institutions to fraudulent transactions which enables the freezing of victim funds if certain reporting criteria are met.

## Referral & Enhancement

IC3 aggregates related complaints to build referrals, which are provided to local, state, federal, and international law enforcement for potential investigations. Aggregation and enhancement build support and prosecutorial levels for new and ongoing investigations, and assist with detecting emerging methods, trends, and subject identifiers.



## Coordination

IC3 facilitates 24/7/365 coordination of threat response efforts with internal and external partners in support of a unified governmental approach to cyber incident management. IC3 plays a key role in the FBI's cooperation with international partners in the fight against cybercrime, working with FBI Headquarters, Field Offices, and Law Enforcement Attaches to support investigations around the globe.

## Public Awareness

Public Service Announcements, Industry Alerts, and other publications about specific scams are posted to [www.ic3.gov](http://www.ic3.gov). As more become aware of cyber-enabled crimes and methods used to carry them out, we all become better equipped to recognize the dangers associated with cyber activity and are in better position to avoid falling prey to online schemes.



<sup>3</sup> Accessibility description: Image contains icons with the core IC3 roles: Collection, Analysis, Referral and Enhancement, Coordination, and Public Awareness. Each is listed in individual blocks as components of an ongoing process.

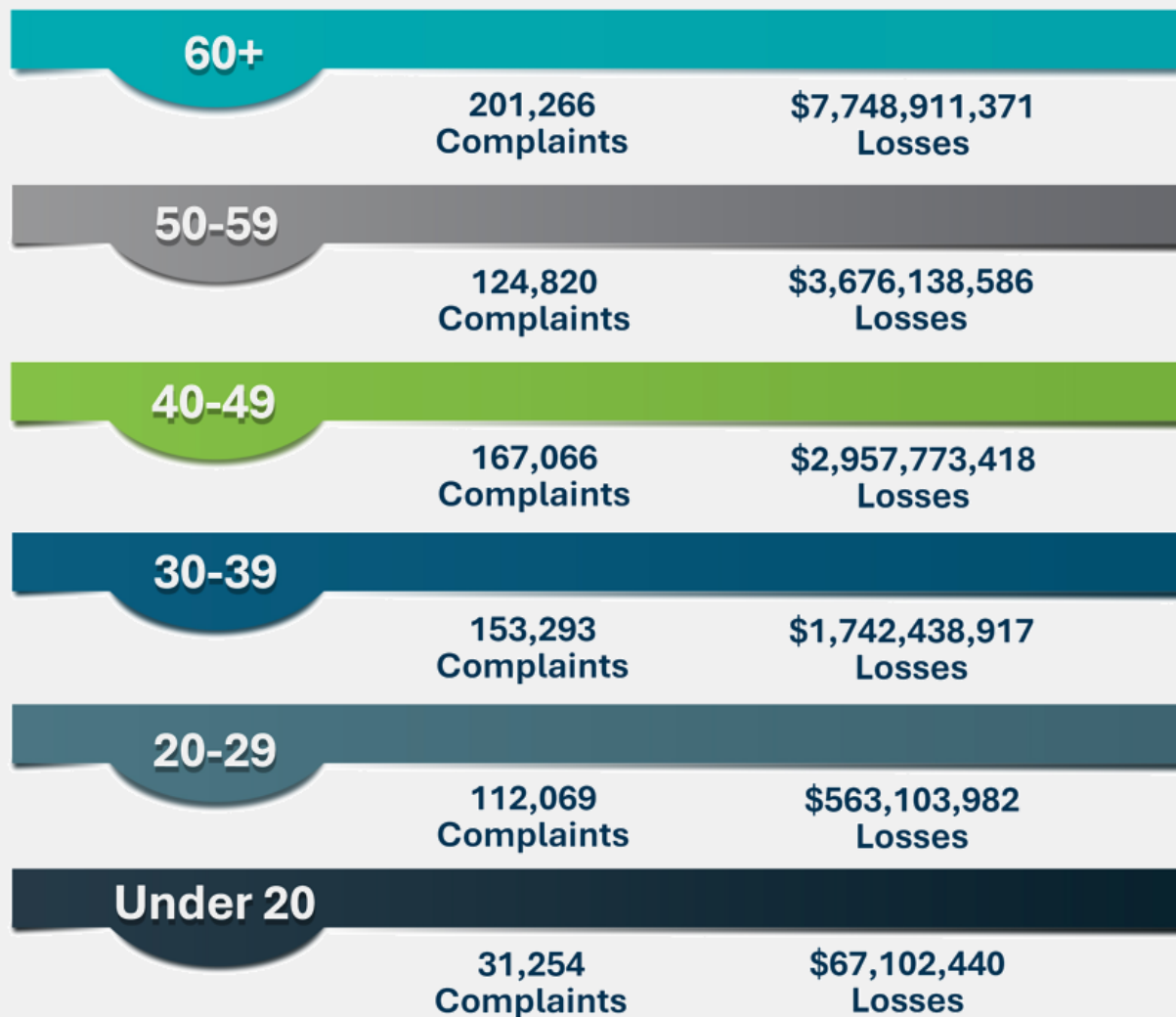
# IC3 Complaints in 2025

4

## Highlights

**1,008,597 Complaints**  
**\$20.877 Billion Total Losses**  
**26% Increase In Losses From 2024**  
**\$20,699 Average Loss**

## By Age Group



<sup>4</sup> Accessibility description: 2025 complaint highlights: 1,008,597 complaints; \$20.877 billion in losses; 26% increase in losses from 2024; \$20,699 Average Loss. Chart shows number of complaints and losses by age group. Under 20: 31,254 complaints, \$67.1 million in losses; 20-29: 112,069 complaints, \$563.1 million in losses; 30-39: 153,293 complaints, \$1.7 billion in losses; 40-49: 167,066 complaints, \$2.957 billion in losses; 50-59: 124,820 complaints, \$3.7 billion in losses; 60+: 201,266 complaints, \$7.7 billion in losses. Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## 2025 Crime Types

<b>By Complaint Count</b>			
<b>Crime Type</b>	<b>Complaints</b>	<b>Crime Type</b>	<b>Complaints</b>
<b>Phishing/Spoofing</b>	191,561	<b>Credit Card/Check Fraud</b>	18,774
<b>Extortion</b>	89,129	<b>Real Estate</b>	12,368
<b>Investment</b>	72,984	<b>Advanced Fee</b>	7,762
<b>Personal Data Breach</b>	67,456	<b>Lottery/Sweepstakes/ Inheritance</b>	5,623
<b>Non-Payment/ Non-Delivery</b>	56,478	<b>Threats of Violence</b>	4,826
<b>Tech/Customer Support</b>	47,794	<b>Data Breach</b>	3,963
<b>Government Impersonation</b>	32,424	<b>Ransomware</b>	3,611
<b>Identity Theft</b>	31,675	<b>IPR/Copyright and Counterfeit</b>	2,386
<b>Business Email Compromise</b>	24,768	<b>Overpayment</b>	2,194
<b>Employment</b>	24,688	<b>SIM Swap</b>	971
<b>Confidence/Romance</b>	23,159	<b>Malware</b>	893
<b>Harassment/Stalking</b>	21,557	<b>Botnet</b>	715
<b>Other</b>	20,031	<b>Charity</b>	662
<b>Descriptors</b>			
<b>Cryptocurrency</b>	181,565		
<b>AI Related</b>	22,364		
<b>Crimes Against Children</b>	7,239		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## 2025 Crime Types, *continued*

### By Complaint Loss

Crime Type	Loss	Crime Type	Loss
Investment	\$8,648,617,756	Lottery/Sweepstakes/ Inheritance	\$194,147,851
Business Email Compromise	\$3,046,598,558	Identity Theft	\$185,832,657
Tech/Customer Support	\$2,134,675,818	Advanced Fee	\$155,910,852
Personal Data Breach	\$1,314,923,988	Extortion	\$122,499,133
Confidence/Romance	\$929,287,469	Ransomware	\$32,320,105
Government Impersonation	\$797,943,193	Harassment/Stalking	\$27,707,167
Other	\$512,146,819	IPR/Copyright and Counterfeit	\$26,667,006
Non-Payment/ Non-Delivery	\$503,373,587	Overpayment	\$22,898,075
Data Breach	\$435,240,992	Malware	\$19,370,572
Employment	\$362,934,762	SIM Swap	\$17,366,758
Credit Card/Check Fraud	\$282,670,235	Botnet	\$13,859,049
Real Estate	\$275,110,419	Threats of Violence	\$9,509,532
Phishing/Spoofing	\$215,843,126	Charity	\$7,907,609
<i>Descriptors</i>			
Cryptocurrency	\$11,366,669,732		
AI Related	\$893,346,472		
Crimes Against Children	\$6,694,350		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

# Cyber-Enabled Fraud in 2025

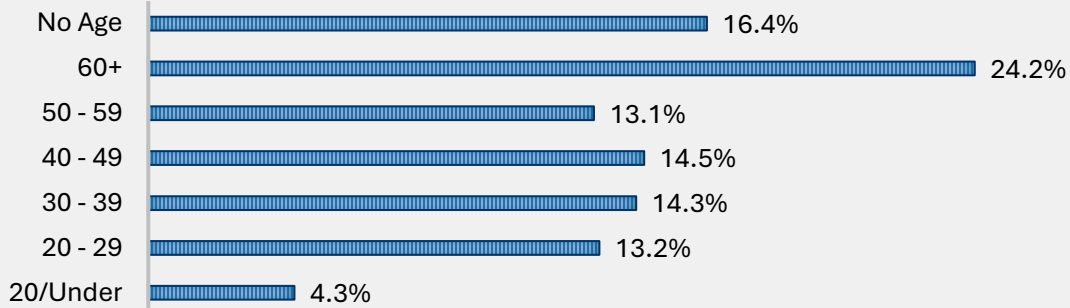
5

Cyber-enabled fraud includes complaints where criminals use the Internet or other technology to commit fraudulent activities, often involving the theft of money, data, identities, or the creation of counterfeit goods or services. Cyber-enabled fraud is responsible for almost 85% of all losses reported to IC3 in 2025.

## Highlights

452,868 Complaints  
 \$17,697,074,980 Losses  
 45% of 2025 Complaints  
 85% of 2025 Losses

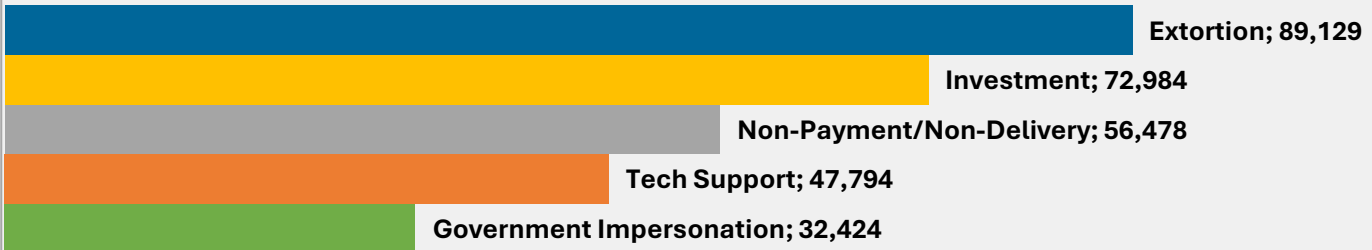
### Age Ranges of Cyber-Enabled Fraud Reporting



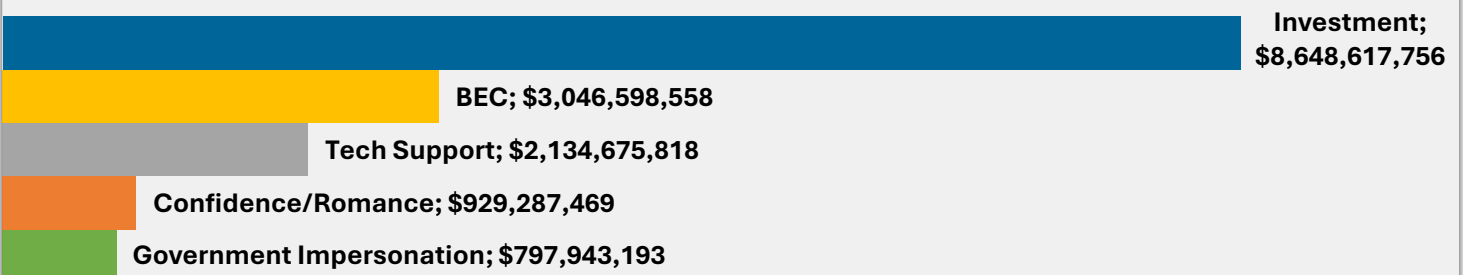
6

7

### Top 5 Cyber-Enabled Fraud Crime Types by Count



### Top 5 Cyber-Enabled Fraud Crime Types by Loss



<sup>5</sup> Cyber-enabled fraud complaint highlights: 452,868 complaints; \$17.697 billion in losses; accounts for 45% of all 2025 complaints and 85% of all 2025 losses.

<sup>6</sup> Accessibility description: Chart shows the counts of cyber-enabled crime complaints by reported age ranges.

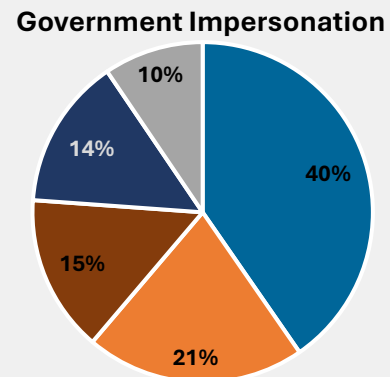
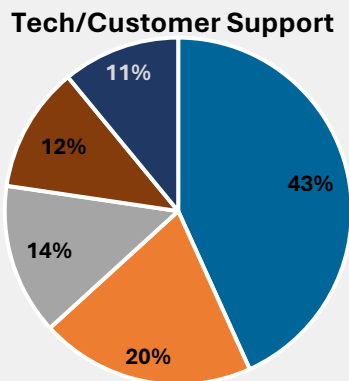
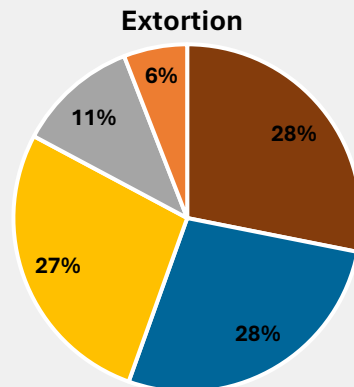
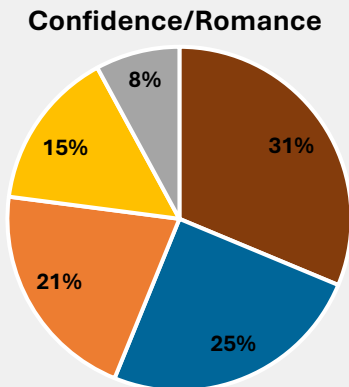
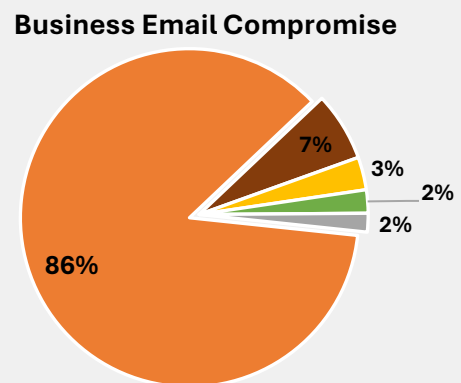
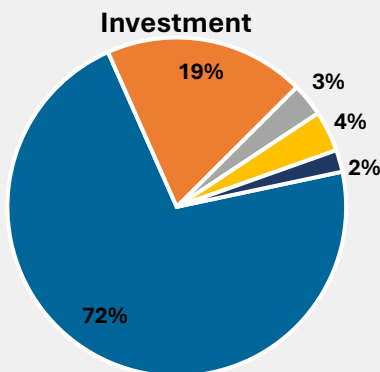
<sup>7</sup> Accessibility description: Chart shows the top five crime types for cyber-enabled fraud by count and loss.

