FVRO

THE FRAUD VICTIM RIGHTS ORGANIZATION

ANALYSIS

Analysis of FBI's 2025 Internet Crime Report

On April 6 the FBI released its 2025 Internet Crime Report, showing a 26% increase in reported financial loss over 2024 due to online crime.[1] This report illustrates several opportunities to reduce scams and consumer fraud in 2026. It also highlights the need for more comprehensive public release of underlying data so additional opportunities for improvement can be identified.

2025 saw several signs of progress is the war against America's scam epidemic.

- Criminal indictments,[2] sanctions,[3] and diplomatic pressure from the U.S. resulted in disruption of large-scale scam compound operations in Cambodia.[4]

- Political instability combined with diplomatic pressure from China resulted in disruption of large-scale scam compound operations in Myanmar.[5]

---

[1] FBI. *Internet Crime Report 2025*, page 4; https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

[2] U.S. v. Chen Zhi; Case # 1:25-cr-00312-RPK, U.S. District Court for the Eastern District of New York.

[3] U.S. Treasury Department. Treasury Sanctions Cambodian Tycoon and Businesses Linked to Human Trafficking and Forced Labor in Furtherance of Cyber and Virtual Currency Scams (September 12, 2024); https://home.treasury.gov/news/press-releases/jy2576;

Financial Crimes Enforcement Network. FinCEN Finds Cambodia-Based Huione Group to be of Primary Money Laundering Concern, Proposes a Rule to Combat Cyber Scams and Heists (May 1, 2025); https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern; and

U.S. Treasury Department. *U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (October 14, 2025); https://home.treasury.gov/news/press-releases/sb0278.

[4] The Guardian. *Thousands of workers flee Cambodia scam centres, officials say* (January 21, 2025); https://www.theguardian.com/world/2026/jan/21/thousands-of-workers-flee-cambodia-scam-centres-officials-say.

[5] South China Morning Post. *Cybercrime crackdown reveals warming ties between China and Myanmar* (September 15, 2023); https://www.scmp.com/news/china/diplomacy/article/3234532/cybercrime-crackdown-reveals-warming-ties-between-china-and-myanmar; and

- U.S. law enforcement relations with overseas counterparts in India[6] and West Africa[7] continued to improve.

- Several important bills have been introduced in Congress focusing on improving law enforcement responses to America's scam epidemic.[8]

As with 2024, the 2025 Internet Crime Report showed 70% of reported loss came from five homogenous scam types specifically associated with three regions of the world.[9]

		REPORTED LOSS FROM COMPLAINTS (IC3)	
Primary Geographic Region	**Scam Initiation Method**	**Crime Type**	**2025**
Southeast Asia	**Text Message or Social Media**	**Cryptocurrency Investment Fraud**	**$7,228,000,000**
West Africa	**Email**	**Business Email Compromise**	**$3,046,598,558**
	Social Media	**Confidence Fraud/Romance Scams**	**$929,287,469**
India	**Phone Call**	**Tech Support Fraud**	**$2,134,675,818**
		Government Impersonation	**$797,943,193**

This indicates the large majority of scam loss comes from a relatively limited number of criminal groups.

U.S. Institute of Peace. *Transnational Crime in Southeast Asia* (May 2024), page 28 and 31; https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf.

[6] Statement for the Record of Gregory Heeb, Deputy Assistant Director, FBI; *U.S. Congress, Join Economic Committee Hearing, The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters* (March 25, 2026), page 6; https://www.jec.senate.gov/public/index.cfm?a=Files.Serve&File_id=2F5CA5C1-44C9-4E23-944E-8008293856F7.

[7] FBI. *Ayotunde Solademi, investigator for the FBI in Lagos, Discusses Financially Motivated Sextortion*; https://www.fbi.gov/video-repository/sextortion-ayo-legat-august2023.mp4/view.

[8] GUARD Act (House); https://www.congress.gov/bill/119th-congress/house-bill/2978;

GUARD Act (Senate); https://www.congress.gov/bill/119th-congress/senate-bill/2544;

Scam Compound Accountability and Mobilization Act; https://www.congress.gov/bill/119th-congress/senate-bill/2950;

National Strategy for Combating Scams Act; https://www.congress.gov/bill/119th-congress/senate-bill/3355;

Strengthening Task Forces to Oppose Predatory Scams Against Seniors Act; https://amo.house.gov/sites/evo-subsites/amo.house.gov/files/evo-media-document/amo_001_xml-stop-scams-against-seniors-act-final.pdf; and

Foreign Robocall Elimination Act; https://www.congress.gov/bill/119th-congress/senate-bill/2666.