## Top Reported Transaction Types in Fraud<sup>8</sup>

Transaction information provided in IC3 complaints helps the FBI understand how victims are losing funds to fraud and assists the IC3 Recovery Asset Team (RAT) Financial Fraud Kill Chain (FFKC) process when complaints are filed as quickly as possible. These charts identify the most frequent ways complainants reported financial losses from cyber-enabled fraud.



- Cryptocurrency
- Wire Transfer/ACH
- Debit Card/Credit Card
- Peer-to-Peer Transfer
- Prepaid card/Gift card
- Check/Cashier's Check
- Cash



<sup>8</sup> Accessibility description: Chart depicts the top reported transaction types: Cryptocurrency, Wire Transfer/ACH, Debit/Credit Card, Peer-to-Peer, Gift/Prepaid Card, Check/Cashier's Check, and Cash.

## Cyber-Enabled Fraud Trends

### Sextortion

Sextortion can start on any site, app, messaging platform, or game where people meet and communicate. In some cases, the first contact from the criminal will be a threat - the person may claim to already have a revealing picture or video of a child that will be shared if the victim does not send more pictures. More often, however, this crime starts when people believe they are communicating with someone their own age who is interested in a relationship, or with someone who is offering something of value. After the criminals have one or more videos or pictures, they threaten to publish that content, or they threaten violence, to compel the victim to produce more images. The shame, fear, and confusion people feel when they are caught in this cycle often prevent them from asking for help or reporting the abuse. The public should understand how sextortion occurs and openly discuss online safety.

In 2025, IC3 received more than 75,000 submissions regarding sextortion. When appropriate, IC3 refers complaints to the National Center for Missing & Exploited Children (NCMEC). In 2025, IC3 referred more than 5,700 submissions involving minors to NCMEC.

2025 Sextortion by Age Range		
Age Range	Count	Adjusted Loss
Under 20	11,316	\$1,297,653
20 - 29	22,061	\$7,282,686
30 - 39	11,855	\$8,063,178
40 - 49	7,791	\$6,507,936
50 - 59	5,139	\$6,186,794
60+	6,121	\$14,894,547

#### Read More

[Financially Motivated Sextortion — FBI](#)  
[Sextortion — FBI](#)

### Cryptocurrency Investment Fraud

Cryptocurrency Investment Scams are sophisticated long-term scams using psychological manipulation, the appearance of legitimacy, and exploitation of cryptocurrencies to deceive victims into investing large sums of money. These scams are largely perpetrated by organized criminal enterprises based in Southeast Asia using victims of human trafficking as forced labor to run the scam operations. Cryptocurrency investment fraud was the highest source of financial losses to Americans in 2025 with \$7.2 billion reported in losses.

The scammers typically initiate contact through text messages, social media sites, advertisements, or dating applications and then quickly move the conversation to a messaging platform. Often the victims are introduced to investment groups representing themselves to be knowledgeable industry insiders offering guidance on trading or investing in cryptocurrency or gold. The victims are enticed to send cryptocurrency to fake investment scam platforms or apps and are shown fake profits and offered loans to encourage larger investments. Eventually, when the victims try to withdraw their money,

they will be charged taxes and fees as a final attempt to exploit money from the victims before the scammers disappear with all the victim funds. Victims are also targeted in recovery scams, claiming to help recover lost funds.

These scams are often devastating because they can leave victims with significant financial loss and emotional distress. The FBI is working to combat these scams through its work on the U.S. Attorney's Office District of Columbia Scam Center Strike Force and Operation Level Up, as detailed in the "Positive Impact" section of this report.

### Read More

[Investment Fraud - Internet Crime Complaint Center \(IC3\)](#)

[Cryptocurrency Investment Fraud — FBI](#)

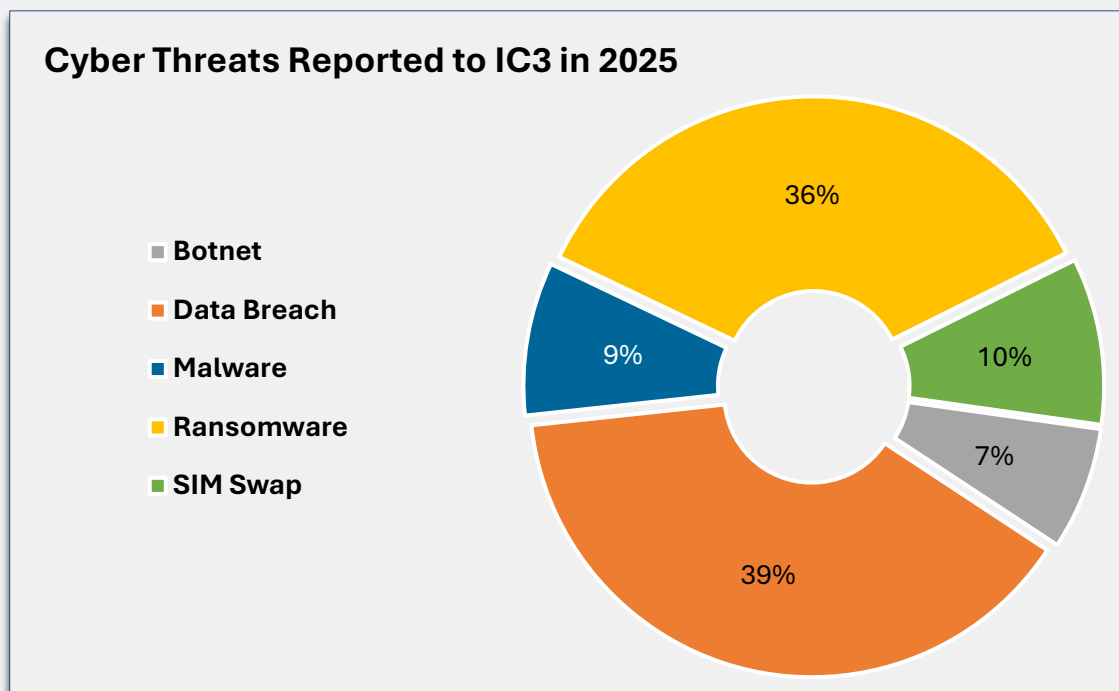
<p style="text-align: center;"><b>Account Takeover (ATO)</b></p> <p style="text-align: center;">Approximately 4,700 complaints \$359.7 million in losses</p> <p style="text-align: center;">----</p> <p style="text-align: center;"><a href="#">IC3 - Account Takeover Fraud via Impersonation of Financial Institution Support</a></p>	<p style="text-align: center;"><b>Gold Courier Scams</b></p> <p style="text-align: center;">Approximately 725 complaints \$311.8 million in losses</p> <p style="text-align: center;">----</p> <p style="text-align: center;"><a href="#">IC3 - Scammers Use Couriers to Retrieve Cash and Precious Metals from Victims of Tech Support and Government Impersonation Scams</a></p>
<p style="text-align: center;"><b>Investment Club Scams</b></p> <p style="text-align: center;">Approximately 1,600 complaints \$160 million in losses</p> <p style="text-align: center;">----</p> <p style="text-align: center;"><a href="#">IC3 - Fraudsters Target US Stock Investors through Investment Clubs Accessed on Social Media and Messaging Applications</a></p>	<p style="text-align: center;"><b>Government Impersonation</b></p> <p style="text-align: center;">Approximately 32,000 complaints \$798 million in losses</p> <p style="text-align: center;">----</p> <p style="text-align: center;"><a href="#">IC3 - Senior US Officials Impersonated in Malicious Messaging Campaign</a></p> <p style="text-align: center;"><a href="#">IC3 - Criminals Impersonate US Health Insurance Providers and Chinese Law Enforcement to Target Chinese Speakers Residing in the United States</a></p>

## Cyber Threats in 2025

Hijacked networks, cryptocurrency heists, and corporate espionage are a few examples of the spiraling cyber threat. Every year, our adversaries become savvier and increasingly callous – attacking power grids, shutting down hospitals, and stoking geopolitical tensions. State-sponsored cyber actors wield every element of their national power to target the United States and its critical infrastructure. Skilled cybercriminals exploit new and longstanding vulnerabilities to steal our money and hold our data for ransom.

Combating these threats is the primary mission of the FBI's Cyber program. As the lead federal agency for investigating cyberattacks and intrusions, we engage with victims and work to unmask those committing malicious cyber activities, wherever they are.

9



<sup>9</sup> Accessibility description: Chart shows the typically associated cyber threat crime types and percentage of the total cyber threat complaints received.

## Ransomware as Reported to IC3 in 2025

Ransomware is among the highest reported cyber threats targeting critical infrastructure organizations. Ransomware is a type of malicious software designed to block access to a computer system until money is paid. In 2025, the IC3 received more than 3,600 complaints reporting ransomware, with losses exceeding \$32 million.

In 2025, the following ransomware variants were among those most frequently reported variants to the FBI via IC3, accounting for 56.8% of the total number of ransomware incidents reported. The 2025 loss amount reported to IC3 attributed to these variants is over \$16 million, almost half (49.8%) of the total losses reported. Regarding ransomware adjusted losses, this number does not normally include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by an entity. In some cases, entities do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to the FBI via IC3 and does not account for the entity directly reporting to FBI field offices.

### Highlights

- 63 New Ransomware Variants Identified via IC3
- Average 5.25 New Variants Per Month

## Top 10 Reported Variants

The top 10 reported ransomware variants most impacted the following Critical Sectors: Critical Manufacturing, Healthcare and Public Health, and Government Facilities.

Joint Cyber Security Advisories (JCSAs) are available to learn more about several of these variants.



1. <a href="#">Akira</a>	2. <a href="#">Qilin</a>	3. <a href="#">INC./Lynx/Sinobi</a>	4. <a href="#">BianLian</a>	5. <a href="#">Play</a>
6. <a href="#">Ransomhub</a>	7. <a href="#">Lockbit</a>	8. <a href="#">Dragonforce</a>	9. <a href="#">SAFEPAY</a>	10. <a href="#">Medusa</a>

## Recommendations to Protect Against Ransomware

A key step to limit damage and lower risk is to establish and maintain a solid foundation of industry best practices, which can help mitigate the threat and reduce your organization's attack surface. The FBI recommends the following mitigating practices for companies:

- Create off-site or offline backups and regularly maintain backup and restoration. Additionally, ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure.
- Eliminate default passwords and credentials when installing software and require all accounts with password logins (e.g., service accounts, admin accounts, and domain admin accounts) to comply with NIST's standards.
- Disable and remove unnecessary protocols by default. Audit user accounts with administrative privileges and configure access controls according to the principle of least privilege.
- Enable multi-factor authentication (MFA) for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- Secure initial access points - To help in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- Segment networks to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to— various subnetworks and by restricting adversary lateral movement.
- Keep all operating systems, software, and firmware up to date. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities in internet-facing systems.

If you are impacted by ransomware or cybercrime, file a report with IC3 to share information with the FBI.

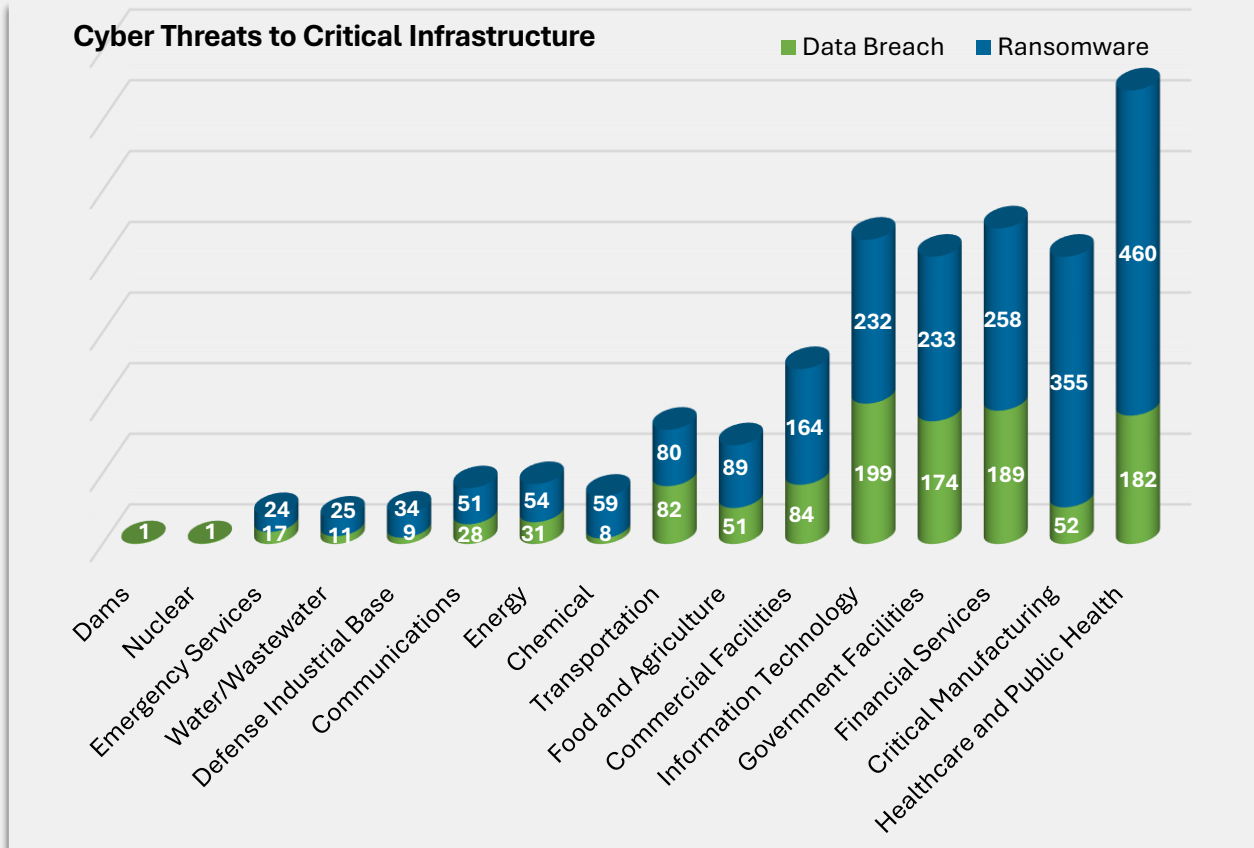
For a more extensive list of mitigations and recommendations regarding ransomware, please refer to [#StopRansomware Guide | CISA](#).

### Cyber Threats to Critical Infrastructure in 2025

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the U.S., their incapacitation or destruction would have a debilitating effect on national security, economic security, or public health and safety.

**Read More** – <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>

10



### Non-Critical Sector Ransomware Reporting

IC3 received more than 1,400 ransomware complaints from businesses and organizations not related to a critical sector. Below are the most reported industries for these complaints.

		<i>Example</i>
18%	Legal services	law firms, estate planning
17%	Contracting services	electricians, general contractors
10%	Engineering, architectural services	engineering firms, land surveying
7%	Consulting services	project management, marketing services
5%	Non-critical manufacturing	furniture, building materials

<sup>10</sup> Accessibility description: This chart outlines complaints categorized as ransomware and data breach complaints related to one of the 16 critical infrastructure sectors.

# IC3 Recovery Asset Team - Financial Fraud Kill Chain in 2025

Established in 2018, the IC3 RAT 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 FFKC.

For the domestic FFKC process, the IC3 RAT will expand the FFKC process beyond the initial recipient bank if information is provided during the FFKC initiation on “second hop” transactions to other domestic or international accounts to request freezes on as much of the lost funds as possible. For the international FFKC process, the IC3 RAT coordinates with the Financial Crimes Enforcement Network Rapid Response Team and law enforcement entities, including FBI LEGAT offices and international law enforcement partners to assist in freezing funds.

### Highlights

3,900 Incidents

\$1,163,919,846  
Attempted Theft

\$679,013,183 Frozen

58% Success Rate

<u>Domestic FFKC</u>	<u>International FFKC</u>
3,574 Incidents	326 Incidents
\$507,042,623 Frozen	\$171,970,560 Frozen

In the past, the majority of FFKC incidents initiated by the IC3 RAT were Business Email Compromises (BECs), however in 2025 the FFKC process saw a rise in Tech Support and Account Takeover (ATO) initiations. ATO-related incidents can contain upwards of 50 or more transactions to different recipient accounts at multiple banks happening simultaneously via ACH transactions. It is extremely important for individuals and businesses to follow this guidance:

- If you discover a fraudulent transfer, time is of the essence. Immediately, contact your financial institution and request a recall of the funds along with any necessary indemnification documents. Different financial institutions have varying policies; it is important to know what assistance your financial institution will provide when attempting to recover funds.
- Regardless of the amount lost, file a complaint at [www.ic3.gov](http://www.ic3.gov). Be sure to include the full transaction details in your report. IC3 may be able to assist both the financial institutions and law enforcement in freezing funds.

### FFKC in Elder Fraud

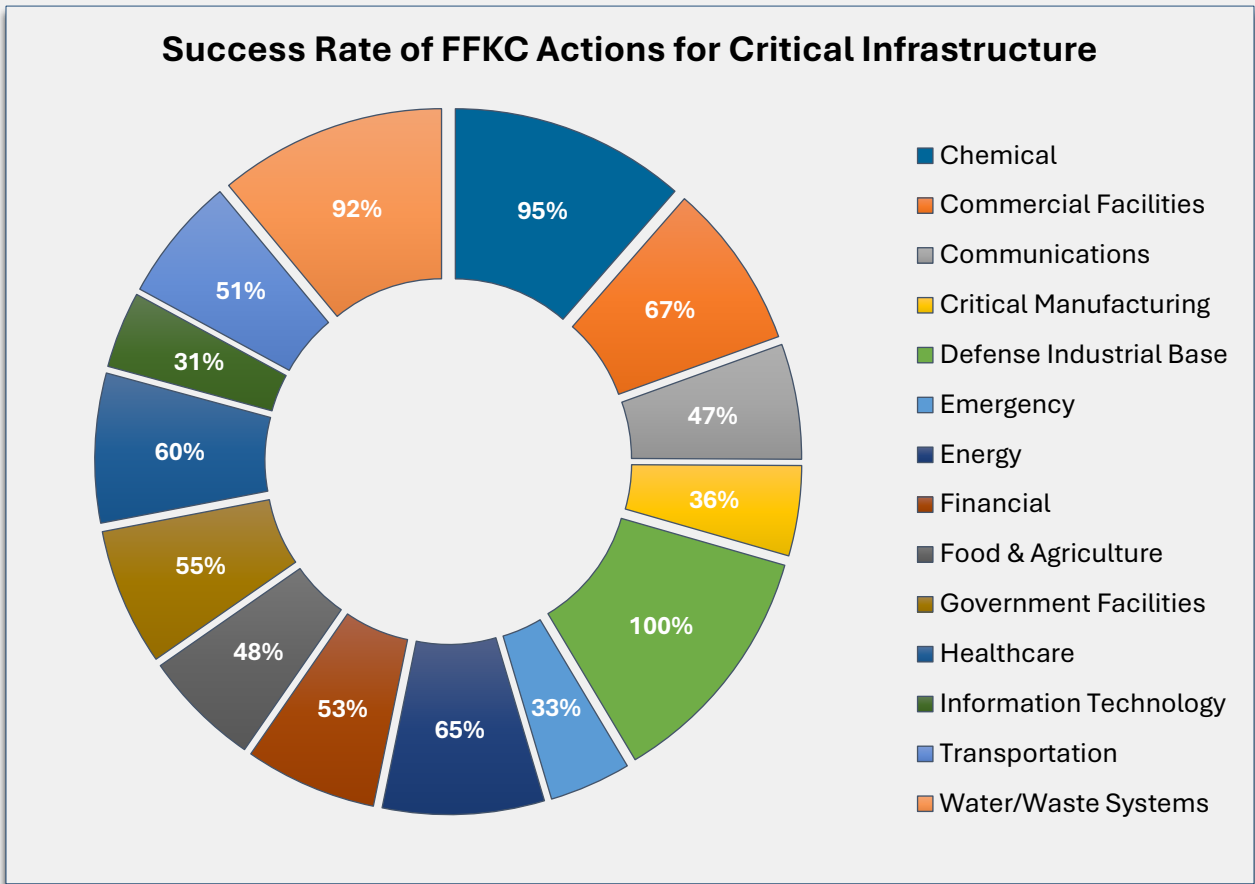
Of the 3,900 FFKCs incidents initiated for 2025, there were 642 incidents involving victims aged 60+ with a total reported loss of \$65,367,648. The FFKC process was able to assist in freezing \$32,865,655 of those funds. The top three IC3 crime types in 2025 FFKC incidents involving 60+ victims:

- Tech Support/ATO scams: 360 FFKC incidents
- BEC (BEC/Real Estate): 104 FFKC incidents
- Investment (Investment/Crypto): 64 FFKC incidents

### FFKC Initiated for Critical Infrastructure

In 2025, the RAT initiated 655 FFKC incidents reported by businesses and organizations belonging to one of the 16 critical infrastructure sectors. Of the \$261,451,001 in reported losses, the RAT was able to freeze \$146,561,094, for an overall success rate of 56%.

11



<sup>11</sup> Accessibility description: Chart shows the success rate of FFKC incidents initiated related to critical infrastructure sectors.

## Positive Impacts

---

### U.S. Attorney's Office District of Columbia Scam Center Strike Force on Cryptocurrency Investment Fraud

In response to the massive losses to cryptocurrency investment scams, the newly formed U.S. Attorney's Office District of Columbia Scam Center Strike Force combines the power, reach, and resources of the U.S. Attorney's Office with the Department of Justice's Criminal Division, the FBI, and the U.S. Secret Service to crackdown and disrupt these schemes. The Strike Force is also seeking to use all government tools available, partnering with the State Department, the Department of Treasury's Office of Foreign Assets Control (OFAC), and the Department of Commerce.

The Scam Center Strike Force is investigating the worst scam compounds located in Southeast Asia. Strike Force teams focus on identifying and pursuing key leaders—including Chinese organized crime affiliates operating in Cambodia, Laos, and Burma—to bring them to justice.

The Scam Center Strike Force is also working to seize and disable the U.S.-based facilities and infrastructure that provide the manner and means to execute these scams, which includes U.S. internet service providers and social media accounts scammers use to prey on Americans. The Scam Center Strike Force will collaborate with U.S. companies to sever access to the scam centers and prevent U.S. infrastructure from being weaponized against American citizens.

#### Read More

[New Scam Center Strike Force Battles Southeast Asian Crypto Investment Fraud Targeting Americans | United States Department of Justice](#)

---

## Positive Impacts, *continued*

### Operation Level Up

Launched in January 2024, Operation Level Up identifies victims of cryptocurrency investment fraud and notifies them of the scam. The operation was initiated with the support of agents from the FBI and U.S. Secret Service. Since its launch, Operation Level Up has achieved big milestones, surpassing 8,000 total victims notified and \$500 million in savings to notified victims.

#### **2025 Success Stories**

Utilizing IC3 complaint data, Operation Level Up reported:

- 3,780 victims of cryptocurrency investment fraud were notified
- 78% of those victims were unaware they were being scammed
- Estimated victim savings of \$225,871,319
- 38 victims were referred to a Victim Specialist for suicide intervention

#### **Read More**

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

#### **Prevented Losses**

- Stopped a victim from cashing out \$750,000 from his 401K.
- Stopped a victim from selling her house to invest \$500,000.
- Stopped a victim from obtaining a loan to send \$400,000 to the scammer.
- Multiple FBI initiations to the FFKC reversed wires and returned funds to victims.
- Several victims' finances, which needed to pay for serious medical treatments, were saved. Victims were planning to send these funds in hopes of earning more to pay for their treatments.
- Intervened with multiple victims who were contemplating suicide or self-harm. Along with FBI Victim Specialists, FBI Agents maintained contact with the victim until local law enforcement arrived.

## Positive Impacts, *continued*

### 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. In 2025, the number of complaints totaled more than 80,000, with losses exceeding \$2.9 billion.

#### **DOJ, FBI, and Central Bureau of Investigation**

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

#### **Success Stories**

In 2025, the FBI enabled approximately 175 arrests through 13 joint operations with the CBI and other local law enforcement. Since 2022, the FBI and CBI have had over 1,200 exchanges of information to support criminal investigations, with more than 475 arrests across 27 joint operations. The FBI has conducted hundreds of interviews and continues to support Indian law enforcement efforts to dismantle and disrupt fraudulent call centers and the prosecution of individuals in Indian perpetrating these frauds.

**FBI Baltimore Field Office:** The CBI, in a joint operation with the FBI, dismantled a large Noida, India-based transnational cybercrime network in December 2025, arresting six individuals for duping more than 600 U.S. citizens through tech-support scams and impersonating U.S. agencies like the Drug Enforcement Administration and the Social Security Administration. The operation, codenamed "Operation Chakra," involved raiding an illegal call center, seizing cash and devices, and uncovering complex money laundering through crypto and bank transfers, with ongoing efforts to trace international funds and execute further arrests. Victim reporting to IC3 identified more than \$48.7 million in losses attributed to the criminal network, which encouraged the CBI to pursue the call center.

**Read More** [Maryland police, Prosecutor, FBI announce arrests in international fraud scheme](#)

**FBI San Diego Field Office:** The FBI San Diego Elder Justice Task Force (EJTF), along with over 100 law enforcement personnel, executed multiple federal and state arrest and search warrants in November 2025, targeting alleged members and associates of an international elder scam network. Via IC3 reporting, the FBI identified over 500 suspected or confirmed U.S. victims with the approximate loss amount exceeding \$40 million. **Read More** [Nineteen Alleged Fraudsters Arrested for Conspiring to Scam Over 500 U.S. Seniors — FBI](#)

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

## Positive Impacts, *continued*

### Ransomware

#### **BlackSuit (Royal) Ransomware**

IC3 enhances and supports intelligence analysis, while triaging victim reporting in support of ongoing investigations. In 2025, BlackSuit (Royal) ransomware attacks targeted critical infrastructure sectors including, but not limited to, critical manufacturing, government facilities, healthcare and public health, and commercial facilities. IC3 provided information regarding numerous victims of the BlackSuit (Royal) Ransomware group to the field for victim notification and assistance. On August 11, 2025, the Department of Justice issued a press release highlighting coordinated actions taken to disrupt this group which involved multiple domestic and foreign law enforcement partner participation.

**Read More** [Office of Public Affairs | Justice Department Announces Coordinated Disruption Actions Against BlackSuit \(Royal\) Ransomware Operations | United States Department of Justice](#)

---

### Data Breach

#### **DPRK**

IC3 identified dozens of victim companies of the Democratic People's Republic of Korea (DPRK) Information Technology (IT) worker scam through complaints filed on IC3.gov. The DPRK government reportedly dispatched thousands of individuals around the globe with the aim of deceiving U.S. and other businesses worldwide into hiring them as remote IT workers to generate revenue to fund its weapons program. In addition, the FBI observed these IT workers leverage unlawful access to company networks to exfiltrate proprietary and sensitive data and facilitate cyber-criminal activities on behalf of the DPRK.

#### **Read More**

[IC3 - North Korean IT Workers Conducting Data Extortion](#)

[IC3 - North Korean IT Worker Threats to U.S. Businesses](#)

---

## Positive Impacts, *continued*

### Financial Fraud Kill Chain

In March 2025, the RAT received an IC3 complaint regarding a BEC incident involving a Missouri victim who was a senior citizen. The victim was attempting to close on a property and received a compromised email from the “title company” containing wire instructions for over \$1.3 million to a fraudulent bank account. The RAT immediately initiated the FFKC with domestic banking partners to freeze the fraudulent recipient account and confirmed funds were frozen and other wires had come into the fraudulent account from additional victims. The RAT was notified the owner of the fraudulent recipient account was a victim of an overpayment scam and instructed to send \$1 million to a fraudulent international account in Hong Kong. The RAT immediately initiated the International FFKC to the Financial Crime Enforcement Network and LEGAT Hong Kong partners.

In April 2025, the FBI Portland Office notified the RAT a city government office in Oregon was the victim of a BEC incident with a reported loss of over \$6 million dollars. The RAT searched FFKC records for the fraudulent recipient bank account and found the March 2025 FFKC was for the same recipient account. The RAT notified the FBI Portland Field Office of the details regarding the prior FFKC and notified the recipient banking partners of the additional wire transfer to the fraudulent recipient account. Due to the previous FFKC notification and freeze on the recipient account, the recipient bank notified the originating bank in Oregon of the situation and to confirm the validity of the wire instructions. The wire instructions were determined to be fraudulent, and the originating bank was able to issue a recall for the \$6 million wire. <https://www.justice.gov/usao-or/pr/united-states-files-forfeiture-action-recover-67-million-stolen-funds>

---

In August 2025, the RAT received a complaint reporting a BEC/Real Estate incident. The individuals were closing on a home when they received an email impersonating their legitimate attorneys. A wire was submitted at their bank for over \$449,000 and was sent to the recipient bank. After the fraud was discovered, the individuals reported the fraud to their bank, and their attorneys made separate attempts to contact the recipient bank with negative results. Upon receiving the IC3 complaint filed about the incident, the RAT immediately initiated the FFKC to request a freeze of the fraudulent account at the recipient bank. The RAT received notification from the recipient bank that the full amount was still in the account and on hold.

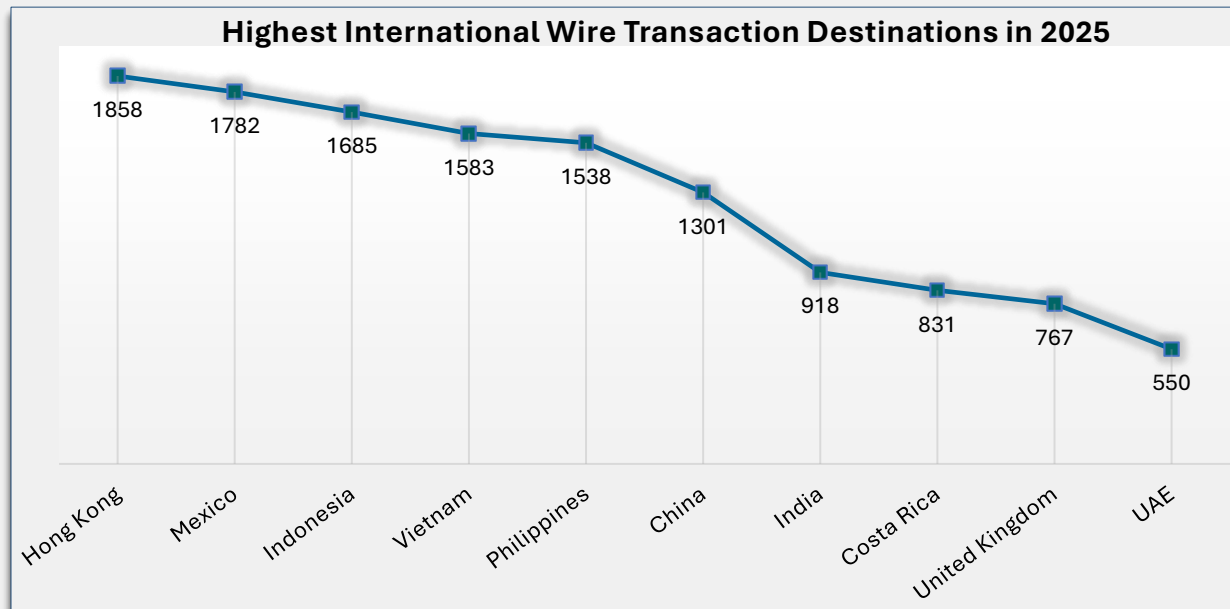
---

## International Complaint Countries <sup>12</sup>

IC3 received complaints from more than 200 countries in 2025, which accounts for almost \$1.6 billion of the overall 2025 losses.