[9] FBI. *Internet Crime Report 2025*, page 8; https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

Cryptocurrency Investment Fraud

Cryptocurrency Investment Fraud is primarily associated with large-scale scam compounds in Southeast Asia[10]—though similar operations have been discovered in other parts of the world.[11]

Overall, FBI reported a 26% increase in loss due to internet crime, from $16.6 billion in 2024 to $20.9 billion in 2025.[12] Cryptocurrency Investment Fraud increased 24%, from $5.8 billion in 2024 to $7.2 billion in 2025.[13]

Of note, Investment Fraud not categorized as Cryptocurrency Investment Fraud increased at a significantly higher rate than Cryptocurrency Investment Fraud.[14]

REPORTED LOSS FROM COMPLAINTS (IC3)			
Crime Type	**2024**	**2025**	**Change**
Investment Fraud	**$6,570,639,864**	**$8,648,617,756**	**▲31.6%**
Cryptocurrency Investment Fraud	**$5,819,531,069**	**$7,228,000,000**	**▲24.2%**
Investment Fraud (Other)	**$751,108,795**	**$1,420,617,756**	**▲89.1%**

- Does this indicate the emergence of new fraud types or new large-scale crime groups outside Southeast Asia?

- Or does this mean some investment scams from Southeast Asia were not categorized as Cryptocurrency Investment Fraud because funds were transferred by wire to recipients other than cryptocurrency exchanges?

The IC3 report provides limited details. Other questions are also left unanswered.

- Was the increase in Cryptocurrency Investment Fraud significantly higher than 24% in the first half of 2025 and then significantly lower in the second half?

---

[10] FBI. *Internet Crime Report 2025*, page 19; https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

[11] BBC. Zambia uncovers 'sophisticated' Chinese cybercrime syndicate (April 10, 2024); https://www.bbc.com/news/world-africa-68777137;

BBC. Nigeria deports Chinese scammers in crackdown on 'foreign-led' cyber crime (August 22, 2025); https://www.bbc.com/news/articles/c89059k37ezo; and

Georgia Today. MIA: Illegal call center uncovered in Dusheti hotel, 14 Chinese citizens detained (May 15, 2025); https://georgiatoday.ge/mia-illegal-call-center-uncovered-in-dusheti-hotel-14-chinese-citizens-detained/.

[12] FBI. *Internet Crime Report 2025*, page 4; https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

[13] *Id.*, page 8.

[14] *Id.*

- Or were crackdowns in Myanmar and Cambodia ineffective and/or largely performative?
- Or were scam operations successfully able to relocate and disperse within Myanmar and Cambodia?
- Or did the relocation of large-scale scam operations outside Southeast Asia significantly accelerate in 2025?

Additional public information is needed to answer these questions and develop opportunities for improvement. At a minimum, FBI needs to publish loss statistics by category and month.

Tech Support Fraud and Government Impersonation

Tech Support Fraud and Government Impersonation primarily originate from criminal call centers in India.[15]

		REPORTED LOSS FROM COMPLAINTS (IC3)			
Primary Geographic Region	Scam Initiation Method	Crime Type	2024	2025	Change
India	Phone Call	Tech Support Fraud	$1,464,755,976	$2,134,675,818	▲45.7%
		Government Impersonation	$405,624,084	$797,943,193	▲96.7%

While U.S. law enforcement executives report good relations with their Indian counterparts, the 47% increase in tech support fraud clearly indicates the previous practice of bundling cases into annual or periodic "sweep" operations is not effectively driving deterrence.[16] The cycle time between development of evidence and transmission of Foreign Dissemination Reports to Indian

[15] FBI. Internet Crime Report 2022, page 16; https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf.

[16] FBI. *Internet Crime Report 2025*, page 8; https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

India Today. *CBI searches 105 locations under 'Operation Chakra' against cyber criminals* (October 4, 2022); https://www.indiatoday.in/india/story/cbi-search-multiple-locations-operation-chakra-cyber-crime-financial-fraud-2008321-2022-10-04.

DeshGujarat. *CBI raids 24 locations nationwide, including Gujarat; Recovers Rs. 2.2 cr in fake call center scam* (November 23, 2023); https://deshgujarat.com/2023/11/23/cbi-raids-24-locations-nationwide-including-gujarat-recovers-rs-2-2-cr-in-fake-call-center-scam/.

The Hindu. *Operation Chakra-III: CBI arrests 26 more 'cybercriminals'* (September 30, 2024); https://www.thehindu.com/news/national/operation-chakra-iii-cbi-arrests-26-more-cybercriminals/article68700515.ece.