Top 20 Foreign Countries with IC3 Complainants			
Country	Complaints	Country	Complaints
Canada	7,479	Mexico	1,654
India	5,879	South Africa	1,532
Japan	5,764	Pakistan	1,514
United Kingdom	4,106	Nigeria	1,219
Germany	3,056	Greece	1,205
Philippines	2,725	Iran	1,101
Brazil	2,686	China	1,030
France	2,326	Spain	993
Colombia	2,222	Turkey	944
Australia	2,069	Italy	918

Transactional information provided in IC3 complaints also helps identify where funds are going when victims are directed to send funds overseas. <sup>13</sup>



<sup>12</sup> Accessibility description: Chart lists the top 20 countries by number of total complaints submitted to IC3, aside from the U.S. Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

<sup>13</sup> Accessibility description: Chart shows the countries with the highest number of reported fraudulent wire transactions in 2025.

## IC3 Complaints in 2025

### Three Year Complaint Count Comparison

By Complaint Count			
Crime Type	2025	2024	2023
Advanced Fee	7,762	7,097	8,045
BEC	24,768	21,442	21,489
Botnet	715	587	540
Charity	662	*	*
Confidence/Romance	23,159	17,910	17,823
Credit Card/Check Fraud	18,774	12,876	13,718
Crimes Against Children	*	4,472	2,361
Data Breach	3,963	3,204	3,727
Employment	24,688	20,044	15,443
Extortion	89,129	86,415	48,223
Government Impersonation	32,424	17,367	14,190
Harassment/Stalking	21,557	11,672	9,587
Identity Theft	31,675	21,403	19,778
Investment	72,984	47,919	39,570
IPR/Copyright and Counterfeit	2,386	1,583	1,498
Lottery/Sweepstakes/Inheritance	5,623	3,690	4,168
Malware	893	441	659
Non-Payment/Non-Delivery	56,478	49,572	50,523
Other	20,031	12,318	8,808
Overpayment	2,194	2,705	4,144
Personal Data Breach	67,456	64,882	55,851
Phishing/Spoofing	191,561	193,407	298,878
Ransomware	3,611	3,156	2,825
Real Estate	12,368	9,359	9,521
SIM Swap	971	982	1,075
Tech/Customer Support	47,794	36,002	37,560
Threats of Violence	4,826	1,360	1,697

\* Crime Type or Descriptor was not captured in these years.

## IC3 Complaints in 2025

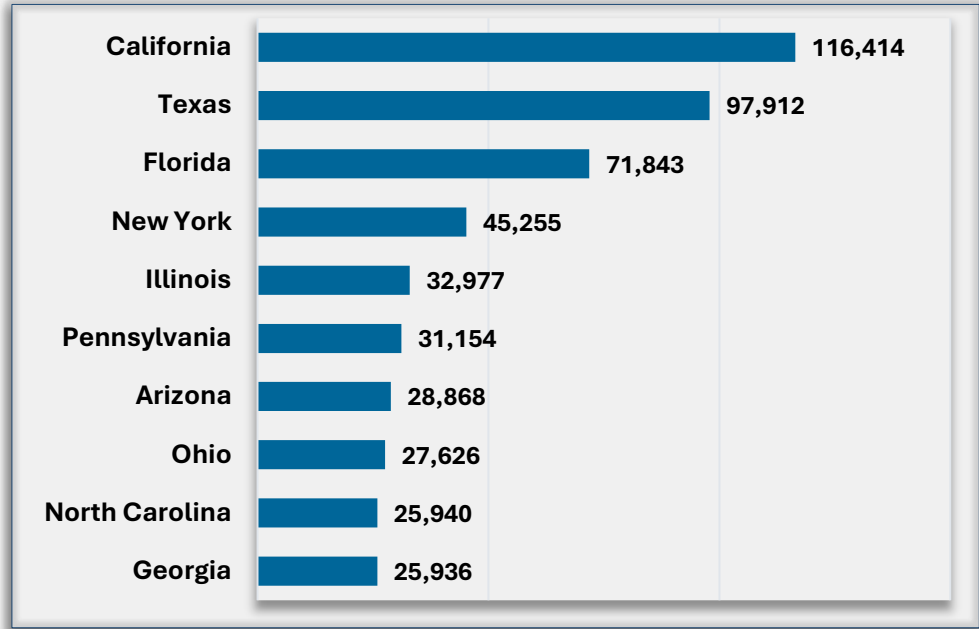
### Three Year Complaint Loss Comparison

By Complaint Loss			
Crime Type	2025	2024	2023
Advanced Fee	\$155,910,852	\$102,074,512	\$134,516,577
BEC	\$3,046,598,558	\$2,770,151,146	\$2,946,830,270
Botnet	\$13,859,049	\$8,860,202	\$22,422,708
Charity	\$7,907,609	*	*
Confidence/Romance	\$929,287,469	\$672,009,052	\$652,544,805
Credit Card/Check Fraud	\$282,670,235	\$199,889,841	\$173,627,614
Crimes Against Children	*	\$519,424	\$2,031,485
Data Breach	\$435,240,992	\$364,855,818	\$534,397,222
Employment	\$362,934,762	\$264,223,271	\$70,234,079
Extortion	\$122,499,133	\$143,185,736	\$74,821,835
Government Impersonation	\$797,943,193	\$405,624,084	\$394,050,518
Harassment/Stalking	\$27,707,167	\$10,611,223	\$9,677,332
Identity Theft	\$185,832,657	\$174,354,745	\$126,203,809
Investment	\$8,648,617,756	\$6,570,639,864	\$4,570,275,683
IPR/Copyright and Counterfeit	\$26,667,006	\$8,715,512	\$7,555,329
Lottery/Sweepstakes/Inheritance	\$194,147,851	\$102,212,250	\$94,502,836
Malware	\$19,370,572	\$1,365,945	\$1,213,317
Non-Payment/Non-Delivery	\$503,373,587	\$785,436,888	\$309,648,416
Other	\$512,146,819	\$280,278,325	\$240,053,059
Overpayment	\$22,898,075	\$21,452,521	\$27,955,195
Personal Data Breach	\$1,314,923,988	\$1,453,296,303	\$744,219,879
Phishing/Spoofing	\$215,843,126	\$70,013,036	\$18,728,550
Ransomware	\$32,320,105	\$12,473,156	\$59,641,384
Real Estate	\$275,110,419	\$173,586,820	\$145,243,348
SIM Swap	\$17,366,758	\$25,983,946	\$48,798,103
Tech/Customer Support	\$2,134,675,818	\$1,464,755,976	\$924,512,658
Threats of Violence	\$9,509,532	\$1,842,186	\$13,531,178

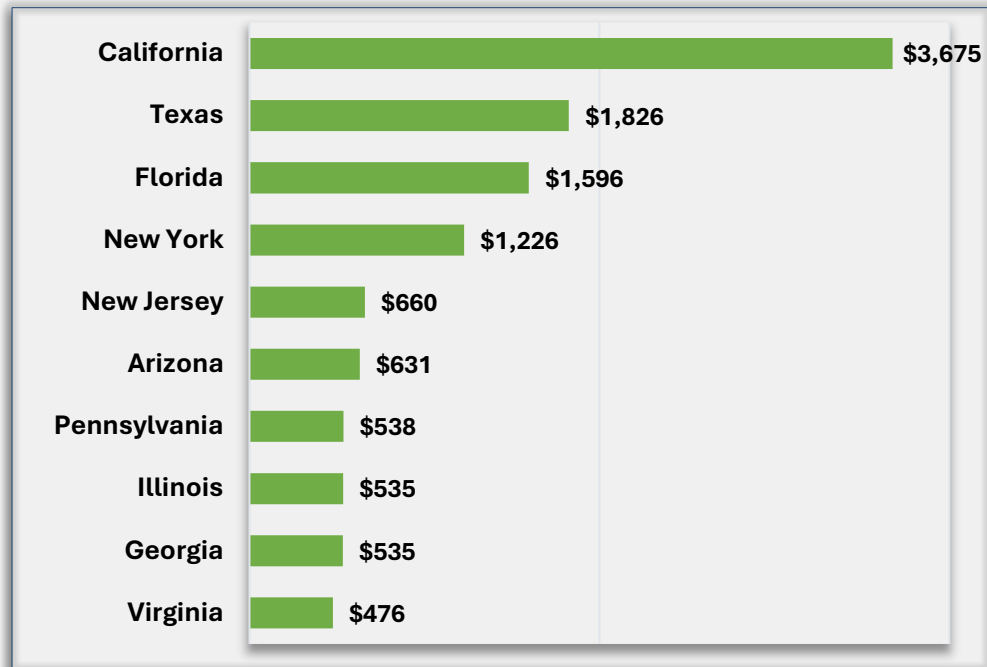
\* Crime Type or Descriptor was not captured in these years.

## Complaints by State

### Top 10 States by Number of Complaints<sup>14</sup>



### Top 10 States by Loss (In Millions)<sup>15</sup>



<sup>14</sup> Accessibility description: Chart depicts the top 10 states based on number of complaints. These include California, Texas, Florida, New York, Illinois, Pennsylvania, Arizona, Ohio, North Carolina, and Georgia. Please see Appendix C for more information regarding IC3 data.

<sup>15</sup> Accessibility description: Chart depicts the top 10 states based on reported losses are labeled. These include California, Texas, Florida, New York, New Jersey, Arizona, Pennsylvania, Illinois, Georgia, and Virginia. Please see Appendix C for more information regarding IC3 data.

### States by Complaint Count

Rank	State	Complaints	State	Complaints
1	California	116,414	30 Kentucky	9,414
2	Texas	97,912	31 Louisiana	8,623
3	Florida	71,843	32 Kansas	7,927
4	New York	45,255	33 Arkansas	6,161
5	Illinois	32,977	34 New Mexico	5,688
6	Pennsylvania	31,154	35 Iowa	5,436
7	Arizona	28,868	36 Mississippi	5,084
8	Ohio	27,626	37 Idaho	4,479
9	North Carolina	25,940	38 New Hampshire	4,374
10	Georgia	25,936	39 West Virginia	4,209
11	Washington	25,619	40 Puerto Rico	4,108
12	Virginia	25,314	41 Nebraska	3,724
13	Massachusetts	22,936	42 Hawaii	3,328
14	Michigan	22,191	43 Alaska	3,202
15	Indiana	20,777	44 District of Columbia	3,113
16	New Jersey	20,648	45 Delaware	3,089
17	Maryland	19,430	46 Maine	2,888
18	Colorado	18,847	47 Rhode Island	2,700
19	Wisconsin	16,680	48 Montana	2,618
20	Tennessee	16,261	49 South Dakota	2,514
21	South Carolina	14,699	50 Vermont	1,580
22	Missouri	14,087	51 Wyoming	1,552
23	Minnesota	13,595	52 North Dakota	1,418
24	Nevada	13,366	53 United States Minor Outlying Islands	211
25	Oregon	12,477	54 American Samoa	188
26	Oklahoma	11,964	55 Guam	171
27	Alabama	9,936	56 Virgin Islands, U.S.	125
28	Utah	9,903	57 Northern Mariana Islands	30
29	Connecticut	9,714		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## States by Complaint Loss

Rank	State	Loss	State	Loss
1	California	\$3,674,716,305	30 Oklahoma	\$131,921,776
2	Texas	\$1,825,636,181	31 Kentucky	\$119,685,861
3	Florida	\$1,596,138,595	32 Hawaii	\$106,447,375
4	New York	\$1,226,307,877	33 Louisiana	\$105,440,238
5	New Jersey	\$660,411,901	34 Arkansas	\$102,541,947
6	Arizona	\$630,700,609	35 District of Columbia	\$97,368,097
7	Pennsylvania	\$537,787,231	36 Iowa	\$95,520,131
8	Illinois	\$535,255,201	37 West Virginia	\$92,648,544
9	Georgia	\$534,581,965	38 Idaho	\$88,725,284
10	Virginia	\$476,120,025	39 New Mexico	\$85,571,285
11	Washington	\$458,165,375	40 Mississippi	\$77,360,761
12	North Carolina	\$431,561,716	41 Rhode Island	\$71,960,439
13	Ohio	\$421,289,526	42 Nebraska	\$71,844,724
14	Massachusetts	\$410,924,066	43 Delaware	\$62,012,494
15	Maryland	\$390,242,821	44 New Hampshire	\$59,283,023
16	Michigan	\$381,068,131	45 Maine	\$56,536,020
17	Colorado	\$355,049,719	46 Montana	\$53,192,859
18	Nevada	\$302,235,247	47 South Dakota	\$51,452,806
19	Tennessee	\$269,214,519	48 Puerto Rico	\$44,266,380
20	South Carolina	\$264,083,026	49 Alaska	\$39,972,438
21	Minnesota	\$248,892,986	50 North Dakota	\$37,865,442
22	Missouri	\$233,933,401	51 Vermont	\$26,567,033
23	Indiana	\$233,016,771	52 Wyoming	\$25,826,205
24	Connecticut	\$219,500,212	53 United States Minor Outlying Islands	\$3,486,871
25	Utah	\$195,417,205	54 Virgin Islands, U.S.	\$2,448,598
26	Wisconsin	\$194,227,722	55 Guam	\$1,416,690
27	Oregon	\$193,196,479	56 Northern Mariana Islands	\$290,585
28	Alabama	\$167,212,658	57 American Samoa	\$172,395
29	Kansas	\$147,337,101		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

**Complaints per 100K Citizens\***

<b>Rank</b>	<b>State</b>	<b>Count</b>		<b>State</b>	<b>Count</b>
1	<b>District of Columbia</b>	448.8	27	<b>Vermont</b>	245.1
2	<b>Alaska</b>	434.3	28	<b>Rhode Island</b>	242.3
3	<b>Nevada</b>	407.2	29	<b>Pennsylvania</b>	238.6
4	<b>Arizona</b>	378.7	30	<b>West Virginia</b>	238.3
5	<b>Massachusetts</b>	320.6	31	<b>Minnesota</b>	233.2
6	<b>Washington</b>	320.2	32	<b>Hawaii</b>	232.3
7	<b>Colorado</b>	313.5	33	<b>Ohio</b>	232.1
8	<b>Maryland</b>	310.1	34	<b>North Carolina</b>	231.6
9	<b>New Hampshire</b>	309.0	35	<b>Georgia</b>	229.5
10	<b>Texas</b>	308.8	36	<b>Montana</b>	228.7
11	<b>Florida</b>	306.2	37	<b>New York</b>	226.2
12	<b>Indiana</b>	297.9	38	<b>Missouri</b>	224.7
13	<b>California</b>	295.8	39	<b>Tennessee</b>	222.3
14	<b>Oregon</b>	292.0	40	<b>Idaho</b>	220.7
15	<b>Delaware</b>	291.4	41	<b>Michigan</b>	219.1
16	<b>Oklahoma</b>	290.2	42	<b>New Jersey</b>	216.2
17	<b>Virginia</b>	285.1	43	<b>Kentucky</b>	204.3
18	<b>Utah</b>	279.8	44	<b>Maine</b>	204.1
19	<b>Wisconsin</b>	279.3	45	<b>Arkansas</b>	197.8
20	<b>South Dakota</b>	268.8	46	<b>Alabama</b>	191.3
21	<b>New Mexico</b>	267.6	47	<b>Louisiana</b>	186.7
22	<b>Kansas</b>	266.3	48	<b>Nebraska</b>	184.5
23	<b>South Carolina</b>	263.9	49	<b>North Dakota</b>	177.4
24	<b>Wyoming</b>	263.6	50	<b>Mississippi</b>	172.1
25	<b>Connecticut</b>	263.4	51	<b>Iowa</b>	167.9
26	<b>Illinois</b>	259.3	52	<b>Puerto Rico</b>	129.0

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

### Losses per 100K Citizens\*

Rank	State	Loss	Rank	State	Loss
1	District of Columbia	\$14,037,165	27	Oregon	\$4,520,711
2	California	\$9,337,282	28	Wyoming	\$4,386,594
3	Nevada	\$9,208,347	29	Idaho	\$4,371,279
4	Arizona	\$8,272,766	30	Minnesota	\$4,268,880
5	Hawaii	\$7,429,222	31	Illinois	\$4,208,265
6	New Jersey	\$6,916,601	32	New Hampshire	\$4,188,601
7	Florida	\$6,802,930	33	Vermont	\$4,121,073
8	Rhode Island	\$6,456,625	34	Pennsylvania	\$4,117,999
9	Maryland	\$6,228,591	35	New Mexico	\$4,025,941
10	New York	\$6,130,795	36	Maine	\$3,995,834
11	Connecticut	\$5,950,941	37	North Carolina	\$3,853,929
12	Colorado	\$5,905,133	38	Michigan	\$3,762,564
13	Delaware	\$5,850,500	39	Missouri	\$3,730,673
14	Texas	\$5,757,321	40	Tennessee	\$3,680,270
15	Massachusetts	\$5,743,909	41	Nebraska	\$3,560,184
16	Washington	\$5,726,337	42	Ohio	\$3,540,096
17	Utah	\$5,521,970	43	Indiana	\$3,341,541
18	South Dakota	\$5,502,421	44	Arkansas	\$3,292,097
19	Alaska	\$5,421,682	45	Wisconsin	\$3,251,878
20	Virginia	\$5,361,647	46	Alabama	\$3,219,908
21	West Virginia	\$5,245,800	47	Oklahoma	\$3,199,432
22	Kansas	\$4,948,815	48	Iowa	\$2,949,621
23	South Carolina	\$4,740,934	49	Mississippi	\$2,618,706
24	North Dakota	\$4,736,982	50	Kentucky	\$2,597,990
25	Georgia	\$4,729,664	51	Louisiana	\$2,283,151
26	Montana	\$4,646,906	52	Puerto Rico	\$1,389,911

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## Crime Types by Age Groups

Counts	Under 20	20 - 29	30 - 39	40 - 49	50 - 59
<b>Advanced Fee</b>	288	991	1,170	1,120	1,169
<b>BEC</b>	73	1,250	3,619	5,090	4,910
<b>Botnet</b>	106	155	137	129	56
<b>Charity</b>	34	87	114	148	101
<b>Confidence/Romance</b>	393	1,886	2,501	3,010	3,745
<b>Credit Card/ Check Fraud</b>	451	1,760	2,767	2,958	2,810
<b>Data Breach</b>	21	135	443	625	522
<b>Employment</b>	835	4,555	5,025	4,524	3,671
<b>Extortion</b>	13,110	26,963	15,866	11,279	7,841
<b>Government Impersonation</b>	420	3,401	5,446	6,136	5,636
<b>Harassment/Stalking</b>	1,827	4,711	5,473	4,076	2,249
<b>Identity Theft</b>	487	3,526	6,498	6,433	5,528
<b>Investment</b>	901	6,102	10,996	13,737	12,773
<b>IPR/Copyright and Counterfeit</b>	70	261	504	502	359
<b>Lottery/Sweepstakes/ Inheritance</b>	75	315	528	679	773
<b>Malware</b>	57	159	193	147	93
<b>Non-payment/ Non-Delivery</b>	2,351	8,331	9,947	9,981	8,158
<b>Other</b>	2,159	2,864	3,938	3,659	2,620
<b>Overpayment</b>	304	350	294	295	310
<b>Personal Data Breach</b>	2,601	7,877	13,238	13,403	9,703
<b>Phishing/Spoofing</b>	2,380	19,765	27,433	27,800	26,782
<b>Ransomware</b>	15	67	204	427	457
<b>Real Estate</b>	158	1,986	2,189	2,037	2,036
<b>SIM Swap</b>	6	61	162	210	194
<b>Tech/Customer Support</b>	405	3,045	4,864	5,182	5,512
<b>Threats of Violence</b>	508	1,045	1,084	829	531

60+ crime type information is available in the 2025 IC3 Elder Fraud Section.

Losses	Under 20	20 - 29	30 - 39	40 - 49	50 - 59
<b>Advanced Fee</b>	\$327,823	\$7,081,874	\$13,311,458	\$18,801,337	\$25,811,979
<b>BEC</b>	\$15,137,36	\$45,754,756	\$356,707,180	\$624,292,591	\$618,105,890
<b>Botnet</b>	\$20,532	\$53,205	\$383,680	\$5,923,019	\$191,046
<b>Charity</b>	\$41,917	\$914,968	\$282,824	\$323,872	\$224,605
<b>Confidence/ Romance</b>	\$3,057,718	\$25,097,693	\$42,460,967	\$74,644,395	\$131,385,454
<b>Credit Card/ Check Fraud</b>	\$606,192	\$6,076,760	\$32,039,262	\$49,971,180	\$43,817,766
<b>Data Breach</b>	\$1,741,450	\$4,158,310	\$72,145,136	\$64,973,932	\$77,385,567
<b>Employment</b>	\$1,489,854	\$33,049,422	\$42,865,213	\$57,604,303	\$100,853,442
<b>Extortion</b>	\$1,715,733	\$12,179,028	\$14,964,819	\$13,427,693	\$15,710,381
<b>Government Impersonation</b>	\$8,583,219	\$50,358,843	\$82,005,707	\$55,019,630	\$84,516,785
<b>Harassment/ Stalking</b>	\$218,229	\$591,102	\$5,343,712	\$6,098,635	\$4,721,979
<b>Identity Theft</b>	\$1,547,663	\$10,815,080	\$19,440,941	\$27,807,082	\$35,573,535
<b>Investment</b>	\$17,022,80	\$163,145,27	\$564,898,178	\$1,152,243,858	\$1,748,651,287
<b>IPR/Copyright &amp; Counterfeit</b>	\$72,650	\$377,545	\$2,108,962	\$14,161,896	\$3,270,925
<b>Lottery/ Sweepstakes/ Inheritance</b>	\$89,050	\$2,273,833	\$5,047,453	\$12,877,295	\$19,385,699
<b>Malware</b>	\$3,766	\$504,839	\$1,714,483	\$1,998,406	\$10,661,574
<b>Non-payment/ Non-Delivery</b>	\$2,391,036	\$37,006,257	\$69,016,236	\$97,620,771	\$73,863,630
<b>Other</b>	\$2,616,321	\$12,967,479	\$58,543,283	\$96,902,505	\$85,195,234
<b>Overpayment</b>	\$181,495	\$783,264	\$3,937,790	\$2,601,879	\$2,301,154
<b>Personal Data Breach</b>	\$7,314,429	\$86,102,381	\$173,434,730	\$241,244,329	\$225,239,544
<b>Phishing/ Spoofing</b>	\$360,429	\$7,954,797	\$32,669,619	\$33,063,856	\$30,918,367
<b>Ransomware</b>	\$0	\$2,956,745	\$821,075	\$6,918,385	\$5,394,639
<b>Real Estate</b>	\$189,875	\$7,294,459	\$23,316,890	\$33,724,892	\$46,373,027
<b>SIM Swap</b>	\$6,303	\$153,247	\$796,329	\$3,399,856	\$2,698,369
<b>Tech/ Customer Support</b>	\$2,328,729	\$45,718,725	\$119,274,031	\$261,313,644	\$283,494,484
<b>Threats of Violence</b>	\$40,982	\$159,365	\$7,335,885	\$454,130	\$239,803

60+ crime type information is available in the 2025 IC3 Elder Fraud Section.

# Complainants 17 Years Old or Younger

Recent trends indicate a serious rise in cybercrimes targeting minors (17 years old or younger), driven by sextortion, cyberbullying, and online grooming.

The FBI is actively investigating a violent online group known as "764," which coerces children into engaging in self-harm, animal cruelty, and suicidal acts on live stream, sometimes leading to the death of the victim.

In 2025, IC3 referred more than 5,700 submissions involving minors to NCMEC.

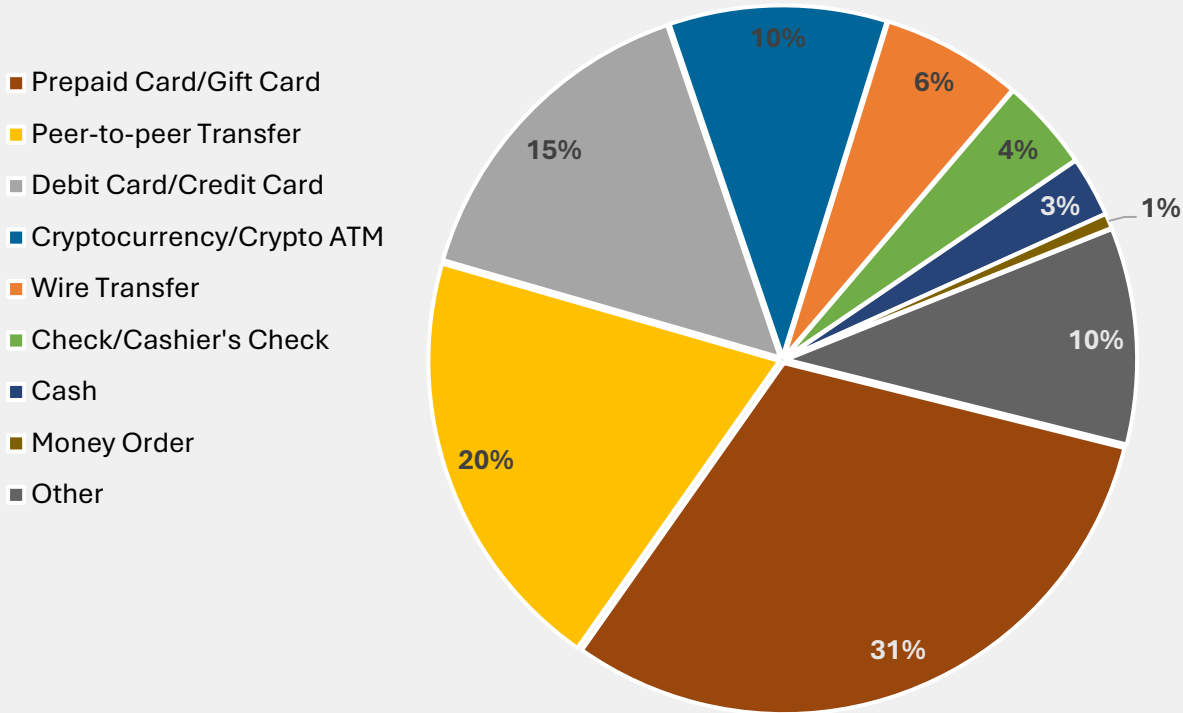
### Highlights

13,168 Complaints  
\$12,988,892 Losses  
\$986 Average Loss

**Read More:** [IC3 - Violent Online Networks Target Vulnerable and Underage Populations Across the United States and Around the Globe](#)

16

Transaction Types Reported by 17 and Younger



<sup>16</sup> Accessibility description: Chart depicts the most reported transaction types by complainants 17 years old or younger.

### 17 or Younger By Complaint Count

Crime Type	Complaints	Crime Type	Complaints
<b>Extortion</b>	5,151	<b>Government Impersonation</b>	99
<b>Personal Data Breach</b>	1,510	<b>Tech Support</b>	85
<b>Other</b>	1,460	<b>Botnet</b>	65
<b>Harassment/Stalking</b>	1,053	<b>Confidence/Romance</b>	57
<b>Phishing/Spoofing</b>	878	<b>IPR/Copyright and Counterfeit</b>	42
<b>Non-payment/Non-Delivery</b>	825	<b>Malware</b>	29
<b>Threats of Violence</b>	251	<b>Real Estate</b>	23
<b>Employment</b>	246	<b>Charity</b>	16
<b>Investment</b>	237	<b>Lottery/Sweepstakes/Inheritance</b>	13
<b>Identity Theft</b>	181	<b>Data Breach</b>	9
<b>Overpayment</b>	164	<b>Ransomware</b>	5
<b>Credit Card/Check Fraud</b>	125	<b>BEC</b>	4
<b>Advanced Fee</b>	102	<b>SIM Swap</b>	1

### *Descriptors*

<b>Cryptocurrency</b>	950
<b>AI Related</b>	355
<b>Crimes Against Children</b>	5,200

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

**17 or Younger By Complaint Loss**

<b>Crime Type</b>	<b>Loss</b>	<b>Crime Type</b>	<b>Loss</b>
<b>Investment</b>	\$4,743,664	<b>Confidence/Romance</b>	\$75,440
<b>Other</b>	\$1,810,134	<b>IPR/Copyright and Counterfeit</b>	\$72,188
<b>Data Breach</b>	\$1,693,400	<b>Overpayment</b>	\$61,918
<b>Government Impersonation</b>	\$1,412,003	<b>Real Estate</b>	\$43,861
<b>Non-payment/ Non-Delivery</b>	\$648,538	<b>Advanced Fee</b>	\$23,765
<b>Identity Theft</b>	\$510,553	<b>BEC</b>	\$10,750
<b>Personal Data Breach</b>	\$500,264	<b>Charity</b>	\$4,552
<b>Extortion</b>	\$468,831	<b>Threats of Violence</b>	\$1,547
<b>Tech Support</b>	\$396,487	<b>Lottery/Sweepstakes/ Inheritance</b>	\$488
<b>Harassment/Stalking</b>	\$203,807	<b>Botnet</b>	\$82
<b>Credit Card/Check Fraud</b>	\$121,506	<b>Malware</b>	\$35
<b>Employment</b>	\$106,727	<b>Ransomware</b>	\$0
<b>Phishing/Spoofing</b>	\$77,852	<b>SIM Swap</b>	\$0
<b>Descriptors</b>			
<b>Cryptocurrency</b>	\$5,620,716		
<b>AI Related</b>	\$126,391		
<b>Crimes Against Children</b>	\$298,240		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

### 17/Younger Complaints by State

Rank	State	Count	Rank	State	Count
1	California	1,492	30	Oregon	146
2	Texas	1,082	31	Kentucky	143
3	Florida	702	32	Connecticut	129
4	New York	539	33	Louisiana	111
5	Illinois	371	34	Kansas	94
5	Pennsylvania	366	35	Idaho	91
7	North Carolina	365	36	Mississippi	91
8	Arizona	341	37	Arkansas	89
9	Ohio	337	38	Iowa	82
10	Georgia	317	39	Nebraska	71
11	Washington	312	40	Alaska	63
12	Michigan	292	41	New Mexico	62
13	Virginia	292	42	West Virginia	55
14	Colorado	240	43	Maine	44
15	New Jersey	240	44	New Hampshire	38
16	Indiana	226	44	Hawaii	37
17	Maryland	224	46	Rhode Island	35
18	Missouri	205	47	Delaware	34
18	Nevada	202	47	Montana	33
20	Tennessee	197	49	Puerto Rico	30
21	Massachusetts	195	50	District of Columbia	23
22	Minnesota	180	51	North Dakota	23
23	Alabama	175	52	South Dakota	22
23	Utah	168	53	Wyoming	21
25	South Carolina	165	54	Vermont	16
26	Oklahoma	160	55	United States Minor Outlying Islands	8
27	Wisconsin	154	56	Guam	2