India Today. *CBI–FBI joint crackdown busts $40 million tech-support scam targeting US nationals* (August 28, 2025); https://www.indiatoday.in/world/us-news/story/cbi-fbi-joint-crackdown-busts-40-million-tech-support-scam-targeting-us-nationals-glbs-2777901-2025-08-28.

police needs to be reduced. U.S. law enforcement needs to focus less on building large, comprehensive cases and more on getting information about locations of scammers to Indian police as quickly as possible.

To facilitate this, internet browser providers like Microsoft, Google, Apple, and Mozilla need to identify and send tech support fraud pop-up ad images to IC3 in near real time.

In addition, the 97% increase in government impersonation loss[17] almost certainly indicates the emergence of new criminal groups outside India—most likely in the Dominican Republic.[18]

Business E-Mail Compromise and Romance Scams

Business E-Mail Compromise and Romance Scams primarily originate from criminal groups in Nigeria and Ghana.[19]

		REPORTED LOSS FROM COMPLAINTS (IC3)			
Primary Geographic Region	Scam Initiation Method	Crime Type	2024	2025	Change
West Africa	Email	Business Email Compromise	$2,770,151,146	$3,046,598,558	▲10.0%
	Social Media	Confidence Fraud/Romance Scams	$672,009,052	$929,287,469	▲38.3%

Of particular note is the fact that loss from these scams do not always increase every year.[20]

	Business Email Compromise	% Change	Confidence Fraud/Romance	% Change
2025	$3,046,598,558	▲10.0%	$929,287,469	▲38.3%
2024	$2,770,151,146	▼6.0%	$672,009,052	▲3.0%
2023	$2,946,830,270	▲7.5%	$652,544,805	▼11.3%
2022	$2,742,354,049	▲14.5%	$735,882,192	▼23.0%
2021	$2,395,953,296	▲28.4%	$956,039,740	▲59.3%
2020	$1,866,642,107	▲5.1%	$600,249,821	▲26.4%
2019	$1,776,549,688		$475,014,032	

[17] FBI. *Internet Crime Report 2025*, page 8; https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

[18] U.S. Department of Justice. *Thirteen Individuals Charged for Operating Transnational Elder Fraud Scheme* (August 12, 2025); https://www.justice.gov/usao-ma/pr/thirteen-individuals-charged-operating-transnational-elder-fraud-scheme.

[19] The London School of Economics. *How do the cybercriminals behind business email compromise fraud operate?* (January 28, 2025); https://www.lse.ac.uk/research/research-for-the-world/society/cybercrime-business-email-fraud.

[20] FBI. *Internet Crime Report* [2019-2025]; https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf, *et seq*.

- Does this indicate the emergence of new criminal groups outside West Africa?
- Or does this indicate West African crime groups transition between scams reported in IC3 data and other frauds such as identity theft, access device fraud, bank fraud, or public benefits fraud that may not be reflected in IC3 complaint data?

Additional public information is needed.

Other Internet Crimes

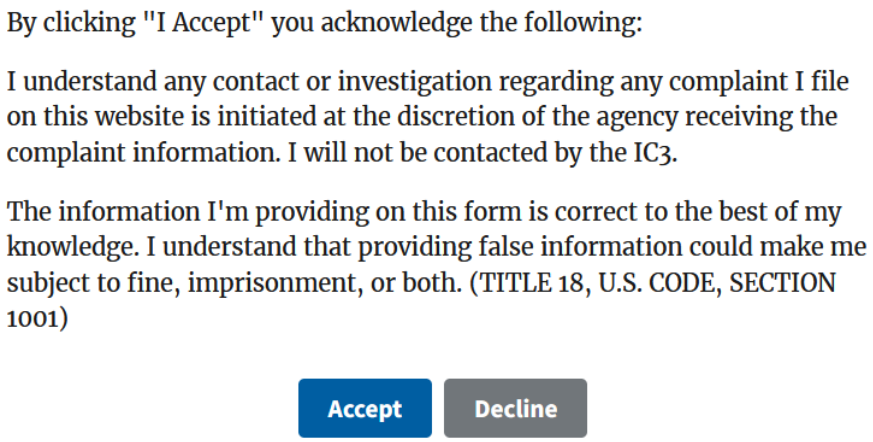
Year-over-year changes in fraud loss for all reported categories internet crime are shown below.[21]