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## 17/Younger Losses by State

Rank	State	Loss	State	Loss
1	Georgia	\$3,087,376	30 District of Columbia	\$34,840
2	Texas	\$1,676,326	31 Tennessee	\$27,917
3	Utah	\$1,017,481	32 North Carolina	\$27,457
4	Washington	\$758,830	33 Missouri	\$24,678
5	South Carolina	\$758,428	34 Puerto Rico	\$16,566
6	California	\$719,483	35 Louisiana	\$14,661
7	New York	\$578,293	36 Wisconsin	\$14,612
8	Arizona	\$491,722	37 Iowa	\$14,576
9	Illinois	\$269,389	38 Maryland	\$14,395
10	Florida	\$211,888	39 Wyoming	\$13,749
11	New Mexico	\$170,580	40 Indiana	\$10,691
12	West Virginia	\$153,035	41 Maine	\$9,345
13	Virginia	\$150,736	42 Idaho	\$7,171
14	Michigan	\$148,264	43 Nebraska	\$6,404
15	Massachusetts	\$101,315	44 Hawaii	\$6,231
16	New Jersey	\$85,885	45 Alaska	\$4,880
17	Minnesota	\$76,832	46 South Dakota	\$4,080
18	Oregon	\$59,874	47 Arkansas	\$3,479
19	Colorado	\$55,032	48 Mississippi	\$3,041
20	Ohio	\$53,439	49 North Dakota	\$2,365
21	Alabama	\$52,541	50 Montana	\$2,261
22	Kansas	\$47,016	51 New Hampshire	\$1,862
23	Pennsylvania	\$46,527	52 Rhode Island	\$1,021
24	Connecticut	\$43,520	52 Vermont	\$744
25	Nevada	\$40,475	52 Delaware	\$475
26	Oklahoma	\$39,442	52 Guam	\$0
27	Kentucky	\$37,653	52 United States Minor Outlying Islands	\$0

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

# Artificial Intelligence (AI) Used in Cybercrime

Like most technology, artificial intelligence (AI) is a tool which can be used for legitimate, helpful purposes or for criminal motives. AI technology enables the creation of convincing synthetic content, such as social media profiles and personalized conversations, often in mass quantities. People have manipulated video and audio similarly for decades, but the widespread availability of this developing technology makes it possible to create high-quality content. AI-enabled synthetic content is becoming increasingly difficult to detect and easier to make, which allows criminal actors to potentially conduct successful fraud schemes against individuals, businesses, and financial institutions.

In 2025, IC3 received more than 22,000 complaints reporting AI-related information. Adjusted losses of these complaints exceed \$893 million.

## Highlights

22,364 Complaints

\$893,346,472  
Losses

## How AI Could Be Used in Frauds/Scams

**BEC:** Chat generators can quickly create official-sounding emails mimicking a company's CEO or other officials. These emails can contain phishing links or directions to wire funds. Voice cloning can also be used to request wire payment or provide employee. There are multiple BEC tactics, and not all are AI-enabled. In 2025, businesses reported losses over \$30 million to BEC scams involving AI.

**Confidence/Romance Scams:** Scammers are creating fake profiles and scripts produced by AI chat generators to make speech more believable. In 2025, victims lost over \$19 million to Confidence/Romance scams with a likely AI-nexus. This type of scam also includes grandparent scams, or "distress" scams, in which voice cloning technology is used to mimic the sound of a loved one in distress. Victims claimed losses over \$5 million in 2025 to distress scams. This type of scam is evolving to mimic other family members or close friends in different types of emergency scenarios.

**Employment:** The use of voice spoofing, or potentially voice deepfakes, during online interviews of the potential applicants. In these interviews, the actions and lip movement of the person interviewed on-camera do not completely coordinate with the audio of the person speaking. At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually. From IC3 complaint data, there does not seem to be significant dollar loss associated as the goal generally appears to be gaining access to private computer networks. In 2025, victims reported losses of almost \$13 million to AI-involved employment type scams.

**Investment Scams:** Subjects in investment scams often use AI to enhance their conversations with potential victims allowing the scammers to quickly generate thousands of conversations that appear different to each prospective victim. Investment clubs employ AI-generated videos and voices of celebrities, CEOs, or trusted figures to create fraudulent, high-stakes opportunities. These scams often feature fake, professional-looking endorsements on social media or in video calls. This makes it harder for victims to detect they are in a scam. In 2025, losses in Investment complaints with a reported AI-nexus, surpassed \$632 million. However, overall losses to Investment scams exceeded \$8 billion, demonstrating that many victims do not realize the extent AI may be involved in scams.

### Read More

[IC3 - Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud](#)

[IC3 - Criminals Using Altered Proof-of-Life Media to Extort Victims in Virtual Kidnapping for Ransom Scams](#)

[IC3 - Fraudsters Target US Stock Investors through Investment Clubs Accessed on Social Media and Messaging Applications](#)

[Infographic; ABA Foundation and FBI Release New Infographic to Help Americans Spot and Avoid Deepfake Scams](#)

<b>AI References by Complaint Count</b>			
<b>Crime Type</b>	<b>Complaint</b>	<b>Crime Type</b>	<b>Complaint</b>
<b>Investment</b>	4,356	<b>BEC</b>	135
<b>Extortion</b>	1,764	<b>Real Estate</b>	115
<b>Personal Data Breach</b>	1,204	<b>Advanced Fee</b>	105
<b>Phishing/Spoofing</b>	803	<b>Threats of Violence</b>	95
<b>Harassment/Stalking</b>	763	<b>IPR/Copyright and Counterfeit</b>	63
<b>Employment</b>	691	<b>Data Breach</b>	60
<b>Confidence/Romance</b>	626	<b>Lottery/Sweepstakes/Inheritance</b>	54
<b>Non-Payment/ Non-Delivery</b>	609	<b>Malware</b>	42
<b>Tech/Customer Support</b>	574	<b>Charity</b>	19
<b>Other</b>	504	<b>Ransomware</b>	16
<b>Identity Theft</b>	460	<b>SIM Swap</b>	14
<b>Government Impersonation</b>	260	<b>Overpayment</b>	13
<b>Credit Card/Check Fraud</b>	139	<b>Botnet</b>	12
<i>Descriptors</i>			
<b>Crimes Against Children</b>	214		
<b>Cryptocurrency</b>	7,623		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

<b>AI References by Complaint Loss</b>			
<b>Crime Type</b>	<b>Loss</b>	<b>Crime Type</b>	<b>Loss</b>
<b>Investment</b>	\$632,041,188	<b>Extortion</b>	\$2,940,642
<b>BEC</b>	\$30,256,592	<b>Real Estate</b>	\$2,699,085
<b>Tech/Customer Support</b>	\$19,457,078	<b>Credit Card/Check Fraud</b>	\$1,836,105
<b>Confidence/Romance</b>	\$19,041,653	<b>Identity Theft</b>	\$1,643,308
<b>Personal Data Breach</b>	\$18,767,964	<b>Advanced Fee</b>	\$1,642,712
<b>Employment</b>	\$12,550,185	<b>Harassment/Stalking</b>	\$1,445,378
<b>Other</b>	\$11,750,591	<b>Malware</b>	\$1,248,199
<b>Phishing/Spoofing</b>	\$10,283,732	<b>Botnet</b>	\$697,226
<b>IPR/Copyright and Counterfeit</b>	\$10,103,789	<b>Charity</b>	\$531,455
<b>Government Impersonation</b>	\$7,061,628	<b>SIM Swap</b>	\$13,082
<b>Lottery/Sweepstakes/Inheritance</b>	\$4,486,965	<b>Threats of Violence</b>	\$9,576
<b>Data Breach</b>	\$4,319,380	<b>Overpayment</b>	\$4,719
<b>Non-Payment/Non-Delivery</b>	\$3,726,777	<b>Ransomware</b>	\$0
<b>Descriptors</b>			
<b>Crimes Against Children</b>	\$9,866		
<b>Cryptocurrency</b>	\$658,714,247		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

# 2025 Elder Fraud



INTERNET CRIME COMPLAINT CENTER

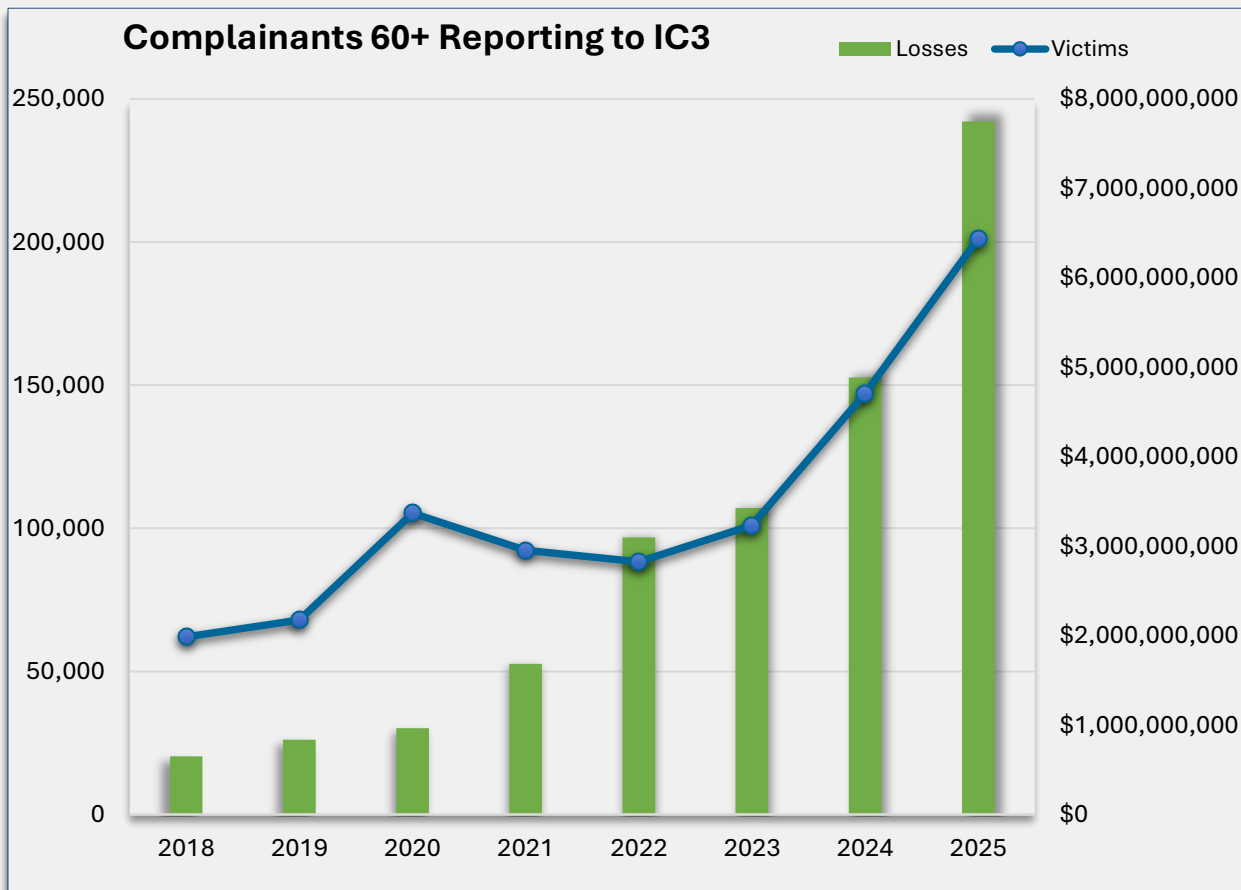
# IC3 Elder Fraud – Complaints filed by Individuals 60+

17

## Highlights

- 201,266 Complaints  
↑ 37% FROM 2024
- \$7.748 Billion in Losses  
↑ 59% FROM 2024
- \$38,500 Average Loss
- 12,444 Complainants Lost > \$100K

18



<sup>17</sup> Accessibility Description: Describes Elder Fraud highlights: 201,266 complaints (37% increase from 2024); \$7,748 billion losses (59% increase from 2024); \$38,500 average loss; 12,444 complainants lost more than \$100K.

<sup>18</sup> Accessibility Description: Chart describes counts and losses for those reporting as 60+ from 2018 to 2025. Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## Crime Types Reported by 60+

<b>Complainants 60+</b>			
<b>Crime Type</b>	<b>Count</b>	<b>Crime Type</b>	<b>Count</b>
<b>Phishing/Spoofing</b>	48,064	<b>Lottery/Sweepstakes/Inheritance</b>	2,785
<b>Tech/Customer Support</b>	21,333	<b>Real Estate</b>	2,473
<b>Investment</b>	16,926	<b>Advanced Fee</b>	2,020
<b>Personal Data Breach</b>	11,705	<b>Harassment/Stalking</b>	1,160
<b>Confidence/Romance</b>	10,188	<b>Overpayment</b>	477
<b>Non-Payment/Non-Delivery</b>	9,743	<b>Ransomware</b>	358
<b>Extortion</b>	9,111	<b>Data Breach</b>	350
<b>Government Impersonation</b>	8,628	<b>Threats of Violence</b>	349
<b>Identity Theft</b>	5,359	<b>IPR/Copyright and Counterfeit</b>	316
<b>Credit Card/Check Fraud</b>	5,200	<b>SIM Swap</b>	222
<b>Business Email Compromise*</b>	4,566	<b>Malware</b>	138
<b>Other</b>	3,001	<b>Charity</b>	126
<b>Employment</b>	2,853	<b>Botnet</b>	36
<b>Descriptors</b>			
<b>Cryptocurrency</b>	42,271		
<b>AI Related</b>	3,143		
<b>Crimes Against Children</b>	94		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## Crime Types Reported by 60+, *continued*

<b>Complainants 60+ Losses</b>			
<b>Crime Type</b>	<b>Loss</b>	<b>Crime Type</b>	<b>Loss</b>
<b>Investment</b>	\$3,519,296,354	<b>Advanced Fee</b>	\$65,877,660
<b>Tech/Customer Support</b>	\$1,040,730,043	<b>Extortion</b>	\$54,309,050
<b>Confidence/Romance</b>	\$584,032,745	<b>Data Breach</b>	\$48,555,751
<b>Business Email Compromise</b>	\$568,048,472	<b>Identity Theft</b>	\$48,546,133
<b>Government Impersonation</b>	\$413,206,251	<b>Overpayment</b>	\$8,045,862
<b>Personal Data Breach</b>	\$324,470,413	<b>SIM Swap</b>	\$6,741,791
<b>Other</b>	\$153,412,996	<b>Ransomware</b>	\$5,644,789
<b>Lottery/Sweepstakes/Inheritance</b>	\$136,328,519	<b>IPR/Copyright and Counterfeit</b>	\$4,493,512
<b>Non-Payment/Non-Delivery</b>	\$127,041,813	<b>Charity</b>	\$3,474,668
<b>Real Estate</b>	\$123,671,936	<b>Malware</b>	\$3,433,325
<b>Employment</b>	\$78,712,899	<b>Harassment/Stalking</b>	\$3,134,436
<b>Phishing/Spoofing</b>	\$77,020,936	<b>Botnet</b>	\$945,812
<b>Credit Card/Check Fraud</b>	\$71,880,416	<b>Threats of Violence</b>	\$394,040
<b>Descriptors</b>			
<b>Cryptocurrency</b>	\$4,347,081,557		
<b>AI Related</b>	\$352,496,231		
<b>Crimes Against Children</b>	\$5,806,300		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## Three Year Comparison

<b>60+ Complaint Count</b>			
<b>Crime Type</b>	<b>2025</b>	<b>2024</b>	<b>2023</b>
<b>Advanced Fee</b>	2,020	1,897	1,951
<b>Business Email Compromise</b>	4,566	3,300	3,080
<b>Botnet</b>	36	23	17
<b>Charity</b>	126	*	*
<b>Confidence/Romance</b>	10,188	7,626	6,740
<b>Credit Card/Check Fraud</b>	5,200	3,226	3,182
<b>Data Breach</b>	350	300	336
<b>Employment</b>	2,853	1,928	1,079
<b>Extortion</b>	9,111	12,618	5,396
<b>Government Impersonation</b>	8,628	4,521	3,517
<b>Harassment/Stalking</b>	1,160	696	568
<b>Identity Theft</b>	5,359	4,064	3,010
<b>Investment</b>	16,926	9,448	6,443
<b>IPR/Copyright and Counterfeit</b>	316	163	152
<b>Lottery/Sweepstakes/Inheritance</b>	2,785	1,711	1,771
<b>Malware</b>	138	45	67
<b>Non-Payment/Non-Delivery</b>	9,743	7,646	6,693
<b>Other</b>	3,001	2,017	1,447
<b>Overpayment</b>	477	527	698
<b>Personal Data Breach</b>	11,705	9,827	7,333
<b>Phishing/Spoofing</b>	48,064	23,252	2,856
<b>Ransomware</b>	358	208	175
<b>Real Estate</b>	2,473	1,765	1,498
<b>SIM Swap</b>	222	205	174
<b>Tech/Customer Support</b>	21,334	16,777	17,696
<b>Threats of Violence</b>	348	111	115
<b>Cryptocurrency</b>	42,271	33,369	16,968
<b>AI Related</b>	3,143	*	*
<b>Crimes Against Children</b>	94	25	26

\* Crime Type or Descriptor was not captured in these years.

## Three Year Comparison, *continued*

<b>60+ Complaint Losses</b>			
<b>Crime Type</b>	<b>2025</b>	<b>2024</b>	<b>2023</b>
<b>Advanced Fee</b>	\$65,877,660	\$41,622,868	\$67,923,263
<b>Business Email Compromise</b>	\$568,048,472	\$385,001,099	\$382,372,731
<b>Botnet</b>	\$945,812	\$14,852	\$23,142
<b>Charity</b>	\$3,474,668	*	*
<b>Confidence Fraud/Romance</b>	\$584,032,745	\$389,312,356	\$356,888,968
<b>Credit Card/Check Fraud</b>	\$71,880,416	\$33,813,267	\$37,862,023
<b>Data Breach</b>	\$48,555,751	\$28,546,213	\$23,913,130
<b>Employment</b>	\$78,712,899	\$37,882,347	\$6,835,684
<b>Extortion</b>	\$54,309,050	\$24,901,693	\$23,093,451
<b>Government Impersonation</b>	\$413,206,251	\$208,096,366	\$179,646,103
<b>Harassment/Stalking</b>	\$3,134,436	\$713,693	\$1,930,347
<b>Identity Theft</b>	\$48,546,133	\$28,463,106	\$34,551,900
<b>Investment</b>	\$3,519,296,354	\$1,834,242,515	\$1,243,010,600
<b>IPR/Copyright and Counterfeit</b>	\$4,493,512	\$1,076,710	\$183,169
<b>Lottery/Sweepstakes/Inheritance</b>	\$136,328,519	\$75,897,926	\$67,396,206
<b>Malware</b>	\$3,433,325	\$187,911	\$261,144
<b>Non-Payment/Non-Delivery</b>	\$127,041,813	\$76,794,753	\$59,018,965
<b>Other</b>	\$153,412,996	\$111,300,637	\$72,707,042
<b>Overpayment</b>	\$8,045,862	\$5,900,921	\$7,496,049
<b>Personal Data Breach</b>	\$324,470,413	\$254,187,196	\$109,724,027
<b>Phishing/Spoofing</b>	\$77,020,936	\$20,202,521	\$3,355,436
<b>Ransomware</b>	\$5,644,789	\$43,199	\$635,548
<b>Real Estate</b>	\$123,671,936	\$76,324,236	\$65,634,851
<b>SIM Swap</b>	\$6,741,791	\$6,342,329	\$15,148,072
<b>Tech/Customer Support</b>	\$1,040,879,243	\$982,440,006	\$589,759,770
<b>Threats of Violence</b>	\$244,840	\$300,488	\$5,128,768
<b>Cryptocurrency</b>	\$4,347,081,557	\$2,839,333,197	\$1,653,484,444
<b>AI Related</b>	\$352,496,231	*	*
<b>Crimes Against Children</b>	\$5,806,300	\$231,600	\$1,159,939

\* Crime Type or Descriptor was not captured in these years.

## Overall State Statistics for 60+

<b>Counts by State from Complainants 60+*</b>					
<b>Rank</b>	<b>State</b>	<b>Count</b>		<b>State</b>	<b>Count</b>
1	California	22,157	30	Alabama	2,057
2	Florida	17,147	31	Kansas	2,013
3	Texas	14,410	32	Louisiana	1,906
4	Arizona	9,834	33	Arkansas	1,658
5	New York	8,537	34	New Mexico	1,449
6	Illinois	7,701	35	Iowa	1,202
7	Pennsylvania	7,088	36	Idaho	1,136
8	Ohio	6,948	37	New Hampshire	1,063
9	North Carolina	5,942	38	Mississippi	959
10	Michigan	5,731	39	West Virginia	931
11	Virginia	5,509	40	Hawaii	917
12	Massachusetts	5,463	41	Montana	814
13	Washington	5,392	42	Delaware	796
14	Georgia	4,865	43	Nebraska	781
15	Maryland	4,573	44	Maine	721
16	Indiana	4,199	45	Alaska	666
17	New Jersey	4,111	46	Rhode Island	581
18	Colorado	4,061	47	Vermont	436
19	Tennessee	3,525	48	South Dakota	398
20	Missouri	3,247	49	Wyoming	397
21	South Carolina	3,136	50	District of Columbia	382
22	Wisconsin	3,014	51	Puerto Rico	351
23	Nevada	3,008	52	North Dakota	251
24	Oregon	2,910	53	United States Minor	33
25	Minnesota	2,550	54	U.S. Virgin Islands.	24
26	Oklahoma	2,449	55	Guam	18
27	Connecticut	2,360	56	American Samoa	4
28	Utah	2,341	57	Northern Mariana Islands	3
29	Kentucky	2,127			

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## Overall State Statistics for 60+, *continued*

Losses by State from Complainants 60+*					
Rank	State	Loss	State	Loss	
1	California	\$1,403,975,91	30	New Mexico	\$55,820,259
2	Florida	\$709,823,172	31	Kansas	\$55,730,977
3	Texas	\$678,564,081	32	Hawaii	\$55,385,929
4	New York	\$408,741,632	33	Oklahoma	\$53,333,350
5	Arizona	\$343,984,935	34	Iowa	\$44,136,901
6	New Jersey	\$249,808,786	35	Idaho	\$37,394,229
7	Virginia	\$220,941,233	36	Arkansas	\$36,958,369
8	Georgia	\$218,218,618	37	Louisiana	\$35,856,847
9	Pennsylvania	\$215,887,466	38	Mississippi	\$33,087,218
10	Illinois	\$189,491,209	39	Montana	\$31,773,898
11	Washington	\$179,706,909	40	Nebraska	\$28,430,567
12	Maryland	\$176,380,737	41	New Hampshire	\$25,068,671
13	Michigan	\$169,931,948	42	Maine	\$23,317,413
14	North Carolina	\$164,214,173	43	Rhode Island	\$21,561,918
15	Ohio	\$163,748,647	44	West Virginia	\$18,953,441
16	Colorado	\$144,529,956	45	Alaska	\$16,252,410
17	Nevada	\$115,267,384	46	Delaware	\$16,189,240
18	Massachusetts	\$113,880,471	47	South Dakota	\$14,708,875
19	Minnesota	\$111,387,313	48	District of Columbia	\$10,077,243
20	Tennessee	\$108,305,976	49	Vermont	\$8,548,782
21	South Carolina	\$97,344,480	50	Puerto Rico	\$8,167,452
22	Wisconsin	\$92,041,492	51	Wyoming	\$5,923,260
23	Missouri	\$91,563,419	52	North Dakota	\$5,895,155
24	Indiana	\$81,517,309	53	United States Minor	\$2,886,025
25	Oregon	\$77,481,475	54	U.S. Virgin Islands	\$1,088,540
26	Connecticut	\$73,178,714	55	Guam	\$380,178
27	Utah	\$65,946,070	56	American Samoa	\$46,362
28	Kentucky	\$64,441,069	57	Northern Mariana	\$15,500
29	Alabama	\$58,838,411			

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

# 2025 Cryptocurrency Fraud



INTERNET CRIME COMPLAINT CENTER

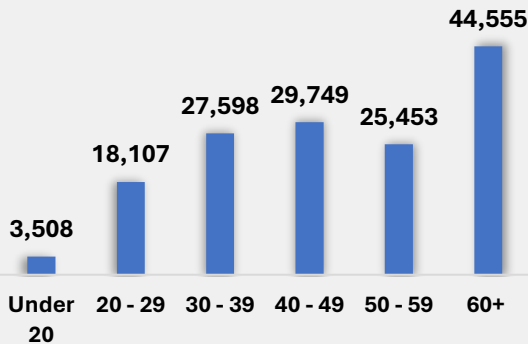
# Complaints Involving Cryptocurrency - 2025

## Highlights

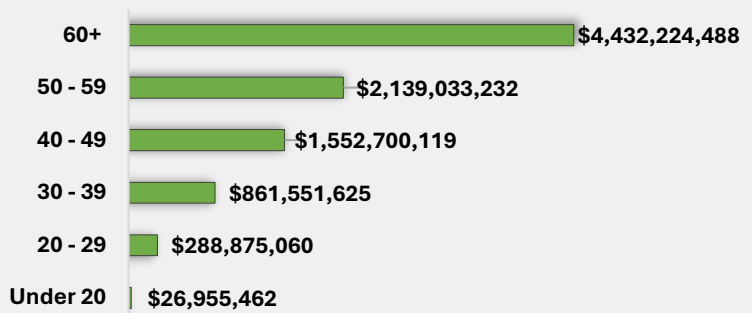
181,565 Complaints  
 ↑ 21% FROM 2024  
 \$11.366 Billion in Losses  
 ↑ 22% FROM 2024  
 18,589 Complainants Lost >\$100K  
 \$62,604 Average Loss

19

Crypto Counts by Age Range

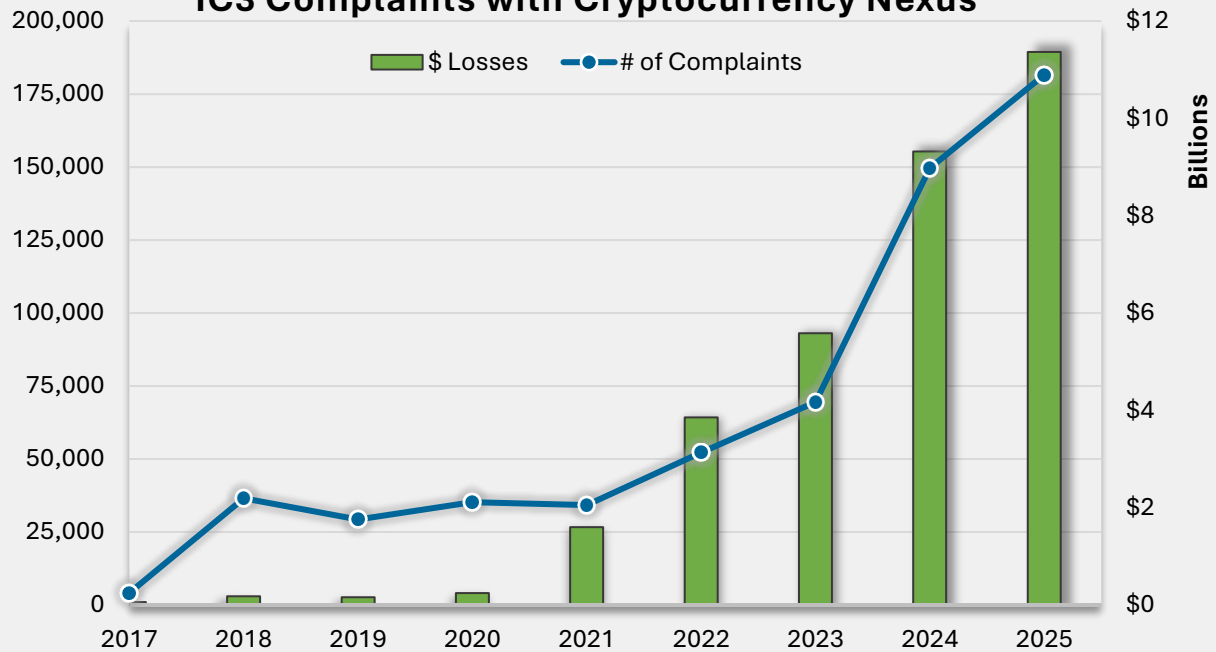


Crypto Losses by Age Range



20

IC3 Complaints with Cryptocurrency Nexus



21

<sup>19</sup> Accessibility Description: Describes Cryptocurrency highlights: 181,565 complaints (21% increase from 2024); \$11.366 billion in losses (22% increase from 2024), \$62,604 average loss, 18,589 complainants lost more than \$100,000

<sup>20</sup> Accessibility Description: Charts describe the count and losses associated with complaints reporting cryptocurrency by age range.

<sup>21</sup> Accessibility Description: Chart describes complaint counts and loss with a cryptocurrency nexus from 2017 to 2025.

## Cryptocurrency Fraud Trends

Cryptocurrency Investment	Crypto Investment Fraud Reported by Age Group		
	Age Group	Count	Losses
61,559 Complaints; \$7.228 billion			
-----			
48% Increase in Complaints from 2024	<b>Under 20</b>	629	\$12,582,997
25% Increase in Losses from 2024	<b>20 - 29</b>	4,627	\$117,353,587
-----	<b>30 - 39</b>	8,576	\$412,626,617
New Scam Center Strike Force Battles	<b>40 - 49</b>	10,750	\$924,623,370
Southeast Asian Crypto Investment Fraud	<b>50 - 59</b>	9,856	\$1,383,263,248
Targeting Americans   United States	<b>60+</b>	13,685	\$2,763,921,910
Department of Justice			

Cryptocurrency ATMs/Kiosks	Crypto ATM/Kiosk Use Reported by Age Group		
	Age Group	Count	Losses
13,460 Complaints; \$389 million in Losses			
-----			
23% Increase in Complaints from 2024	<b>Under 20</b>	58	\$124,013
58% Increase in Losses from 2024	<b>20 - 29</b>	825	\$6,474,240
-----	<b>30 - 39</b>	1,275	\$10,936,943
The FBI Warns of Fraudulent Schemes	<b>40 - 49</b>	1,472	\$20,826,227
Leveraging Cryptocurrency ATMs and QR	<b>50 - 59</b>	1,524	\$44,584,724
Codes to Facilitate Payment	<b>60+</b>	6,188	\$257,466,130

Recovery Scams	Recovery Scams Reported by Age Group		
	Age Group	Count	Losses*
10,516 Complaints; \$1.4 billion in Losses			
-----			
Increase in complaints reporting	<b>Under 20</b>	106	\$3,825,212
impersonation of government officials and	<b>20 - 29</b>	841	\$22,498,411
recovery firms.	<b>30 - 39</b>	1,511	\$76,183,433
-----	<b>40 - 49</b>	1,977	\$194,670,794
Fictitious Law Firms Targeting	<b>50 - 59</b>	1,706	\$298,233,813
Cryptocurrency Scam Victims Combine	<b>60+</b>	2,529	\$540,505,980
Multiple Exploitation Tactics While			
Offering to Recover Funds			
FBI Warns of Scammers Impersonating			
the IC3			

\*Losses may also include losses experienced from previous scams which prompted the contact with the recovery company.