Crime Type	2024 Loss	2025 Loss	% Change	$ Change	$ Change % of Total Change
Cryptocurrency Investment	$5,819,531,069	$7,228,000,000	▲24.20%	▲$1,408,468,931	▲33.49%
Tech Support	$1,464,755,976	$2,134,675,818	▲45.74%	▲$669,919,842	▲15.93%
Investment (Other)	$751,108,795	$1,420,617,756	▲89.14%	▲$669,508,961	▲15.92%
Government Impersonation	$405,624,084	$797,943,193	▲96.72%	▲$392,319,109	▲9.33%
Business Email Compromise	$2,770,151,146	$3,046,598,558	▲9.98%	▲$276,447,412	▲6.57%
Confidence Fraud/Romance	$672,009,052	$929,287,469	▲38.28%	▲$257,278,417	▲6.12%
Other	$280,278,325	$512,146,819	▲82.73%	▲$231,868,494	▲5.51%
Phishing/Spoofing	$70,013,036	$215,843,126	▲208.29%	▲$145,830,090	▲3.47%
Real Estate	$173,586,820	$275,110,419	▲58.49%	▲$101,523,599	▲2.41%
Employment	$264,223,271	$362,934,762	▲37.36%	▲$98,711,491	▲2.35%
Lottery/Sweepstakes/Inheritance	$102,212,250	$194,147,851	▲89.95%	▲$91,935,601	▲2.19%
Credit Card/Check Fraud	$199,889,841	$282,670,235	▲41.41%	▲$82,780,394	▲1.97%
Data Breach	$364,855,818	$435,240,992	▲19.29%	▲$70,385,174	▲1.67%
Advanced Fee	$102,074,512	$155,910,852	▲52.74%	▲$53,836,340	▲1.28%
Ransomware	$12,473,156	$32,320,105	▲159.12%	▲$19,846,949	▲0.47%
Malware	$1,365,945	$19,370,572	▲1318.11%	▲$18,004,627	▲0.43%
IPR/Copyright and Counterfeit	$8,715,512	$26,667,006	▲205.97%	▲$17,951,494	▲0.43%
Harassment/Stalking	$10,611,223	$27,707,167	▲161.11%	▲$17,095,944	▲0.41%
Identity Theft	$174,354,745	$185,832,657	▲6.58%	▲$11,477,912	▲0.27%
Threats of Violence	$1,842,186	$9,509,532	▲416.21%	▲$7,667,346	▲0.18%
Crimes Against Children	$519,424	$6,694,350	▲1188.80%	▲$6,174,926	▲0.15%
Botnet	$8,860,202	$13,859,049	▲56.42%	▲$4,998,847	▲0.12%
Overpayment	$21,452,521	$22,898,075	▲6.74%	▲$1,445,554	▲0.03%
SIM Swap	$25,983,946	$17,366,758	▼33.16%	▼$8,617,188	▼0.20%
Extortion	$143,185,736	$122,499,133	▼14.45%	▼$20,686,603	▼0.49%
Personal Data Breach	$1,453,296,303	$1,314,923,988	▼9.52%	▼$138,372,315	▼3.29%
Non-Payment/Non-Delivery	$785,436,888	$503,373,587	▼35.91%	▼$282,063,301	▼6.71%

[21] FBI. *Internet Crime Report 2025*, page 8; https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

Victim Rights Waivers

Throughout 2025, FBI required crime victims to waive certain rights under the Federal Crime Victims' Rights Act (CVRA) in order to be able to file reports online through IC3.gov.[22] Victims who decline these waivers are unable to file reports online through IC3.gov.



This is almost certainly illegal.

CVRA provides victims of Federal crimes with certain rights, including: "(5) The reasonable right to confer with the attorney for the Government in the case."[23] The purpose of filing a police report is so law enforcement can protect the victim, try to make them hole, and to bring criminals to justice. That is why taxpayers fund law enforcement agencies.

For most internet crimes, there are multiple State, local, and Federal law enforcement agencies with which a crime victim can file a report. If the FBI is unwilling to disclose whether any particular report is being investigated at all, a crime victim has no idea whether or not they should file reports with other agencies.

RAT

The FBI's Recovery Asset Team significantly increased victim recoveries during 2025.[24]

	2024	2025	% Change
Attempted Theft	$848,400,000	$1,163,919,846	▲37.2%
Recovered	$469,100,000	$679,013,183	▲44.7%
Success Rate	55%	58%	▲3.0%

[22] ic3.gov > File a Complaint.

[23] Title 18 United States Code § 3771(a)(5).

[24] *Id.*, page 17.

This indicates additional recovery is possible through streamlining processes; for example: centralizing tasks within IC3 instead of referring recovery attempts to an FBI field office.

Operation Level Up

FBI saw a reduction in the number of fraud victims proactively notified through Operation Level Up.[25]

	2024	2025	% Change
Victims Notified	4,323	3,780	▼**12.6%**

This may have been due to changes in how large-scale scam compounds use certain internet service providers. If so, FBI should explore additional opportunities for notifying scam victims through certain internet service providers.

AI Enabled Crime

The 2025 Internet Crime report showed $893,346,472 in loss (5% of reported loss) from AI enabled cybercrime.[26]

[25] *Id.*, page 20.

[26] *Id.*, page 39.