## Crime Types with Cryptocurrency Nexus

<b>Complaints</b>			
<b>Crime Type</b>	<b>Count</b>	<b>Crime Type</b>	<b>Count</b>
<b>Investment</b>	61,559	<b>Ransomware</b>	902
<b>Extortion</b>	23,797	<b>Credit Card/Check Fraud</b>	901
<b>Tech/Customer Support</b>	17,355	<b>Data Breach</b>	866
<b>Personal Data Breach</b>	13,486	<b>Lottery/Sweepstakes/Inheritance</b>	826
<b>Employment</b>	10,338	<b>Real Estate</b>	715
<b>Phishing/Spoofing</b>	7,164	<b>Harassment/Stalking</b>	711
<b>Government Impersonation</b>	5,955	<b>Overpayment</b>	304
<b>Confidence/Romance</b>	5,925	<b>Threats of Violence</b>	210
<b>Non-Payment/Non-Delivery</b>	4,761	<b>Malware</b>	196
<b>Other</b>	2,332	<b>IPR/Copyright and Counterfeit</b>	182
<b>Advanced Fee</b>	2,319	<b>SIM Swap</b>	121
<b>Identity Theft</b>	1,656	<b>Charity</b>	65
<b>Business Email Compromise</b>	1,526	<b>Botnet</b>	53
<b>Descriptor</b>			
<b>AI Related</b>	8,712		
<b>Crimes Against Children</b>	276		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## Crime Types with Cryptocurrency Nexus, *continued*

<b>Losses</b>			
<b>Crime Type</b>	<b>Loss</b>	<b>Crime Type</b>	<b>Loss</b>
Investment	\$7,277,868,919	Lottery/Sweepstakes/ Inheritance	\$29,765,165
Tech/Customer Support	\$1,226,298,080	Real Estate	\$25,169,423
Personal Data Breach	\$939,398,686	Ransomware	\$17,068,810
Confidence/Romance	\$394,787,515	Identity Theft	\$16,995,129
Employment	\$288,199,807	Malware	\$15,693,486
Government Impersonation	\$281,146,737	Credit Card/Check Fraud	\$13,423,130
Other	\$147,700,762	Threats of Violence	\$7,375,785
Phishing/Spoofing	\$111,025,191	Overpayment	\$6,356,416
Data Breach	\$95,861,120	Harassment/Stalking	\$4,682,411
Business Email Compromise	\$83,771,329	SIM Swap	\$4,405,259
Non-Payment/ Non-Delivery	\$76,196,341	IPR/Copyright and Counterfeit	\$4,020,461
Advanced Fee	\$67,554,554	Charity	\$3,221,048
Extortion	\$63,195,612	Botnet	\$60,916
<b>Descriptor</b>			
AI Related	\$741,639,787		
Crimes Against Children	\$596,843		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## Overall State Statistics

<b>Cryptocurrency Complaints by State</b>					
<b>Rank</b>	<b>State</b>	<b>Count</b>	<b>State</b>	<b>Count</b>	<b>Count</b>
1	<b>California</b>	20,878	30	<b>Kentucky</b>	1,453
2	<b>Texas</b>	13,965	31	<b>Louisiana</b>	1,366
3	<b>Florida</b>	13,381	32	<b>Arkansas</b>	1,084
4	<b>New York</b>	8,088	33	<b>Kansas</b>	1,057
5	<b>Pennsylvania</b>	5,118	34	<b>Idaho</b>	1,023
6	<b>Arizona</b>	4,936	35	<b>New Mexico</b>	914
7	<b>Ohio</b>	4,925	36	<b>Puerto Rico</b>	903
8	<b>Illinois</b>	4,910	37	<b>Iowa</b>	887
9	<b>Washington</b>	4,589	38	<b>Hawaii</b>	826
10	<b>Georgia</b>	4,492	39	<b>Mississippi</b>	815
11	<b>New Jersey</b>	4,459	40	<b>New Hampshire</b>	767
12	<b>North Carolina</b>	4,340	41	<b>Nebraska</b>	730
13	<b>Virginia</b>	4,246	42	<b>South Dakota</b>	603
14	<b>Colorado</b>	4,066	43	<b>Montana</b>	590
15	<b>Michigan</b>	3,648	44	<b>West Virginia</b>	556
16	<b>Maryland</b>	3,226	45	<b>Maine</b>	524
17	<b>Wisconsin</b>	3,092	46	<b>Alaska</b>	482
18	<b>Massachusetts</b>	2,983	47	<b>District of Columbia</b>	448
19	<b>Tennessee</b>	2,854	48	<b>Delaware</b>	436
20	<b>Nevada</b>	2,518	49	<b>Rhode Island</b>	414
21	<b>Missouri</b>	2,500	50	<b>North Dakota</b>	300
22	<b>Minnesota</b>	2,253	51	<b>Wyoming</b>	273
23	<b>Indiana</b>	2,211	52	<b>Vermont</b>	212
24	<b>South Carolina</b>	2,176	53	<b>Guam</b>	26
25	<b>Oregon</b>	2,175	53	<b>United States Minor Outlying Islands</b>	26
26	<b>Utah</b>	1,833	55	<b>Virgin Islands, U.S.</b>	22
27	<b>Alabama</b>	1,687	56	<b>American Samoa</b>	8
28	<b>Oklahoma</b>	1,581	57	<b>Northern Mariana Islands</b>	2
29	<b>Connecticut</b>	1,480			

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## Overall State Statistics, *continued*

Cryptocurrency Losses by State					
Rank	State	Loss		State	Loss
1	California	\$2,099,014,715	30	Kansas	\$78,062,42
2	Texas	\$1,016,062,841	31	Oklahoma	\$62,394,49
3	Florida	\$914,525,497	32	Kentucky	\$60,156,29
4	New York	\$593,370,013	33	Louisiana	\$53,679,26
5	Oregon	\$545,938,510	34	Idaho	\$48,296,73
6	New Jersey	\$383,662,185	35	New Mexico	\$45,229,20
7	Arizona	\$346,269,314	36	Arkansas	\$44,064,46
8	Pennsylvania	\$292,893,338	37	Iowa	\$43,685,42
9	Georgia	\$264,502,467	38	Mississippi	\$38,286,77
10	Washington	\$263,067,281	39	District of Columbia	\$37,013,58
11	Virginia	\$261,243,361	40	New Hampshire	\$36,481,77
12	Illinois	\$257,919,562	41	Maine	\$35,795,02
13	Maryland	\$246,476,431	42	Montana	\$35,136,68
14	North Carolina	\$229,649,863	43	Nebraska	\$34,861,42
15	Michigan	\$210,230,468	44	Delaware	\$26,893,09
16	Ohio	\$208,874,675	45	Puerto Rico	\$24,234,78
17	Nevada	\$205,388,286	46	West Virginia	\$23,208,70
18	Colorado	\$202,127,121	47	South Dakota	\$23,169,15
19	Massachusetts	\$180,158,815	48	North Dakota	\$20,083,06
20	Minnesota	\$151,658,166	49	Alaska	\$18,610,38
21	Tennessee	\$142,006,339	50	Rhode Island	\$14,125,09
22	South Carolina	\$118,509,954	51	Wyoming	\$13,695,30
23	Missouri	\$108,769,750	52	Vermont	\$7,532,107
24	Utah	\$107,495,105	53	Virgin Islands, U.S.	\$1,056,161
25	Indiana	\$99,629,036	54	United States Minor Outlying Islands	\$1,045,183
26	Alabama	\$93,813,940	55	Guam	\$696,853
27	Connecticut	\$91,039,266	56	American Samoa	\$105,197
28	Wisconsin	\$87,426,944	57	Northern Mariana	\$1,000
29	Hawaii	\$79,759,336			

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

## Appendix A: About IC3

Today's FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. The 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, the 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 the 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 such as ransomware, intrusions (hacking), extortion, international money laundering, investment fraud, and a growing list of crimes. As of this publication, IC3 has received over 10 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 the 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, PSAs, and Industry Alerts to further educate and protect yourself, as well as your family, friends, and community.

## Appendix B: Definitions and Descriptors

### 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.

**Charity:** Using deception to get money from individuals believing they are making donations to legitimate charities and/or charities representing victims of natural disasters shortly after the incident occurs.

**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.

**Data Breach:** A data breach in cyber context is the use of a computer intrusion to acquire confidential or secure 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 less 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/Customer 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.

**Descriptors**

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

**AI Related:** Information reported contains a reference to artificial intelligence (AI).

**Crimes Against Children:** Related to the sexual abuse/exploitation of children, including child abuse, of complainants age 17 or younger. This descriptor can also be applied when a person from another age group is reporting a crime against a child on behalf of the complainant.

**Cryptocurrency:** Information reported contains some reference to virtual currency.

## 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. Not all complaints include an associated age range. Those without this information are excluded from tables depicting age ranges.
- 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. Losses are de-duplicated as much as possible.
- Losses reported in foreign currencies are converted to U.S. dollars when possible.
- Regarding Ransomware adjusted losses: This number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by an entity. In some cases, entities do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to the FBI via IC3 and do not account for the entity directly reporting to FBI field offices/agents.
- 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.
- All location-based reports are generated from information entered when known/provided by the complainant.
  - Regarding State-related statistics: 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.
  - Complaint counts represent the number of individual complaints received from each state and do not represent the number of individuals filing a complaint.
  - Per 100K Citizens: This information is based on the estimated 2025 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. <https://www.census.gov/data/tables/time-series/demo/pepest/2020s-state-total.html#v2025>

## Appendix D: Public Service Announcements Published in 2025

Title	Date
Threat of Copycat Attacks after ISIS-Inspired Vehicle Attack in New Orleans	13-Jan-25
Beware of Charitable Fraud Related to Mass Casualty and Disaster Events	16-Jan-25
North Korean IT Workers Conducting Data Extortion	23-Jan-25
Mail Theft-Related Check Fraud is on the Rise	27-Jan-25
North Korea Responsible for \$1.5 Billion Bybit Hack	26-Feb-25
Safety Concerns Related to Fraudulent Compounding Practices Associated with Weight Loss Drugs	28-Feb-25
Beijing Leveraging Freelance Hackers and Information Security Companies to Compromise Computer Networks Worldwide	5-Mar-25
Mail Scam Targeting Corporate Executives Claims Ties to Ransomware	6-Mar-25
Violent Online Networks Target Vulnerable and Underage Populations Across the United States and Around the Globe	6-Mar-25
Individuals Target Tesla Vehicles and Dealerships Nationwide with Arson, Gunfire, and Vandalism	21-Mar-25
Criminal Actors Steal US Taxpayer Identity to File False Tax Returns and Claim Refunds	2-Apr-25
FBI Warns of Scammers Impersonating the IC3	18-Apr-25
FBI Seeking Tips about PRC-Targeting of US Telecommunications ( <a href="#">简体中文版</a> ) ( <a href="#">繁體中文版</a> )	24-Apr-25
Cyber Criminals Impersonating Employee Self-Service Websites to Steal Victim Information and Funds	24-Apr-25
Threat Actors Use "Swatting" to Target Victims Nationwide	29-Apr-25
Emerging Discount Medical Insurance Scams	30-Apr-25
Cyber Criminal Proxy Services Exploiting End of Life Routers	7-May-25
Impersonation Scheme Targeting Middle Eastern Students in the United States	13-May-25
Senior US Officials Impersonated in Malicious Messaging Campaign	15-May-25
Cyber Criminals Defraud Hedera Hashgraph Network Non-Custodial Wallet Users Through Nonfungible Token Airdrops Disguised as Free Rewards	3-Jun-25

Recent Attacks Highlight Elevated Threat to Israeli and Jewish Communities	5-Jun-25
Home Internet Connected Devices Facilitate Criminal Activity	5-Jun-25
Criminals Posing as Legitimate Health Insurers and Fraud Investigators to Commit Health Care Fraud	27-Jun-25
Fraudsters Target US Stock Investors through Investment Clubs Accessed on Social Media and Messaging Applications	3-Jul-25
North Korean IT Worker Threats to U.S. Businesses	23-Jul-25
The Com: Theft, Extortion, and Violence are a Rising Threat to Youth Online	23-Jul-25
Hacker Com: Cyber Criminal Subset of The Community (Com) is a Rising Threat to Youth Online	23-Jul-25
In Real Life (IRL) Com: Violent Subset of The Community (Com) is a Rising Threat to Youth Online	23-Jul-25
Unsolicited Packages Containing QR Codes Used to Initiate Fraud Schemes	31-Jul-25
Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds	13-Aug-25
Russian Government Cyber Actors Targeting Networking Devices, Critical Infrastructure	20-Aug-25
ABA Foundation and FBI Release New Infographic to Help Americans Spot and Avoid Deepfake Scams	4-Sep-25
Threat Actors Spoofing the FBI IC3 Website for Possible Malicious Activity	19-Sep-25
Criminals Impersonate US Health Insurance Providers and Chinese Law Enforcement to Target Chinese Speakers Residing in the United States	13-Nov-25
Criminals Using Altered Proof-of-Life Media to Extort Victims in Virtual Kidnapping for Ransom Scams	5-Dec-25
Great Odds, High Risk: The FBI Encourages U.S. Bettors to Know the Risks of Illegal Gambling	17-Dec-25
Senior U.S. Officials Continue to be Impersonated in Malicious Messaging Campaign	19-Dec-25

## Appendix E: Industry Alerts Published in 2025

Title	Date
Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products	13-Jan-25
Product Security Bad Practices	17-Jan-25
Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications	22-Jan-25
Guidance on Digital Forensics and Protective Monitoring Specifications for Producers of Network Devices and Appliances	4-Feb-25
Malicious Cyber Actors Use Buffer Overflow Vulnerabilities to Compromise Software	12-Feb-25
#StopRansomware: Ghost (Cring) Ransomware	19-Feb-25
#StopRansomware: Medusa Ransomware	12-Mar-25
Fast Flux: A National Security Threat	3-Apr-25
BADBAZAAR and MOONSHINE: Spyware Targeting Uyghur, Taiwanese, and Tibetan Groups and Civil Society Actors	9-Apr-25
Phishing Domains Associated with LabHost PhaaS Platform Users (LabHost Domains)	29-Apr-25
Primary Mitigations to Reduce Cyber Threats to Operational Technology	6-May-25
Cyber Criminal Services Target End-of-Life Routers to Launch Attacks and Hide Their Activities	7-May-25
Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations	21-May-25
Russian GRU Targeting Western Logistics Entities and Technology Companies	21-May-25
AI Data Security	22-May-25
Silent Ransom Group Targeting Law Firms	23-May-25
Infrastructure Used to Manage Domains Related to Cryptocurrency Investment Fraud Scams between October 2023 and April 2025	29-May-25
<a href="#">(Funnell Technology Inc. Associated CAMEs)</a> <a href="#">(Complete List of Domains Attributed to Funnell)</a>	
#StopRansomware: Play Ransomware	4-Jun-25
People's Republic of China Cyber Threat Activity	20-Jun-25
Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest	30-Jun-25

#StopRansomware: Interlock	22-Jul-25
Scattered Spider	29-Jul-25
Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators	13-Aug-25
Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System	27-Aug-25
Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion	12-Sep-25
Creating and maintaining a definitive view of your Operational Technology (OT) Architecture	29-Sep-25
#StopRansomware: Akira Ransomware	13-Nov-25
Bulletproof Defense: Mitigating Risks From Bulletproof Hosting Providers	19-Nov-25
Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure	9-Dec-25
Principles for the Secure Integration of Artificial Intelligence in Operational Technology	15-Dec-25

#### INTERNET CRIME COMPLAINT CENTER



REPORT – ANALYZE – ENHANCE – REFER – COLLABORATE – SHARE

#### INTERNET CRIME COMPLAINT CENTER OUTREACH MATERIALS



REPORT – ANALYZE – ENHANCE – REFER – COLLABORATE – SHARE